

Configurazione di vRealize Automation

21 luglio 2021

vRealize Automation 7.6

È possibile trovare la documentazione tecnica più aggiornata sul sito Web di VMware all'indirizzo:

<https://docs.vmware.com/it/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
Centro Leoni Palazzo A
Via Spadolini 5
Ground Floor
Milan, MI 20121
tel: +39 02 30412700
fax: +39 02 30412701
www.vmware.com/it

Copyright © 2015-2021 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

Configurazione di vRealize Automation 6

Informazioni aggiornate 7

1 Preparazioni esterne per il provisioning del blueprint 8

Preparazione dell'ambiente per la gestione di vRealize Automation 8

Elenco di controllo per la preparazione della configurazione di rete e sicurezza di NSX 10

Elenco di controllo per fornire il supporto del provider IPAM di terze parti 15

Elenco di controllo per la configurazione dei Contenitori per vRealize Automation 19

Preparazione dell'ambiente di vCloud Director per vRealize Automation 20

Preparazione dell'ambiente di vCloud Air per vRealize Automation 21

Preparazione dell'ambiente di Amazon Web Services 21

Preparazione delle funzionalità di rete e sicurezza di Red Hat OpenStack 28

Preparazione dell'ambiente di SCVMM 29

Configurazione della connettività VPC da rete ad Azure 30

Preparazione per il provisioning delle macchine 31

Scelta del metodo di provisioning delle macchine da preparare 32

Elenco di controllo per l'esecuzione di script Visual Basic durante il provisioning 35

Utilizzo dell'agente guest di vRealize Automation nel provisioning 36

Elenco di controllo per la preparazione al provisioning tramite clonazione 45

Preparazione per il provisioning di vCloud Air e vCloud Director 60

Preparazione per il provisioning Linux Kickstart 61

Preparazione per il provisioning SCCM 64

Preparazione per il provisioning di WIM 66

Preparazione per il provisioning dell'immagine delle macchine virtuali 74

Preparazione per il provisioning dell'immagine della macchina Amazon 74

Scenario: preparazione di risorse vSphere per il provisioning di macchine 77

Preparazione per il provisioning Software 79

Preparazione per il provisioning delle macchine con Software 80

Preparazione di un modello di vSphere per clonare blueprint di componenti software e macchine 84

Scenario: preparazione per l'importazione di Dukes Bank per il blueprint dell'applicazione campione di vSphere 88

2 Preparazione di tenant e risorse per il provisioning dei blueprint 94

Configurazione delle impostazioni del tenant 94

Scelta delle opzioni di configurazione di Gestione directory 95

Aggiornamento di connettori esterni per la gestione delle directory 165

Scenario: configurazione di un collegamento Active Directory per un vRealize Automation ad alta disponibilità	174
Configurazione dei connettori esterni per smart card e dell'autenticazione del provider di identità di terze parti in vRealize Automation	176
Creazione di un link di Active Directory multidominio o a più foreste	184
Configurazione dei ruoli di utenti e gruppi	186
Creazione di tenant aggiuntivi	194
Eliminazione di un tenant	197
Configurazione delle impostazioni di sicurezza per il multi-tenancy	197
Configurazione del branding personalizzato	198
Elenco di controllo per la configurazione delle notifiche	200
Creazione di un file RDP personalizzato per il supporto di connessioni RDP per le macchine di cui è stato eseguito il provisioning	212
Scenario: aggiunta di posizioni di data center per distribuzioni tra più regioni	212
Configurazione di vRealize Orchestrator	214
Configurazione delle risorse	218
Elenco di controllo per la configurazione di risorse di IaaS	218
Configurazione delle risorse XaaS	367
Creazione e configurazione di contenitori	380
Installazione di plug-in aggiuntivi sul server vRealize Orchestrator predefinito	405
Utilizzo dei criteri di Active Directory	405
Preferenze utente per notifiche e delegati	409

3 Fornire blueprint di servizio agli utenti 410

Progettazione dei blueprint	410
Creazione di una libreria di progettazione	412
Progettazione dei blueprint delle macchine	415
Progettazioni di componenti Software	539
Progettazione di blueprint e azioni risorsa di XaaS	553
Pubblicazione di un blueprint	620
Utilizzo di blueprint gestiti dagli sviluppatori	621
Esportazione e importazione di blueprint e contenuti	621
Download e configurazione del blueprint autonomo fornito	628
Creazione di blueprint e altri contenuti di IaaS in un ambiente con più sviluppatori	628
Assemblaggio di blueprint compositi	629
Informazioni sul comportamento dei blueprint nidificati	631
Utilizzo di componenti macchina e componenti Software durante l'assemblaggio di un blueprint	634
Creazione di binding di proprietà tra componenti di blueprint	636
Creazione di dipendenze e controllo dell'ordine di provisioning	637
Personalizzazione dei moduli di richiesta di blueprint	638
Creazione di un modulo di richiesta personalizzato con opzioni di Active Directory	642
Proprietà personalizzate dei campi di designer modulo	651

Utilizzo delle azioni di vRealize Orchestrator nel designer di moduli personalizzati	657
Utilizzo degli elementi del selettore del valore e del selettore della struttura nel designer moduli personalizzati	659
Utilizzo dell'elemento Griglia dati nel designer di moduli personalizzati	661
Utilizzo della convalida esterna nel designer di moduli personalizzati	666
Richieste di provisioning non riuscite per test e risoluzione dei problemi	671
Funzionamento dell'azione Riprendi	674
Eliminazione forzata di una distribuzione dopo una richiesta di eliminazione non riuscita	676
Risoluzione dei problemi relativi a una distribuzione non riuscita che include un workflow vRealize Orchestrator	677
Gestione del catalogo dei servizi	678
Elenco di controllo per la configurazione del catalogo dei servizi	679
Creazione di un servizio	680
Funzionamento di elementi del catalogo e azioni	683
Creazione di permessi	686
Utilizzo dei criteri di approvazione	694
Richiesta di provisioning di una macchina mediante un blueprint con parametri	723
Scenario: rendere un blueprint dell'applicazione CentOS con MySQL disponibile nel catalogo dei servizi	725

4 Uso del catalogo e gestione delle distribuzioni 730

Utilizzo del catalogo	731
Come inviare una richiesta di catalogo	732
Utilizzo delle distribuzioni	734
Monitoraggio delle richieste di provisioning	734
Gestione degli elementi di catalogo distribuiti	738
Utilizzo della posta in arrivo	785

Configurazione di vRealize Automation

Configurazione di vRealize Automation fornisce informazioni sulla configurazione di vRealize Automation e dell'ambiente esterno in preparazione al provisioning di vRealize Automation e alla gestione del catalogo.

Destinatari

Le presenti informazioni sono destinate ai professionisti IT responsabili per la configurazione dell'ambiente vRealize Automation, nonché per gli amministratori di infrastruttura responsabili per la preparazione di elementi nell'infrastruttura esistente da utilizzare nel provisioning di vRealize Automation. Si rivolgono ad amministratori di sistema Windows o Linux esperti che hanno familiarità con la tecnologia delle macchine virtuali e le operazioni di data center.

Informazioni aggiornate

Nella seguente tabella sono elencate le modifiche apportate a *Configurazione di vRealize Automation* per questa release del prodotto.

Revisione	Descrizione
XX TBD 202X	Aggiornato Configurazione di un provider di metriche .
14 FEB 2020	<ul style="list-style-type: none">■ Aggiornato Visualizzazione delle risorse di elaborazione ed esecuzione della raccolta dati.■ Aggiornato Creazione di un endpoint NSX-T e associazione a un endpoint vSphere in vRealize Automation.
24 OTT 2019	<ul style="list-style-type: none">■ Aggiunto Risoluzione dei problemi relativi alle voci impreviste per il filtro.■ Modifiche e aggiornamenti minori al testo.
9 SET 2019	<ul style="list-style-type: none">■ Aggiunto Configurazione di endpoint di Microsoft Azure.■ Modifiche minori al testo.
18 LUG 2019	Chiarita opzione di propagazione in Impostazioni delle proprietà dei blueprint .
14 GIU 2019	Modifiche minori al testo.
30 MAG 2019	<ul style="list-style-type: none">■ Aggiunto un argomento relativo all'utilizzo della corrispondenza con caratteri jolly con gli utenti JIT. Vedere Utilizzo della corrispondenza basata su caratteri jolly per gli utenti JIT
7 MAG 2019	<ul style="list-style-type: none">■ Corretti un paio di collegamenti ipertestuali.■ Aggiornato Preparazione per il provisioning SCCM per descrivere le proprietà di configurazione aggiunte di recente.
11 APR 2019	Release del documento iniziale.

Preparazioni esterne per il provisioning del blueprint

1

Potrebbe essere necessario creare o preparare alcuni elementi all'esterno di vRealize Automation per supportare il provisioning degli elementi di catalogo. Se ad esempio si desidera fornire un elemento di catalogo per il provisioning di una macchina clone, è necessario creare un modello da cui clonare sull'hypervisor.

Questo capitolo include i seguenti argomenti:

- [Preparazione dell'ambiente per la gestione di vRealize Automation](#)
- [Configurazione della connettività VPC da rete ad Azure](#)
- [Preparazione per il provisioning delle macchine](#)
- [Preparazione per il provisioning Software](#)

Preparazione dell'ambiente per la gestione di vRealize Automation

A seconda dell'ambiente di lavoro, potrebbe essere necessario apportare alcune modifiche alla configurazione prima di poter sottoporre il proprio ambiente alla gestione di vRealize Automation o prima di poter sfruttare determinate funzionalità.

Tabella 1-1. Preparazione dell'ambiente per l'integrazione di vRealize Automation







Ambiente	Preparazioni
 NSX for vSphere e NSX-T	<p>Se si desidera sfruttare NSX for vSphere o NSX-T per gestire rete, sicurezza e funzionalità di bilanciamento del carico di macchine virtuali fornite in provisioning con vRealize Automation, preparare l'istanza di NSX per l'integrazione. Vedere Elenco di controllo per la preparazione della configurazione di rete e sicurezza di NSX.</p>
 vCloud Director	<p>Installare e configurare la propria istanza di vCloud Director, impostare le risorse cloud e vSphere e identificare o creare credenziali appropriate per fornire a vRealize Automation l'accesso all'ambiente vCloud Director. Vedere Preparazione dell'ambiente di vCloud Director per vRealize Automation.</p>
 vCloud Air	<p>Effettuare la registrazione per ottenere il proprio account di vCloud Air, configurare l'ambiente di vCloud Air e identificare o creare credenziali appropriate per fornire a vRealize Automation l'accesso all'ambiente. Vedere Preparazione per il provisioning di vCloud Air e vCloud Director.</p>
 Amazon Web Services	<p>Preparare gli elementi e i ruoli utente nell'ambiente Amazon Web Services per l'uso in vRealize Automation e analizzare le corrispondenze delle funzionalità di Amazon Web Services con le funzionalità di vRealize Automation. Vedere Preparazione dell'ambiente di Amazon Web Services.</p>
<p>Microsoft Azure</p>	<p>Configurare i servizi di rete in modo che utilizzino il tunneling VPN per supportare i componenti software sui blueprint Azure. Vedere Configurazione della connettività VPC da rete ad Azure.</p>
 Red Hat OpenStack	<p>Se si desidera sfruttare Red Hat OpenStack per gestire le funzionalità di networking e sicurezza delle macchine fornite in provisioning con vRealize Automation, preparare la propria istanza di Red Hat OpenStack per l'integrazione. Vedere Preparazione delle funzionalità di rete e sicurezza di Red Hat OpenStack.</p>

Tabella 1-1. Preparazione dell'ambiente per l'integrazione di vRealize Automation (continua)

Ambiente	Preparazioni
 SCVMM	Configurare le impostazioni di storage e networking e informarsi sulle restrizioni imposte sui nomi dei modelli e dei profili hardware. Vedere Preparazione dell'ambiente di SCVMM .
Provider IPAM esterni	Registrare un pacchetto o plug-in di provider IPAM esterni, eseguire i workflow di configurazione e registrare la soluzione IPAM come nuovo endpoint di vRealize Automation. Vedere Elenco di controllo per fornire il supporto del provider IPAM di terze parti .
Tutti gli altri ambienti	Non è necessario apportare modifiche al proprio ambiente. È possibile iniziare a prepararsi per il provisioning della macchina creando modelli, ambienti di avvio o immagini della macchina. Vedere Preparazione per il provisioning delle macchine .

Elenco di controllo per la preparazione della configurazione di rete e sicurezza di NSX

Prima di poter utilizzare le opzioni di rete e sicurezza di NSX in vRealize Automation, è necessario configurare l'ambiente di rete e sicurezza di NSX for vSphere o NSX-T esterno che si intende utilizzare.

Per utilizzare XaaS per estendere l'integrazione di vRealize Automation e NSX for vSphere, installare il plug-in NSX in vRealize Orchestrator. Il plug-in non supporta NSX-T.

Nella preparazione per l'utilizzo delle funzionalità di rete, sicurezza e bilanciamento del carico di NSX in vRealize Automation, quando si utilizzano credenziali di NSX Manager è necessario utilizzare l'account amministratore di NSX Manager.

vRealize Automation supporta NSX for vSphere e NSX-T. Per informazioni relative all'applicazione NSX, vedere la [documentazione del prodotto NSX for vSphere](#) o la [documentazione del prodotto NSX-T](#).

La maggior parte delle impostazioni di rete e sicurezza NSX che si utilizzano in vRealize Automation viene configurata esternamente e resa disponibile dopo l'esecuzione della raccolta dati nelle risorse di elaborazione.

Per informazioni sulle impostazioni NSX che è possibile configurare per i blueprint di vRealize Automation, vedere [Configurazione delle impostazioni dei componenti rete e sicurezza in vRealize Automation](#).

Tabella 1-2. Elenco di controllo per la preparazione di rete e sicurezza di NSX

Attività	Posizione	Dettagli
<input type="checkbox"/> Configurare le impostazioni di rete di NSX, incluse le impostazioni del gateway e della zona di trasporto.	Configurare le impostazioni di rete nell'applicazione NSX.	<p>A seconda del prodotto NSX in uso, vedere gli argomenti relativi all'amministrazione nella documentazione di NSX seguente:</p> <ul style="list-style-type: none"> ■ Documentazione del prodotto NSX for vSphere ■ Documentazione del prodotto NSX-T
<input type="checkbox"/> Creare i tag, i gruppi e i criteri di sicurezza di NSX.	Configurare le impostazioni di sicurezza nell'applicazione NSX in uso.	<p>A seconda del prodotto NSX in uso, vedere gli argomenti relativi all'amministrazione nella documentazione di NSX seguente:</p> <ul style="list-style-type: none"> ■ Documentazione del prodotto NSX for vSphere ■ Documentazione del prodotto NSX-T

Tabella 1-2. Elenco di controllo per la preparazione di rete e sicurezza di NSX (continua)

Attività	Posizione	Dettagli
<input type="checkbox"/> Configurare le impostazioni di bilanciamento del carico di NSX.	Configurare le impostazioni di bilanciamento del carico di NSX nell'applicazione NSX in uso.	<p>A seconda del prodotto NSX in uso, vedere gli argomenti relativi all'amministrazione nella documentazione di NSX seguente:</p> <ul style="list-style-type: none"> ■ Documentazione del prodotto NSX for vSphere ■ Documentazione del prodotto NSX-T <p>Vedere anche l'argomento relativo alle proprietà personalizzate per i servizi di rete nel PDF <i>Guida di riferimento alle proprietà personalizzate</i> in docs.vmware.com.</p>
<input type="checkbox"/> Per distribuzioni con vCenter incrociati in NSX for vSphere, verificare che il manager di elaborazione NSX abbia il ruolo di managerNSX primario.	Il provisioning di vRealize Automation richiede che il manager NSX di elaborazione per la regione in cui si trovano le macchine abbia il ruolo di manager NSX primario.	<p>Vedere Requisiti dell'amministratore per gli oggetti universali NSX for vSphere di provisioning.</p> <p>Le informazioni su distribuzione con vCenter incrociati, oggetti universali e il ruolo di manager NSX primario sono disponibili nella documentazione del prodotto NSX for vSphere.</p>

Installazione del plug-in NSX su vRealize Orchestrator

L'installazione del plug-in NSX richiede il download del file del programma d'installazione vRealize Orchestrator, l'uso dell'interfaccia di configurazione di vRealize Orchestrator per caricare il file del plug-in e l'installazione del plug-in su un server vRealize Orchestrator.

Per informazioni generali su aggiornamento e risoluzione dei problemi del plug-in, vedere la [documentazione del prodotto vRealize Orchestrator](#).

Prerequisiti

Per utilizzare XaaS per estendere l'integrazione di vRealize Automation e NSX for vSphere, installare il plug-in NSX in vRealize Orchestrator. Il plug-in non supporta NSX-T.

Se si utilizza un'istanza di vRealize Orchestrator incorporata che contiene già un plug-in NSX installato, è possibile ignorare questa procedura.

- Assicurarsi di eseguire un'istanza di vRealize Orchestrator supportata.
Per informazioni sull'impostazione di vRealize Orchestrator, vedere *Installazione e configurazione di VMware vRealize Orchestrator* nella [documentazione del prodotto vRealize Orchestrator](#).
- Assicurarsi di avere le credenziali di un account dotato dell'autorizzazione a installare plug-in di vRealize Orchestrator e ad autenticare tramite vCenter Single Sign-On.
- Assicurarsi di avere installato il client vRealize Orchestrator e che sia possibile accedere con credenziali dell'amministratore.
- Verificare la versione corretta del plug-in NSX nella [matrice di supporto di vRealize Automation](#).

Procedura

- 1 Scaricare il file del plug-in in una posizione accessibile dal server vRealize Orchestrator.
Il formato del nome del file del programma d'installazione del plug-in, con i valori di versione appropriati, è `o11nplugin-nsx-1.n.n.vmoapp`. I file di installazione del plug-in di NSX for vSphere sono disponibili nel [sito di download dei prodotti VMware](#).
- 2 Aprire un browser e avviare l'interfaccia di configurazione di vRealize Orchestrator.
Un esempio del formato dell'URL è `https://orchestrator_server.com:8283`.
- 3 Fare clic su **Plug-Ins** nel riquadro sinistro e scorrere verso il basso fino alla sezione Installa nuovo plug-in.
- 4 Nella casella di testo **File plug-in**, selezionare il file del programma d'installazione e fare clic su **Carica e installa**.
Il file deve essere nel formato `.vmoapp`.
- 5 Quando richiesto, accettare il contratto di licenza nel riquadro Installa plug-in.

- 6 Nella sezione relativa agli stati d'installazione dei plug-in Enabled, verificare che sia specificato il nome corretto per il plug-in di NSX.

Per informazioni sulla versione, vedere la [matrice di supporto di vRealize Automation](#).

Viene mostrato lo stato Il plug-in sarà installato al prossimo riavvio del server.

- 7 Riavviare il servizio server di vRealize Orchestrator.
- 8 Riavviare l'interfaccia di configurazione di vRealize Orchestrator.
- 9 Fare clic su **Plug-in** e verificare che lo stato sia cambiato in **Installazione eseguita**.
- 10 Avviare l'applicazione client di vRealize Orchestrator, accedere e utilizzare la scheda **Workflow** per sfogliare il contenuto della libreria fino alla cartella NSX.

È possibile sfogliare i workflow forniti dal plug-in NSX.

Operazioni successive

Creare un endpoint vRealize Orchestrator in vRealize Automation per l'esecuzione di workflow. Vedere [Creazione di un endpoint vRealize Orchestrator](#).

Requisiti dell'amministratore per gli oggetti universali NSX for vSphere di provisioning

Per eseguire il provisioning delle macchine in un ambiente NSX con vCenter incrociati quando si utilizzano oggetti universali NSX, è necessario eseguire il provisioning in un vCenter Server in cui il manager di elaborazione NSX abbia il ruolo primario.

In un ambiente NSX for vSphere con vCenter incrociati, è possibile avere più server vCenter, ognuno dei quali deve essere associato al proprio manager NSX. A un manager NSX viene assegnato il ruolo di manager NSX primario, mentre agli altri quello di manager NSX secondario.

Il manager NSX primario può creare oggetti universali, ad esempio commutatori logici universali. Questi oggetti vengono sincronizzati con i manager NSX secondari. Dai manager NSX secondari è possibile visualizzare questi oggetti, ma non è possibile modificarli. Per gestire gli oggetti universali, è necessario utilizzare il manager NSX primario. Il manager NSX primario può essere utilizzato per configurare i manager NSX secondari nell'ambiente.

Per ulteriori informazioni sull'ambiente con vCenter incrociati NSX, vedere *Overview of Cross-vCenter Networking and Security* nella guida all'amministrazione di NSX nella [documentazione del prodotto NSX for vSphere](#).

Per un endpoint vSphere (vCenter) associato all'endpoint NSX di un manager NSX primario, vRealize Automation supporta oggetti locali NSX, ad esempio commutatori logici locali, edge gateway locali, bilanciamenti del carico locali, gruppi di sicurezza e tag di sicurezza. Supporta inoltre reti One-to-One o One-to-Many NAT con zona di trasporto universale, reti instradate con zona di trasporto universale e router logici distribuiti universali, nonché un bilanciamento del carico con qualsiasi tipo di rete.

vRealize Automation non supporta gruppi o tag di sicurezza universali NSX esistenti o su richiesta.

Per eseguire il provisioning di reti su richiesta locali come manager NSX primario, utilizzare una zona di trasporto locale specifica di vCenter. È possibile configurare le prenotazioni vRealize Automation affinché utilizzino la zona di trasporto locale e i cavi virtuali per le distribuzioni nel vCenter Server locale specificato.

Se si connette un endpoint vSphere (vCenter) a un endpoint manager NSX secondario corrispondente, è possibile eseguire il provisioning e utilizzare solo oggetti locali.

vRealize Automation può utilizzare un commutatore logico universale NSX come una rete esterna. Se è presente un commutatore universale, ne vengono raccolti i dati e vien quindi collegato o utilizzato da ciascuna macchina nella distribuzione.

- Il provisioning di una rete su richiesta in una zona di trasporto universale può creare un nuovo adattatore logico universale.
- Il provisioning di una rete su richiesta in una zona di trasporto universale nel manager NSX primario crea un adattatore logico universale.
- Il provisioning di una rete su richiesta in una zona di trasporto universale in un manager NSX secondario non viene eseguito correttamente, perché NSX non può creare un commutatore logico universale in un manager NSX secondario.

Per ulteriori informazioni sugli oggetti universali NSX, leggere l'articolo della Knowledge Base di VMware *Deployment of vRealize Automation blueprints with NSX objects fail (2147240)* all'indirizzo <http://kb.vmware.com/kb/2147240>.

Elenco di controllo per fornire il supporto del provider IPAM di terze parti

È possibile ottenere indirizzi e intervalli IP da utilizzare nella definizione del profilo di rete da un provider IPAM di terze parti supportato, ad esempio Infoblox.

Prima che sia possibile creare e utilizzare un endpoint di provider IPAM esterni in un profilo di rete di vRealize Automation, è necessario scaricare oppure ottenere in altro modo un plug-in o un pacchetto del provider IPAM di vRealize Orchestrator, importarlo ed eseguire i workflow richiesti in vRealize Orchestrator, quindi registrare la soluzione IPAM come endpoint di vRealize Automation.

Per una panoramica sul processo di provisioning per l'utilizzo di un provider IPAM esterno al fine di fornire un intervallo di indirizzi IP possibili, consultare [Provisioning di una distribuzione di vRealize Automation mediante un provider IPAM di terze parti](#).

Tabella 1-3. Elenco di controllo per la preparazione del supporto di provider IPAM esterno

Attività	Descrizione	Dettagli
<input type="checkbox"/> Ottenere e importare il plug-in di vRealize Orchestrator del provider IPAM esterno.	<p>Scaricare il plug-in o il pacchetto del provider IPAM, ad esempio il plug-in The Infoblox IPAM Plug-in for vRealize Orchestrator e la documentazione di supporto, da VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) e importarlo in vRealize Orchestrator.</p> <p>Se VMware Solution Exchange non include il pacchetto del provider IPAM necessario, è possibile crearne uno utilizzando l'SDK di un provider di soluzioni IPAM di terze parti e la documentazione di supporto corrispondente.</p> <p>L'SDK di un provider di soluzioni IPAM di terze parti specifico della versione di vRealize Automation, la documentazione di supporto e il pacchetto starter associato per vRealize Orchestrator e vRealize Automation sono disponibili all'indirizzo https://code.vmware.com/sdks o https://code.vmware.com/samples.</p>	<p>Vedere Download e importazione di un pacchetto di un provider IPAM di terze parti in vRealize Orchestrator.</p>
<input type="checkbox"/> Eseguire i workflow di configurazione richiesti e registrare la soluzione IPAM esterna come endpoint di vRealize Automation.	<p>Eseguire il workflow di configurazione di vRealize Orchestrator e registrare il tipo di endpoint del provider IPAM in vRealize Orchestrator.</p>	<p>Vedere Eseguire il workflow per registrare il tipo di endpoint IPAM di terze parti in vRealize Orchestrator.</p>

Download e importazione di un pacchetto di un provider IPAM di terze parti in vRealize Orchestrator

Per preparare la definizione e l'utilizzo dell'endpoint di un provider IPAM di terze parti, è innanzitutto necessario ottenere il pacchetto del provider IPAM di terze parti e importarlo in vRealize Orchestrator.

È possibile scaricare e utilizzare un plug-in del provider di gestione degli indirizzi IP di terze parti esistente, ad esempio IPAM di Infoblox. È inoltre possibile creare un plug-in o un pacchetto IPAM di terze parti personalizzato utilizzando un pacchetto starter fornito da VMware e la documentazione del relativo SDK da utilizzare con un altro provider di soluzioni IPAM di terze parti, ad esempio BlueCat.

- Scaricare il plug-in [Plug-in IPAM di Infoblox per vRealize Orchestrator](#) e la documentazione di supporto da marketplace.vmware.com. Il download contiene anche la documentazione per l'installazione e l'utilizzo del plug-in.

- Creare una soluzione IPAM personalizzata di terze parti scaricando e utilizzando un SDK del provider di soluzioni IPAM di terze parti, la documentazione di supporto e un pacchetto starter associato per vRealize Orchestrator e vRealize Automation. Vedere la pagina [Esempio di pacchetto IPAM di terze parti di vRealize Automation](#) in code.vmware.com/web/sdk.

Dopo aver importato il plug-in o il pacchetto del provider IPAM di terze parti in vRealize Orchestrator, è necessario eseguire i workflow richiesti e registrare il tipo di endpoint IPAM in vRealize Orchestrator.

Per ulteriori informazioni sull'importazione di plug-in e pacchetti e sull'esecuzione dei workflow di vRealize Orchestrator, consultare *Utilizzo del client di VMware vRealize Orchestrator*. Per ulteriori informazioni su come estendere vRealize Automation con plug-in, pacchetti e flussi di lavoro di vRealize Orchestrator, consultare *Estensibilità del ciclo di vita*.

In questa sequenza di passaggi viene utilizzato il plug-in Infoblox IPAM come esempio. La sequenza di passaggi effettiva potrebbe essere diversa in base alla versione di vRealize Automation o del plug-in in uso.

Prerequisiti

- Scaricare il pacchetto o il plug-in da marketplace.vmware.com.
- Accedere a vRealize Orchestrator con i privilegi di amministratore per importare, configurare e registrare un plug-in o un pacchetto di vRealize Orchestrator.

Procedura

1 Aprire il sito marketplace.vmware.com.

2 Individuare e scaricare il plug-in o il pacchetto.

Ad esempio, importare il plug-in Infoblox che supporta l'endpoint IPAM di terze parti Infoblox in vRealize Orchestrator e vRealize Automation 7.1 e versione successiva.

- Nella categoria **Publisher**, selezionare **Infoblox** e fare clic su **Apply**.
- Selezionare [The Infoblox Plug-in for vRealize Orchestrator](#).
- Fare clic su **Tech Specs** e controllare i prerequisiti.
- Per informazioni aggiuntive e per ricevere un'e-mail con il collegamento al download, fare clic su **Try**.
- Scaricare il file ZIP come specificato nelle istruzioni inviate tramite e-mail.

La versione 4.0 e quelle successive del plug-in supportano vRealize Automation 7.1 e versioni successive. Il file zip contiene anche la documentazione relativa al plug-in.

- 3 In vRealize Orchestrator, fare clic sulla scheda **Amministratore** e fare clic su **Importa pacchetto**.
- 4 Selezionare il pacchetto da importare.
- 5 Selezionare tutti i workflow e gli artefatti e fare clic sul pulsante per **importare gli elementi selezionati**.

Operazioni successive

[Eseguire il workflow per registrare il tipo di endpoint IPAM di terze parti in vRealize Orchestrator.](#)

Eseguire il workflow per registrare il tipo di endpoint IPAM di terze parti in vRealize Orchestrator

Eseguire il workflow di registrazione in vRealize Orchestrator per supportare l'utilizzo di vRealize Automation del provider IPAM di terze parti e registrare il tipo di endpoint IPAM per l'utilizzo in vRealize Automation.

Prerequisiti

- [Download e importazione di un pacchetto di un provider IPAM di terze parti in vRealize Orchestrator](#)
- Verificare di avere effettuato l'accesso a vRealize Orchestrator con l'autorizzazione per eseguire i workflow di registrazione.
- Prepararsi all'immissione delle credenziali di amministratore di vRealize Automation quando richiesto dal workflow di registrazione. Quando si registrano tipi di endpoint IPAM in vRealize Orchestrator, viene richiesto di immettere le credenziali dell'amministratore di vRealize Automation.

Procedura

- 1 In vRealize Orchestrator, fare clic sulla scheda **Progettazione**, selezionare **Amministratore > Libreria**, quindi selezionare l'opzione relativa all'**SDK del pacchetto di servizi IPAM**.

Ogni pacchetto di provider IPAM ha un nome univoco e contiene workflow univoci. Ciascun provider prevede il proprio workflow di registrazione. Sebbene i nomi dei workflow potrebbero essere simili tra i provider di pacchetti, la posizione dei workflow in vRealize Orchestrator può variare ed è specifica in base ai singoli provider.

- 2 Per questo esempio, eseguire il workflow di registrazione di **Register IPAM Endpoint** e specificare il tipo di endpoint di Infoblox IPAM.
- 3 Quando vengono richieste le credenziali di vRealize Automation, immettere le credenziali di amministratore di vRealize Automation ad esempio quelle di amministratore di struttura.

Per il workflow di registrazione, è necessario fornire le credenziali di amministratore di sistema di vRealize Automation. Anche quando un utente amministratore non di sistema è connesso al client vRealize Orchestrator, se vengono fornite le credenziali di amministratore di sistema di vRealize Automation per il workflow, la registrazione verrà eseguita correttamente.

Risultati

In questo esempio, il pacchetto registra Infoblox come nuovo tipo di endpoint IPAM nel servizio endpoint di vRealize Automation e lo rende disponibile durante la creazione o la modifica di endpoint in vRealize Automation.

Nota Se la connessione IPAM Infoblox non viene più visualizzata nella scheda vRealize Orchestrator **Inventario** dopo aver riavviato il server di vRealize Orchestrator nel Control Center di vRealize Orchestrator. Per risolvere questo problema, eseguire il workflow **Create IPAM Connection** dalla sequenza di menu **vRO admin > Libreria > Infoblox > vRA > Helper**. Nella scheda **Inventario** di vRealize Orchestrator, è quindi possibile selezionare **IPAM Infoblox** e aggiornare la pagina per visualizzare la connessione IPAM Infoblox.

Operazioni successive

A questo punto, è possibile creare un endpoint di tipo Infoblox IPAM o un endpoint per qualsiasi pacchetto o plug-in di terze parti appena registrato, in vRealize Automation. Vedere [Creazione di un endpoint di un provider IPAM di terze parti](#).

Elenco di controllo per la configurazione dei Contenitori per vRealize Automation

Per iniziare a utilizzare i Contenitori, è necessario configurare la funzionalità di supporto dei ruoli utente di vRealize Automation.

Dopo aver configurato le definizioni dei contenitori in Contenitori è possibile aggiungere e configurare i componenti dei contenitori in un blueprint.

Tabella 1-4. Elenco di controllo per la configurazione dei Contenitori per vRealize Automation

Attività	Dettagli
Assegnare i ruoli di amministratore e di architetto di contenitori.	Vedere le informazioni sui ruoli dei contenitori in <i>Nozioni fondamentali e concetti</i> .
Specificare le definizioni dei contenitori nella scheda Contenitori di vRealize Automation.	Vedere <i>Configurazione di vRealize Automation</i> .
Nella scheda Progettazione di vRealize Automation aggiungere i componenti dei contenitori e i componenti della rete dei contenitori nei blueprint.	Vedere <i>Configurazione di vRealize Automation</i> .

Configurazione di Contenitori mediante l'appliance vRealize Automation

È possibile accedere alle informazioni sui servizi Xenon nell'appliance vRealize Automation (Impostazioni **vRA > Xenon**).

Contiene informazioni sulla VM dell'host Xenon, sulla porta di ascolto e sullo stato dei servizi. Vengono inoltre fornite informazioni sui nodi di cluster Xenon.

È possibile gestire il servizio Linux Xenon con i seguenti comandi CLI nell'appliance vRealize Automation.

Comando	Descrizione
<code>service xenon-service status</code>	Mostra se il servizio è in esecuzione o se è stato interrotto.
<code>service xenon-service start</code>	Avvia il servizio.
<code>service xenon-service stop</code>	Interrompe il servizio.
<code>service xenon-service restart</code>	Riavvia il servizio.
<code>service xenon-service get_host</code>	Mostra il nome host con cui viene eseguito il servizio.
<code>service xenon-service get_port</code>	Mostra la porta del servizio.
<code>service xenon-service status_cluster</code>	Mostra informazioni su tutti i nodi di cluster in formato JSON.
<code>service xenon-service reset</code>	Elimina la directory in Xenon che contiene i file di configurazione e riavvia il servizio.

Clustering dei contenitori

È possibile utilizzare il servizio Xenon insieme a Contenitori per vRealize Automation per aggiungere nodi a un cluster. Se i nodi sono raggruppati in cluster, all'avvio il servizio Xenon connette altri nodi automaticamente.

È possibile monitorare lo stato del cluster dalla scheda **Xenon** nell'appliance vRealize Automation oppure eseguendo il comando seguente in un'istanza di CLI:

```
service xenon-service status_cluster
```

Xenon supporta il clustering basato sul quorum. Il quorum viene calcolato con la formula $(\text{number of nodes} / 2) + 1$.

Preparazione dell'ambiente di vCloud Director per vRealize Automation

Prima di poter integrare vCloud Director con vRealize Automation, è necessario installare e configurare l'istanza di vCloud Director, configurare le risorse vSphere e cloud e identificare o creare credenziali appropriate per fornire a vRealize Automation l'accesso all'ambiente vCloud Director.

Configurazione dell'ambiente

Configurare le risorse vSphere e le risorse cloud, incluse le reti e i data center virtuali. Per ulteriori informazioni, vedere la documentazione di vCloud Director.

Credenziali richieste per l'integrazione

Creare o identificare le credenziali di amministratore dell'organizzazione o di amministratore di sistema che gli amministratori IaaS di vRealize Automation possono utilizzare per includere l'ambiente vCloud Director sotto la gestione di vRealize Automation come endpoint.

Considerazioni sui ruoli utente

I ruoli degli utenti di vCloud Director in un'organizzazione non devono necessariamente coincidere con i ruoli nei gruppi di business di vRealize Automation. Se l'account utente non esiste in vCloud Director, vCloud Director esegue una ricerca nel servizio di directory LDAP o Active Directory associato e crea l'account utente se l'utente esiste nell'archivio identità. Se non è possibile creare l'account utente, viene registrato un avviso ma viene terminato il processo di provisioning con errore. La macchina con provisioning eseguito viene quindi assegnata all'account utilizzato per configurare l'endpoint vCloud Director.

Per informazioni sulla gestione degli utenti di vCloud Director, vedere la documentazione di vCloud Director.

Preparazione dell'ambiente di vCloud Air per vRealize Automation

Prima di integrare vCloud Air con vRealize Automation, è necessario registrare l'account per vCloud Air, configurare l'ambiente di vCloud Air e identificare o creare credenziali appropriate per fornire a vRealize Automation l'accesso all'ambiente.

Configurazione dell'ambiente

Configurare l'ambiente attenendosi alle istruzioni riportate nella documentazione di vCloud Air.

Credenziali richieste per l'integrazione

Creare o identificare le credenziali di amministratore di infrastruttura virtuale o di amministratore account che gli amministratori IaaS di vRealize Automation possono utilizzare per includere l'ambiente vCloud Air sotto la gestione di vRealize Automation come endpoint.

Considerazioni sui ruoli utente

I ruoli degli utenti di vCloud Air in un'organizzazione non devono necessariamente coincidere con i ruoli nei gruppi di business di vRealize Automation. Per informazioni sulla gestione degli utenti di vCloud Air, vedere la documentazione di vCloud Air.

Preparazione dell'ambiente di Amazon Web Services

Preparare gli elementi e i ruoli utente nell'ambiente Amazon Web Services, preparare Amazon Web Services per comunicare con l'agente guest e con l'agente di avvio automatico di Software e analizzare le corrispondenze delle funzionalità di Amazon Web Services con le funzionalità di vRealize Automation.

Ruoli utente di Amazon Web Services e credenziali richieste per vRealize Automation

È necessario configurare le credenziali in Amazon AWS con le autorizzazioni necessarie per consentire a vRealize Automation di gestire l'ambiente esistente.

vRealize Automation richiede le chiavi di accesso per le credenziali degli endpoint e non supporta nomi utente e password.

■ Ruoli e autorizzazioni in Amazon Web Service

Il ruolo di Power User in AWS concede a un utente o un gruppo di AWS Directory Service l'accesso completo ai servizi e alle risorse di AWS, ma non è obbligatorio. Sono inoltre supportati ruoli utente con privilegi inferiori. Il criterio di protezione di AWS che soddisfa le esigenze delle funzionalità di vRealize Automation è:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",

      "ec2:DisassociateAddress",
      "ec2:GetPasswordData",

      "ec2:ImportKeyPair",
      "ec2:ImportVolume",

      "ec2:CreateVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:ModifyVolumeAttribute",
      "ec2:DetachVolume",

      "ec2:AssignPrivateIpAddresses",
      "ec2:UnassignPrivateIpAddresses",

      "ec2:CreateKeyPair",
      "ec2>DeleteKeyPair",
```

```

        "ec2:CreateTags",
        "ec2:AssociateAddress",
        "ec2:ReportInstanceState",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}]

```

■ Credenziali di autenticazione in Amazon Web Services

Per poter gestire utenti e gruppi di Amazon Identity and Access Management (IAM), è necessario essere configurati con le credenziali di amministratore con accesso completo di AWS.

Quando si crea un endpoint AWS in vRA, viene chiesto di immettere una chiave e la chiave privata. Per ottenere la chiave di accesso necessaria per creare l'endpoint Amazon, l'amministratore deve richiedere una chiave da un utente che dispone delle credenziali di amministratore con accesso completo di AWS oppure essere configurato ulteriormente con il criterio di amministratore con accesso completo di AWS. Vedere [Creazione di un endpoint Amazon](#).

Per informazioni sull'attivazione di criteri e ruoli, vedere la sezione *AWS Identity and Access Management (IAM)* della documentazione di prodotto di Amazon Web Services.

Comunicazione tra Amazon Web Services e gli agenti di avvio automatico e guest di Software

Se si intende eseguire il provisioning di blueprint di applicazioni contenenti Software, oppure si desidera poter personalizzare ulteriormente le macchine fornite in provisioning utilizzando l'agente guest, occorre attivare la connettività tra l'ambiente Amazon Web Services (in cui è stato eseguito il provisioning delle macchine) e l'ambiente vRealize Automation (in cui gli agenti scaricano pacchetti e ricevono istruzioni).

Quando si utilizza vRealize Automation per eseguire il provisioning di macchine Amazon Web Services con l'agente guest di vRealize Automation e l'agente di avvio automatico di Software, è necessario impostare la connettività tra la rete e Amazon VPC affinché le macchine fornite in provisioning possano comunicare con vRealize Automation per esigenze di personalizzazione.

Per ulteriori informazioni sulle opzioni di connettività VPC di Amazon Web Services, vedere la documentazione relativa a Amazon Web Services.

Utilizzo delle funzionalità opzionali di Amazon

vRealize Automation supporta diverse funzionalità di Amazon, inclusi Amazon Virtual Private Cloud, bilanciamenti del carico flessibili, indirizzi IP flessibili e volumi EBOS (Elastic Block Storage).

Utilizzo dei gruppi di sicurezza di Amazon

Quando si crea una prenotazione Amazon, specificare almeno un gruppo di sicurezza. Ogni regione disponibile richiede almeno un gruppo di sicurezza specificato.

Un gruppo di sicurezza agisce come un firewall per controllare l'accesso a una macchina. Ogni regione include almeno il gruppo di sicurezza predefinito. Gli amministratori possono utilizzare la Amazon Web Services Management Console per creare gruppi di sicurezza aggiuntivi, configurare porte per Microsoft Remote Desktop Protocol o SSH e configurare una rete privata virtuale per una Amazon VPN.

Quando si crea una prenotazione Amazon o si configura un componente macchina nel blueprint, è possibile scegliere dall'elenco dei gruppi di sicurezza che sono disponibili nella regione dell'account Amazon specificato. I gruppi di sicurezza vengono importati durante la raccolta dati.

Per informazioni sulla creazione e l'uso dei gruppi di sicurezza in Amazon Web Services, consultare la documentazione di Amazon.

Le regioni di Amazon Web Service

Ciascun account di Amazon Web Services è rappresentato da un endpoint cloud. Quando si crea un endpoint Amazon Elastic Cloud Computing in vRealize Automation, vengono raccolte le regioni come risorse di elaborazione. Dopo che l'amministratore di IaaS ha selezionato le risorse di elaborazione per un gruppo di business, vengono eseguite automaticamente le operazioni di raccolta dei dati di inventario e degli stati.

La raccolta dati inventario, eseguita automaticamente una volta al giorno, raccoglie i dati relativi a ciò che si trova su una risorsa di elaborazione, come ad esempio i seguenti dati:

- Indirizzi IP flessibili
- Bilanciamenti del carico flessibili
- Volumi EBS

La raccolta dati di stato viene eseguita automaticamente ogni 15 minuti per impostazione predefinita. Essa raccoglie le informazioni sullo stato delle istanze gestite, che sono istanze create da vRealize Automation. Esempi di dati di stato sono i seguenti:

- Password di Windows
- Stato delle macchine nei bilanciamenti del carico
- Indirizzi IP flessibili

Un amministratore di struttura può avviare, disattivare o cambiare la frequenza della raccolta dei dati di inventario e degli stati.

Utilizzo di Amazon Virtual Private Cloud

Amazon Virtual Private Cloud consente di eseguire il provisioning di istanze di macchine Amazon in una sezione privata del cloud di Amazon Web Services.

Gli utenti di Amazon Web Services possono utilizzare Amazon VPC per progettare una topologia di rete virtuale in base alle specifiche richieste. È possibile assegnare un Amazon VPC in vRealize Automation. Tuttavia vRealize Automation non tiene traccia del costo d'uso di Amazon VPC.

Quando si esegue il provisioning utilizzando Amazon VPC, vRealize Automation presume la presenza di una subnet di VPC da cui Amazon ottiene un indirizzo IP primario. Questo indirizzo è statico finché l'istanza non viene terminata. È possibile anche utilizzare il pool di indirizzi IP flessibili per associare un indirizzo IP flessibile a un'istanza in vRealize Automation. Ciò consentirebbe all'utente di conservare lo stesso IP se esegue continuamente provisioning e disinstallazione di un'istanza in Amazon Web Services.

Utilizzare la AWS Management Console per creare i seguenti elementi:

- Un Amazon VPC, che includa gateway Internet, tabella di routing, gruppi di sicurezza e subnet e indirizzi IP disponibili.
- Una Amazon Virtual Private Network se gli utenti devono accedere alle istanze delle macchine Amazon al di fuori della AWS Management Console.

Operando con una Amazon VPC, gli utenti di vRealize Automation possono eseguire le seguenti attività:

- Un amministratore di struttura può assegnare un Amazon VPC a una prenotazione cloud. Vedere [Creazione di una prenotazione Amazon EC2](#).
- Il proprietario di una macchina può assegnare l'istanza di una macchina Amazon a un Amazon VPC.

Per ulteriori informazioni sulla creazione di un Amazon VPC, vedere la documentazione di Amazon Web Services.

Utilizzo dei bilanciamenti del carico flessibili per Amazon Web Services

I bilanciamenti del carico flessibili distribuiscono il traffico delle applicazioni in entrata tra istanze di Amazon Web Services. Il bilanciamento del carico di Amazon consente di ottenere prestazioni migliori e un sistema di tolleranza agli errori avanzato.

Amazon rende il bilanciamento del carico flessibile disponibile per le macchine di cui viene eseguito il provisioning tramite blueprint Amazon EC2.

Il bilanciamento del carico flessibile deve essere disponibile in Amazon Web Services, Amazon Virtual Private Network e nella posizione del provisioning. Se ad esempio un bilanciamento del carico è disponibile in us-east1c e la posizione di una macchina è us-east1b, la macchina non può utilizzare il bilanciamento del carico disponibile.

vRealize Automation non crea, gestisce o monitora i bilanciamenti del carico flessibili.

Per informazioni sulla creazione di bilanciamenti del carico flessibili Amazon utilizzando la Amazon Web Services Management Console, vedere la documentazione di Amazon Web Services.

Utilizzo di indirizzi IP flessibili per Amazon Web Services

L'uso di un indirizzo IP flessibile consente di eseguire rapidamente il failover su un'altra macchina in un ambiente cloud dinamico Amazon Web Services. In vRealize Automation, l'indirizzo IP flessibile è disponibile a tutti i gruppi di business che hanno diritti sulla regione.

Un amministratore può allocare indirizzi IP flessibili per l'account Amazon Web Services utilizzando AWS Management Console. Ci sono due gruppi di indirizzi IP flessibili in ogni data regione, un intervallo viene allocato per le istanze non Amazon VPC e un altro intervallo per le istanze Amazon VPC. Se si allocano indirizzi solo in una regione non Amazon VPC, gli indirizzi non sono disponibili in una Amazon VPC. È vero anche il contrario. Se si allocano indirizzi solo in una Amazon VPC, gli indirizzi non sono disponibili in una regione non Amazon VPC.

L'indirizzo IP flessibile viene associato al proprio account Amazon Web Services, non a una determinata macchina, ma può essere utilizzato da una sola macchina alla volta. L'indirizzo resta associato all'account di Amazon Web Services finché non si sceglie di rilasciarlo. È possibile rilasciarlo per associarlo a una specifica istanza di macchina.

Un architetto IaaS può aggiungere una proprietà personalizzata a un blueprint per assegnare un indirizzo IP flessibile alle macchine durante il provisioning. I proprietari e gli amministratori delle macchine possono visualizzare gli indirizzi IP flessibili assegnati alle macchine, mentre i proprietari o gli amministratori delle macchine che dispongono dei diritti per la modifica delle macchine possono assegnare indirizzi IP flessibili dopo il provisioning. Tuttavia, se l'indirizzo è già associato all'istanza di una macchina e l'istanza fa parte della distribuzione Amazon Virtual Private Cloud, Amazon non assegna l'indirizzo.

Per ulteriori informazioni sulla creazione e l'uso degli indirizzi IP flessibili di Amazon, consultare la documentazione di Amazon Web Services.

Utilizzo di EBS per Amazon Web Services

Amazon Elastic Block Storage (EBS) fornisce volumi di storage a livello di blocchi da utilizzare con istanze di macchine Amazon e Amazon Virtual Private Cloud. Un volume di storage può essere conservato nell'ambiente cloud di Amazon Web Services anche dopo la fine della vita dell'istanza della macchina Amazon a esso associata.

Quando si utilizza un volume EBS di Amazon insieme a vRealize Automation, è necessario considerare gli aspetti seguenti:

- Non è possibile allegare un volume EBS esistente quando si esegue il provisioning dell'istanza di una macchina. Se tuttavia si crea un nuovo volume e si richiede più di una macchina in una volta, il volume viene creato e allegato a ogni istanza. Ad esempio, se si crea un volume chiamato volume_1 e si richiedono tre macchine, viene creato un volume per ogni macchina. Tre volumi chiamati volume_1 vengono creati e allegati a ogni macchina. Ogni volume ha un ID di volume unico. Tutti i volumi hanno le stesse dimensioni e si trovano nella stessa posizione.
- Il volume deve essere dello stesso sistema operativo e deve trovarsi nella stessa posizione della macchina alla quale lo si allega.
- vRealize Automation non gestisce il volume primario di un'istanza basata su EBS.

Per ulteriori informazioni sullo storage EBS di Amazon e per i dettagli relativi a come abilitarlo utilizzando Amazon Web Services Management Console, vedere la documentazione di Amazon Web Services.

Configurazione della connettività VPC da rete ad Amazon per un ambiente di prototipazione

In qualità di professionista IT con il compito di configurare un ambiente per valutare vRealize Automation, si desidera configurare temporaneamente la connettività VPC da rete ad Amazon per il supporto della funzionalità del Software vRealize Automation.

La connettività VPC da rete ad Amazon è richiesta solo se si desidera utilizzare l'agente guest per personalizzare macchine di cui è stato eseguito il provisioning o se si desidera includere componenti Software nei blueprint. In un ambiente di produzione, si procederebbe alla configurazione di questa connettività tramite Amazon Web Services, ma poiché si sta lavorando in un ambiente di prototipazione, si desidera configurare una connettività di rete Amazon VPC temporanea. Stabilire il tunnel SSH e quindi configurare una prenotazione Amazon in vRealize Automation da instradare attraverso il tunnel.

Prerequisiti

- Creare un gruppo di sicurezza Amazon Web Services chiamato TunnelGroup e configurarlo per consentire l'accesso alla porta 22.
- Creare o identificare una macchina CentOS nel gruppo di sicurezza TunnelGroup di Amazon Web Services e osservare le configurazioni seguenti:
 - Credenziali utente amministrative, ad esempio *root*.
 - Indirizzo IP pubblico.
 - Indirizzo IP privato.
- Creare o identificare una macchina CentOS sulla stessa rete locale della propria installazione di vRealize Automation.

- Installare il server OpenSSH SSHD su entrambe le macchine tunnel.

Procedura

- 1 Accedere alla macchina tunnel Amazon Web Services come utente root o simile.
- 2 Disattivare iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Modificare /etc/ssh/sshd_config in modo da abilitare AllowTCPForwarding e GatewayPorts.
- 4 Riavviare il servizio.

```
/etc/init.d/sshd restart
```

- 5 Accedere come utente root alla macchina CentOS sulla stessa rete locale dell'installazione di vRealize Automation.
- 6 Richiamare il tunnel SSH dalla macchina della rete locale alla macchina tunnel Amazon Web Services.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \

-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

Si è configurato l'inoltro della porta per consentire alla macchina tunnel Amazon Web Services di accedere alle risorse vRealize Automation, ma il tunnel SSH non funziona fino a quando non si configura una prenotazione Amazon da instradare nel tunnel.

Operazioni successive

- 1 Installare l'agente bootstrap software e l'agente guest su una macchina di riferimento Windows o Linux per creare un'immagine della macchina Amazon che gli architetti IaaS possono utilizzare per creare i blueprint. Vedere [Preparazione per il provisioning Software](#).
- 2 Configurare la prenotazione in vRealize Automation da instradare nel tunnel SSH. Vedere [Scenario: creazione di una prenotazione Amazon per un ambiente di prototipazione](#).

Preparazione delle funzionalità di rete e sicurezza di Red Hat OpenStack

vRealize Automation supporta diverse funzionalità in OpenStack, inclusi i gruppi di sicurezza e gli indirizzi IP mobili. È importante apprendere come queste funzionalità interoperano con vRealize Automation per poterle configurare nel proprio ambiente.

Utilizzo dei gruppi di sicurezza di OpenStack

I gruppi di sicurezza consentono di specificare regole per controllare il traffico di rete su porte specifiche.

Quando si richiede una macchina, è possibile specificare i gruppi di sicurezza. È inoltre possibile specificare un gruppo di sicurezza esistente o su richiesta di NSX nella tela di progettazione.

I gruppi di sicurezza vengono importati durante la raccolta dati.

Ogni regione disponibile richiede almeno un gruppo di sicurezza specificato. Quando si crea una prenotazione, vengono elencati i gruppi di sicurezza disponibili in quella regione. Ogni regione include almeno il gruppo di sicurezza predefinito.

I gruppi di sicurezza aggiuntivi devono essere gestiti nella risorsa di origine. Per ulteriori informazioni sulla gestione dei gruppi di sicurezza per le varie macchine, vedere la documentazione di OpenStack.

Utilizzo degli indirizzi IP mobili con OpenStack

È possibile assegnare indirizzi IP mobili a un'istanza virtuale in esecuzione in OpenStack.

Per abilitare l'assegnazione di indirizzi IP mobili, è necessario configurare l'IP forwarding e creare un pool di IP mobili in Red Hat OpenStack. Per ulteriori informazioni, vedere la documentazione di Red Hat OpenStack.

È necessario autorizzare i proprietari delle macchine alle azioni Associa IP mobile e Annulla associazione IP mobile. Dalle reti esterne collegate alla macchina gli utenti autorizzati possono quindi selezionare un indirizzo disponibile dal pool di indirizzi IP mobili e associarlo a una macchina fornita in provisioning. Dopo aver associato a una macchina un indirizzo IP mobile, un utente di vRealize Automation può selezionare un'opzione di Annulla associazione IP mobile per visualizzare gli indirizzi IP mobili correntemente assegnati e annullare l'associazione di un indirizzo con una macchina.

Preparazione dell'ambiente di SCVMM

Prima di iniziare a creare modelli di SCVMM e profili hardware da utilizzare nel provisioning delle macchine di vRealize Automation, è necessario conoscere le limitazioni imposte ai nomi dei modelli e dei profili hardware e configurare le impostazioni di rete e storage di SCVMM.

Per informazioni correlate alla preparazione dell'ambiente, consultare le informazioni sui requisiti di SCVMM in *Installazione di vRealize Automation*.

Per informazioni correlate al provisioning delle macchine, vedere [Creazione di un endpoint Hyper-V \(SCVMM\)](#).

vRealize Automation non supporta un ambiente di distribuzione che utilizza una configurazione di cloud privati SCVMM. Al momento vRealize Automation non può raccogliere da, allocare a o eseguire il provisioning in base ai cloud privati SCVMM.

Denominazione di modelli e profili hardware

Le convenzioni di denominazione utilizzate da SCVMM e vRealize Automation per i modelli e i profili hardware non consentono di utilizzare nomi di modelli o profili hardware che iniziano con le parole `temporary` e `profile`. Ad esempio, i termini seguenti vengono ignorati durante la raccolta dati:

- `TemporaryTemplate`
- `Temporary Template`
- `TemporaryProfile`
- `Temporary Profile`
- `Profile`

Configurazione di rete richiesta per i cluster di SCVMM

I cluster di SCVMM espongono solo reti virtuali a vRealize Automation, pertanto è necessario avere una relazione 1:1 tra le reti virtuali e logiche. Utilizzando la console di SCVMM, mappare ciascuna rete logica a una rete virtuale e configurare il cluster di SCVMM per accedere alle macchine attraverso la rete virtuale.

Configurazione di storage richiesta per i cluster di SCVMM

Sui cluster Hyper-V di SCVMM, vRealize Automation raccoglie dati ed esegue il provisioning solo su volumi condivisi. Utilizzando la console di SCVMM, configurare i cluster per utilizzare volumi di risorse condivise per lo storage.

Configurazione di storage richiesta per gli host di SCVMM autonomi

Per gli host di SCVMM autonomi, vRealize Automation raccoglie dati ed esegue il provisioning sul percorso predefinito della macchina virtuale. Utilizzando la console di SCVMM, configurare i percorsi predefiniti della macchina virtuale per gli host autonomi.

Configurazione della connettività VPC da rete ad Azure

È necessario configurare la connettività da rete ad Azure se si desidera utilizzare i componenti software nei Blueprint Azure.

Prerequisiti

- Creare un gruppo di sicurezza Azure chiamato `TunnelGroup` e configurarlo per consentire l'accesso alla porta 22.
- Creare o identificare una macchina, ad esempio una macchina CentOS, nel gruppo di sicurezza `TunnelGroup` di Azure e osservare le configurazioni seguenti:
 - Credenziali utente amministrative, ad esempio `root`.
 - Indirizzo IP pubblico.
 - Indirizzo IP privato.

- Creare o identificare una macchina CentOS sulla stessa rete locale della propria installazione di vRealize Automation.
- Installare il server OpenSSH SSHD su entrambe le macchine tunnel.

Procedura

- 1 Accedere alla macchina tunnel Azure come utente root o simile.
- 2 Disattivare iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

- 3 Modificare /etc/ssh/sshd_config in modo da abilitare AllowTCPForwarding e GatewayPorts.
- 4 Riavviare il servizio.

```
/etc/init.d/sshd restart
```

- 5 Accedere come utente root alla macchina CentOS sulla stessa rete locale dell'installazione di vRealize Automation.
- 6 Richiamare il tunnel SSH dalla macchina della rete locale alla macchina tunnel Azure.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Azure tunnel machine@Public IP Address of Azure tunnel machine
```

Si è configurato l'inoltro della porta per consentire alla macchina tunnel Azure di accedere alle risorse di vRealize Automation, ma il tunnel SSH non funziona fino a quando non si configura una prenotazione Azure da instradare nel tunnel.

Operazioni successive

- 1 Installare l'agente bootstrap software e l'agente guest su una macchina di riferimento Windows o Linux per creare un'immagine della macchina Azure che gli architetti IaaS possono utilizzare per creare i Blueprint. Vedere [Preparazione per il provisioning Software](#).
- 2 Configurare la prenotazione Azure in vRealize Automation da instradare nel tunnel SSH. Vedere [Creazione di una prenotazione per Microsoft Azure](#).

Preparazione per il provisioning delle macchine

In base all'ambiente e al metodo di provisioning della macchina, potrebbe essere necessario configurare elementi al di fuori di vRealize Automation.

Potrebbe ad esempio essere necessario configurare modelli o immagini di macchine.

Potrebbe inoltre essere necessario configurare le impostazioni di NSX o eseguire workflow di vRealize Orchestrator.

Per informazioni relative all'indicazione delle porte durante la preparazione per il provisioning delle macchine, vedere il file PDF *Architettura di riferimento* nella [documentazione del prodotto di vRealize Automation](#).

Scelta del metodo di provisioning delle macchine da preparare

Per la maggior parte dei metodi di provisioning, alcuni elementi devono essere preparati all'esterno di vRealize Automation.

Tabella 1-5. Scelta del metodo di provisioning delle macchine da preparare

Scenario	Endpoint supportato	Supporto di agenti	Metodo di provisioning	Preparazioni pre-provisioning
Configurare vRealize Automation in modo che esegua script Visual Basic personalizzati come passaggi aggiuntivi nel ciclo di vita della macchina, prima o dopo il provisioning. Ad esempio è possibile utilizzare uno script pre-provisioning per generare certificati o token di sicurezza prima del provisioning, e quindi uno script post-provisioning per utilizzare i certificati e i token dopo il provisioning della macchina.	È possibile eseguire script Visual Basic con qualsiasi endpoint supportato, ad eccezione di Amazon Web Services.	Dipende dal metodo di provisioning scelto.	Supportato come passaggio aggiuntivo in qualsiasi metodo di provisioning, tuttavia non è possibile eseguire script Visual Basic con macchine Amazon Web Services.	Elenco di controllo per l'esecuzione di script Visual Basic durante il provisioning
Eseguire il provisioning di blueprint di applicazioni per l'automazione dell'installazione, della configurazione e della gestione del ciclo di vita di middleware e componenti per la distribuzione delle applicazioni, come schemi Oracle, MySQL, WAR e di database.	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon Web Services 	<ul style="list-style-type: none"> ■ (Obbligatorio) Agente guest ■ (Obbligatorio) Agente di avvio automatico software e agente guest 	<ul style="list-style-type: none"> ■ Clona ■ Clone (per vCloud Air o vCloud Director) ■ Clone collegato ■ Immagine macchina Amazon 	Per utilizzare componenti Software nei blueprint, preparare un metodo di provisioning che supporti l'agente guest e l'agente di avvio automatico di Software. Per ulteriori informazioni sulla preparazione per Software, vedere Preparazione per il provisioning Software .

Tabella 1-5. Scelta del metodo di provisioning delle macchine da preparare (continua)

Scenario	Endpoint supportato	Supporto di agenti	Metodo di provisioning	Preparazioni pre-provisioning
Dopo il provisioning, è possibile utilizzare l'agente guest per personalizzare ulteriormente le macchine.	Tutti gli endpoint virtuali e Amazon Web Services.	<ul style="list-style-type: none"> ■ (Obbligatorio) Agente guest ■ (Facoltativo) Agente di avvio automatico software e agente guest 	Supportato per tutti i metodi di provisioning ad eccezione di quello basato su immagini delle macchine virtuali.	Per avere la possibilità di personalizzare le macchine dopo il provisioning, selezionare un metodo di provisioning che supporti l'agente guest.
Esegue il provisioning di macchine senza sistema operativo guest. È possibile installare un sistema operativo dopo il provisioning.	Tutti gli endpoint di macchine virtuali.	Non supportato	Di base	Non sono necessarie preparazioni pre-provisioning all'esterno di vRealize Automation.
Esegue il provisioning di una copia dalle dimensioni ottimizzate di una macchina virtuale chiamata clone collegato. I cloni collegati sono basati su uno snapshot di una VM e utilizzano una catena di dischi delta per tenere traccia delle differenze rispetto a una macchina padre.	vSphere	<ul style="list-style-type: none"> ■ (Facoltativo) Agente guest ■ (Facoltativo) Agente di avvio automatico software e agente guest 	Clone collegato	<p>Deve essere presente una macchina virtuale vSphere.</p> <p>Per supportare Software, installare l'agente guest e l'agente di avvio automatico del software sulla macchina da clonare.</p> <p>Prima di eseguire il provisioning delle macchine virtuali dei cloni collegati, spegnere lo snapshot della macchina virtuale.</p>
Esegue il provisioning di una copia dalle dimensioni ottimizzate di una macchina virtuale utilizzando la tecnologia Net App FlexClone.	vSphere	(Facoltativo) Agente guest	NetApp FlexClone	Vedere Elenco di controllo per la preparazione al provisioning tramite clonazione .
Esegue il provisioning di macchine clonando da un oggetto modello creato da una macchina Windows o Linux esistente, chiamata macchina di riferimento, e un oggetto di personalizzazione.	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ (Facoltativo) Agente guest ■ (Facoltativo solo per vSphere) Agente di avvio automatico software e agente guest 	Clona	<p>Vedere Elenco di controllo per la preparazione al provisioning tramite clonazione.</p> <p>Per supportare Software, installare l'agente guest e l'agente di avvio automatico del software sulla macchina vSphere da clonare.</p>

Tabella 1-5. Scelta del metodo di provisioning delle macchine da preparare (continua)

Scenario	Endpoint supportato	Supporto di agenti	Metodo di provisioning	Preparazioni pre-provisioning
Eseguire il provisioning di macchine vCloud Air o vCloud Director mediante clonazione da un modello o da un oggetto di personalizzazione.	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ (Facoltativo) Agente guest ■ (Facoltativo) Agente di avvio automatico software e agente guest 	Clonazione di vCloud Air o vCloud Director	<p>Vedere Preparazione per il provisioning di vCloud Air e vCloud Director.</p> <p>Per supportare Software, creare un modello contenente l'agente guest e l'agente di avvio automatico del software. Per vCloud Air, configurare la connettività di rete tra gli ambienti vRealize Automation e vCloud Air.</p>
Esegue il provisioning di una macchina effettuando l'avvio da un'immagine ISO, utilizzando un file di configurazione kickstart o autoYaSt e un'immagine di distribuzione Linux per installare il sistema operativo sulla macchina.	<ul style="list-style-type: none"> ■ Tutti gli endpoint virtuali ■ Red Hat OpenStack 	L'agente guest è installato come parte delle istruzioni di preparazione.	Linux Kickstart	Preparazione per il provisioning Linux Kickstart
Esegue il provisioning di una macchina e trasferisce il controllo a una sequenza di attività SCCM per eseguire l'avvio da un'immagine ISO, distribuisce un sistema operativo Windows e installa l'agente guest di vRealize Automation.	Tutti gli endpoint di macchine virtuali.	L'agente guest è installato come parte delle istruzioni di preparazione.	SCCM	Preparazione per il provisioning SCCM
Esegue il provisioning di una macchina effettuando l'avvio in un ambiente WinPE e installando un sistema operativo utilizzando l'immagine in formato WIM (Windows Imaging File Format) di una macchina di riferimento Windows esistente.	<ul style="list-style-type: none"> ■ Tutti gli endpoint virtuali ■ Red Hat OpenStack 	L'agente guest è obbligatorio. Quando si crea l'immagine WinPE è necessario specificare manualmente l'agente guest.	WIM	Preparazione per il provisioning di WIM

Tabella 1-5. Scelta del metodo di provisioning delle macchine da preparare (continua)

Scenario	Endpoint supportato	Supporto di agenti	Metodo di provisioning	Preparazioni pre-provisioning
Avvia un'istanza dall'immagine di una macchina virtuale.	Red Hat OpenStack	Non supportato	Immagine di macchina virtuale	Vedere Preparazione per il provisioning dell'immagine delle macchine virtuali .
Avvia un'istanza da un'immagine di macchina Amazon.	Amazon Web Services	<ul style="list-style-type: none"> ■ (Facoltativo) Agente guest ■ (Facoltativo) Agente di avvio automatico software e agente guest 	Immagine macchina Amazon	<p>Associare le immagini di macchine Amazon e i tipi di istanze al proprio account Amazon Web Services.</p> <p>Per supportare Software, creare un'immagine di macchina Amazon contenente l'agente guest e l'agente di avvio automatico del software, quindi configurare la connettività da rete a VPC tra gli ambienti Amazon Web Services e vRealize Automation.</p>

Elenco di controllo per l'esecuzione di script Visual Basic durante il provisioning

È possibile configurare vRealize Automation per eseguire script Visual Basic personalizzati come passaggi aggiuntivi nel ciclo di vita delle macchine, prima o dopo il provisioning di una macchina. Ad esempio è possibile utilizzare uno script pre-provisioning per generare certificati o token di sicurezza prima del provisioning, e quindi uno script post-provisioning per utilizzare i certificati e i token dopo il provisioning della macchina. È possibile eseguire script Visual Basic con qualsiasi metodo di provisioning, ma non è possibile utilizzare script Visual Basic con macchine AWS di Amazon.

Tabella 1-6. Elenco di controllo per l'esecuzione di script Visual Basic durante il provisioning

Attività	Posizione	Dettagli
<input type="checkbox"/> Installare e configurare l'agente EPI per gli script Visual Basic.	Di solito l'host del servizio di gestione	Vedere <i>Installazione di vRealize Automation</i> .
<input type="checkbox"/> Creare i propri script Visual Basic.	Macchina su cui è installato l'agente EPI	<p>vRealize Automation include lo script Visual Basic di esempio <code>PrePostProvisioningExample.vbs</code> situato nella directory <code>Scripts</code> della directory d'installazione dell'agente EPI. Lo script è articolato in un'intestazione in cui vengono caricati tutti gli argomenti in un dizionario, un corpo in cui è possibile includere le proprie funzioni e una sezione finale per la restituzione delle proprietà personalizzate aggiornate a vRealize Automation.</p> <p>Quando si esegue uno script Visual Basic, l'agente EPI passa allo script tutte le proprietà personalizzate delle macchine come argomenti. Per restituire a vRealize Automation i valori delle proprietà aggiornati, inserire queste proprietà in un dizionario e chiamare una funzione fornita da vRealize Automation.</p>
<input type="checkbox"/> Raccogliere le informazioni necessarie da includere negli script nei blueprint.	<p>Catturare le informazioni e trasferirle agli architetti dell'infrastruttura</p> <p>Nota un amministratore di struttura può creare un gruppo di proprietà utilizzando i set di proprietà <code>ExternalPreProvisioningVbScript</code> ed <code>ExternalPostProvisioningVbScript</code> per fornire questa informazioni richiesta. In questo modo sarà più semplice per gli architetti dei blueprint includere correttamente queste informazioni nei propri blueprint.</p>	<ul style="list-style-type: none"> ■ Il percorso completo dello script Visual Basic, incluso il nome file e l'estensione. Ad esempio, <code>%SystemDrive%\Programmi (x86)\VMware\VCAC_Agents\EPI_Agents\Scripts\SendEmail.vbs</code>. ■ Per eseguire uno script prima del provisioning, richiedere agli architetti dell'infrastruttura di specificare il percorso completo dello script come valore della proprietà personalizzata <code>ExternalPreProvisioningVbScript</code>. Per eseguire uno script dopo il provisioning, essi dovranno utilizzare la proprietà personalizzata <code>ExternalPostProvisioningVbScript</code>.

Utilizzo dell'agente guest di vRealize Automation nel provisioning

È possibile installare l'agente guest sulle macchine di riferimento per personalizzare ulteriormente una macchina in seguito alla distribuzione. È possibile utilizzare le proprietà personalizzate dell'agente guest riservate per effettuare personalizzazioni di base quali l'aggiunta e la

formattazione di dischi, oppure è possibile creare i propri script personalizzati per l'agente guest da eseguire all'interno del sistema operativo guest di una macchina con provisioning effettuato.

Una volta completata la distribuzione ed eseguita la specifica di personalizzazione (se ne è stata fornita una), l'agente guest crea un file XML contenente tutte le proprietà personalizzate della macchina distribuita `c:\VRMGuestAgent\site\workitem.xml`, completa tutte le attività a esso assegnate con le proprietà personalizzate dell'agente guest e si auto-elimina dalla macchina fornita in provisioning.

È possibile scrivere i propri script personalizzati da eseguire su macchine distribuite e utilizzare le proprietà personalizzate sul blueprint della macchina per specificare la posizione di tali script nell'ordine in cui si desidera eseguirli. Inoltre è possibile utilizzare proprietà personalizzate blueprint della macchina per passare come parametri i valori delle proprietà personalizzate agli script.

Ad esempio, si può usare l'agente guest per apportare le seguenti personalizzazioni alle macchine distribuite:

- Cambiare l'indirizzo IP
- Aggiungere o formattare unità
- Eseguire script di sicurezza
- Inizializzare un altro agente, ad esempio Puppet o Chef

È inoltre possibile specificare una stringa codificata come proprietà personalizzata nell'argomento di una riga di comando. In questo modo vengono archiviate le informazioni codificate che l'agente guest può decrittografare e comprendere come argomento valido della riga di comando.

Nota L'agente guest di Linux assegna IP statici durante le azioni di creazione e clonazione del provisioning di Linux Kickstart e PXE, in relazione alle proprietà personalizzate di vRealize Automation negli elementi di lavoro. Quando assegna IP statici, l'agente guest non è in grado di contenere il nuovo schema di denominazione uniforme della rete, come in Ubuntu 16.x.

I propri script personalizzati non devono essere necessariamente installati localmente sulla macchina. Se la macchina fornita in provisioning ha un accesso di rete alla posizione degli script, l'agente guest potrà accedervi ed eseguire gli script. Ciò consente di ridurre i costi di manutenzione perché è possibile aggiornare gli script senza dover ricreare tutti i modelli.

È possibile configurare le impostazioni di sicurezza specificando le informazioni in una prenotazione, in un blueprint o in uno script dell'agente guest. Se le macchine richiedono un agente guest, aggiungere una regola di sicurezza alla prenotazione o al blueprint.

Se si sceglie di installare l'agente guest per eseguire script personalizzati sulle macchine di cui è stato eseguito il provisioning, i blueprint devono includere proprietà personalizzate di agente guest appropriate. Ad esempio, se si intende installare l'agente guest su un modello per la clonazione, creare uno script personalizzato che cambia l'indirizzo IP della macchina fornita in provisioning e collocare lo script in una posizione condivisa, è necessario includere una serie di proprietà personalizzate nel blueprint.

Tabella 1-7. Proprietà personalizzate per cambiare l'indirizzo IP di una macchina fornita in provisioning con un agente guest

Proprietà personalizzata	Descrizione
VirtualMachine.Admin.UseGuestAgent	Impostare su true per inizializzare l'agente guest quando la macchina fornita in provisioning viene avviata.
VirtualMachine.Customize.WaitComplete	Impostare su True per evitare che il workflow di provisioning invii gli elementi di lavoro all'agente guest prima che siano state completate tutte le personalizzazioni. Impostare su False per consentire la creazione degli elementi di lavoro prima del completamento della personalizzazione.

Tabella 1-7. Proprietà personalizzate per cambiare l'indirizzo IP di una macchina fornita in provisioning con un agente guest (continua)

Proprietà personalizzata	Descrizione
VirtualMachine.SoftwareN.ScriptPath	<p>Specifica il percorso completo dello script d'installazione di un'applicazione. Il percorso deve essere un percorso assoluto valido, così come visto dal sistema operativo guest, e deve includere il nome del file dello script.</p> <p>È possibile passare i valori delle proprietà personalizzate come parametri allo script inserendo <code>{CustomPropertyName}</code> nella stringa del percorso. Se ad esempio si ha una proprietà personalizzata chiamata <code>ActivationKey</code> il cui valore è 1234, il percorso dello script è <code>D:\InstallApp.bat -key {ActivationKey}</code>. L'agente guest esegue il comando <code>D:\InstallApp.bat -key 1234</code>. Il file dello script può quindi essere programmato per accettare e utilizzare questo valore.</p> <p>Immettere <code>{Owner}</code> per passare il nome del proprietario della macchina allo script.</p> <p>È anche possibile passare i valori delle proprietà personalizzate come parametri allo script inserendo <code>{YourCustomProperty}</code> nella stringa del percorso. Ad esempio, l'immissione del valore <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat</code> esegue lo script <code>changeIP.bat</code> da una posizione condivisa, tuttavia l'immissione del valore <code>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</code> esegue lo script <code>changeIP</code>, ma passa anche il valore della proprietà <code>VirtualMachine.Network0.Address</code> allo script come parametro.</p>
VirtualMachine.ScriptPath.Decrypt	<p>Consente a vRealize Automation di ottenere una stringa crittografata che viene passata come una dichiarazione della proprietà personalizzata <code>VirtualMachine.SoftwareN.ScriptPath</code> formattata in precedenza alla riga di comando guest.</p> <p>È possibile fornire una stringa crittografata, come ad esempio la password, come proprietà personalizzata in un argomento della riga di comando. Ciò consente di memorizzare le informazioni crittografate che l'agente guest può decrittografare e comprendere come argomento della linea di comando valido. Ad esempio, la stringa della proprietà personalizzata <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat password</code> non è sicura in quanto contiene effettivamente una password.</p>

Tabella 1-7. Proprietà personalizzate per cambiare l'indirizzo IP di una macchina fornita in provisioning con un agente guest (continua)

Proprietà personalizzata	Descrizione
	<p>Per crittografare la password, è possibile creare una proprietà personalizzata vRealize Automation, ad esempio <code>MyPassword = password</code>, e consentire la crittografia selezionando la casella di testo disponibile. L'agente guest decrittografa la voce [MyPassword] con il valore nella proprietà personalizzata <code>MyPassword</code> ed esegue lo script come <code>c:\dosomething.bat password</code>.</p> <ul style="list-style-type: none"> ■ Creare la proprietà personalizzata <code>MyPassword = password</code> dove <code>password</code> è il valore della password effettiva. Abilitare la crittografia selezionando la casella di controllo disponibile. ■ Impostare la proprietà personalizzata <code>VirtualMachine.ScriptPath.Decrypt</code> come <code>VirtualMachine.ScriptPath.Decrypt = true</code>. ■ Impostare la proprietà personalizzata <code>VirtualMachine.Software0.ScriptPath</code> come <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</code>. <p>Se si imposta <code>VirtualMachine.ScriptPath.Decrypt</code> su <code>False</code> o non si crea la proprietà personalizzata <code>VirtualMachine.ScriptPath.Decrypt</code>, la stringa all'interno delle parentesi quadre ([e]) non viene decrittografata.</p>

Per ulteriori informazioni sulle proprietà personalizzate che è possibile utilizzare con l'agente guest, vedere *Guida di riferimento alle proprietà personalizzate*.

Configurare l'agente guest in modo che consideri attendibile un server.

Installare il file PEM della chiave pubblica per un host del servizio di gestione di vRealize Automation nella cartella dell'agente guest corretta, è l'approccio più sicuro per configurare l'agente guest in modo che consideri attendibile un determinato server.

Per permettere di considerare un server attendibile, individuare la cartella dell'agente guest in ogni modello per il file PEM `cert.pem` per l'host del servizio di gestione:

- Cartella dell'agente guest di Windows su ciascun modello che utilizza gugent

```
C:\VRMGuestAgent\cert.pem
```

- Cartella dell'agente guest di Linux su ciascun modello che utilizza gugent

```
/usr/share/gugent/cert.pem
```

Se il file `cert.pem` non viene salvato in questo percorso, la macchina di riferimento del modello non può utilizzare l'agente guest. Ad esempio, se si tenta di raccogliere informazioni sulla chiave pubblica dopo che la VM viene avviata modificando gli script, le condizioni di sicurezza non saranno rispettate.

A seconda dell'ambiente configurato, potrebbe essere opportuno valutare altri aspetti:

- Per le installazioni WIM, è necessario aggiungere i contenuti del file PEM della chiave pubblica alla console eseguibile e all'interfaccia utente. Il flag della console è **/cert filename**.
- Per le installazioni Kickstart di RedHat, è necessario tagliare e incollare la chiave pubblica nel file di esempio, altrimenti non risulterà possibile eseguire l'agente guest.
- Per le installazioni SCCM, è necessario che il file `cert.pem` si trovi nella cartella `VRMGuestAgent`.
- Per le installazioni Linux vSphere, è necessario che il file `cert.pem` si trovi nella cartella `/usr/share/gugent`.

Nota Facoltativamente, è possibile installare software e agenti guest insieme scaricando il seguente script da <https://APPLIANCE/software/index.html>. Lo script consente di gestire l'accettazione delle impronte digitali del certificato SSL durante la creazione dei modelli.

- Linux
`prepare_vra_template.sh`
- Windows
`prepare_vra_template.ps1`

Se software e agente guest vengono installati insieme, non è necessario seguire le istruzioni in [Installazione dell'agente guest su una macchina di riferimento Linux](#) o in [Installazione dell'agente guest su una macchina di riferimento Windows](#).

Come ottenere il file `cert.pem` dall'host del servizio di gestione

- 1 Nell'host del servizio di gestione, passare a Strumenti di amministrazione e aprire Gestione Internet Information Services (IIS).
- 2 Nella struttura a sinistra, evidenziare l'host del servizio di gestione.
- 3 Sulla destra, aprire Certificati server.
- 4 Cercare il certificato in cui **Emesso per** è VMware vRA e **Emesso da** sia VMware vRA.
- 5 Fare clic con il pulsante destro del mouse sul certificato ed esportarlo.
- 6 Il certificato salvato sarà in formato PFX. Per convertirlo in PEM, utilizzare OpenSSL dalla riga di comando.

```
openssl pkcs12 -in filename.pfx -out cert.pem -nodes
```

Installazione dell'agente guest su una macchina di riferimento Linux

Installare l'agente guest di Linux sulle macchine di riferimento per personalizzare ulteriormente le macchine dopo la distribuzione.

Prerequisiti

- Identificare o creare la macchina di riferimento.

- I file dell'agente guest scaricato contengono i pacchetti sia nel formato `tar.gz` che nel formato RPM. Se il sistema operativo non può installare file `tar.gz` o RPM, utilizzare uno strumento di conversione per convertire i file d'installazione nel formato di pacchetto preferito.
- Stabilire un rapporto di attendibilità sicura tra l'agente guest e la macchina del servizio di gestione. Vedere [Configurare l'agente guest in modo che consideri attendibile un server..](#)

Procedura

- 1 Aprire la pagina della console di gestione dell'appliance vRealize Automation.

Ad esempio: `https://va-hostname.domain.com`.

- 2 Fare clic sulla pagina **Guest and software agents** (Agenti guest e software) nella sezione dedicata all'installazione dei componenti di vRealize Automation della pagina.

Ad esempio: `https://va-hostname.domain.com/software/index.html`.

Si apre la pagina **Guest and Software Agent Installers** (Programmi di installazione degli agenti guest e software), con i link ai download disponibili.

- 3 Fare clic su **Linux guest agent packages** (Pacchetti agenti guest Linux) nella sezione dedicata ai programmi di installazione degli agenti guest della pagina per scaricare e salvare il file `LinuxGuestAgentPkgs.zip`.

- 4 Decomprimere il file `LinuxGuestAgentPkgs.zip` scaricato per creare la cartella `VraLinuxGuestAgent`.

- 5 Installare il pacchetto dell'agente guest corrispondente al sistema operativo guest distribuito durante il provisioning.

- a Andare alla sottodirectory `VraLinuxGuestAgent` che corrisponde al sistema operativo guest da distribuire durante il provisioning, ad esempio `rhel32`.
- b Individuare il formato di pacchetto preferito o convertire un pacchetto nel formato preferito.
- c Installare il pacchetto dell'agente guest su una macchina di riferimento.

Ad esempio, per installare i file dal pacchetto RPM, eseguire `rpm -i gagent-gugent-7.1.0-4201531.i386.rpm`.

- 6 Configurare l'agente guest per la comunicazione con il servizio di gestione eseguendo `installgugent.sh Manager_Service_Hostname_fdqn:portnumber ssl platform`.

Il numero di porta predefinito per il servizio di gestione è 443. I valori della piattaforma accettati sono `ec2`, `vcd`, `vca` e `vsphere`.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	<p>Specificare il nome di dominio completo e la porta relativi al bilanciamento del carico del servizio di gestione. Ad esempio:</p> <pre>cd /usr/share/gugent ./installgugent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
Senza bilanciamento del carico	<p>Specificare il nome di dominio completo e la porta relativi alla macchina del servizio di gestione. Ad esempio:</p> <pre>cd /usr/share/gugent ./installgugent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 7 Se le macchine distribuite non sono già configurate per considerare attendibile il certificato SSL del servizio di gestione, è necessario installare il file `cert.pem` sulla macchina di riferimento per stabilire l'attendibilità.
- Per l'approccio più sicuro, ottenere il certificato `cert.pem` e installare manualmente il file sulla macchina di riferimento.
 - Per un approccio più comodo, è possibile connettersi al bilanciamento del carico del servizio di gestione o alla macchina del servizio di gestione e scaricare il certificato `cert.pem`.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	<p>In qualità di utente root sulla macchina di riferimento, eseguire il comando seguente:</p> <pre>echo openssl s_client -connect manager_service_load_balancer.mycompany.com:443 sed -ne '/- BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>
Senza bilanciamento del carico	<p>In qualità di utente root sulla macchina di riferimento, eseguire il comando seguente:</p> <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 8 Se si sta installando l'agente guest su un sistema operativo Ubuntu, creare collegamenti simbolici per oggetti condivisi eseguendo uno dei seguenti set di comandi.

Opzione	Descrizione
Sistemi a 64 bit	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
Sistemi a 32 bit	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

Operazioni successive

Convertire la macchina di riferimento in un modello per la clonazione, un'immagine di macchina Amazon o uno snapshot che gli architetti di IaaS possono utilizzare quando creano blueprint.

Installazione dell'agente guest su una macchina di riferimento Windows

Installare l'agente guest Windows di vRealize Automation su una macchina di riferimento Windows da eseguire come servizio Windows e abilitare ulteriori personalizzazioni delle macchine.

Prerequisiti

- Identificare o creare la macchina di riferimento.
- Stabilire un rapporto di attendibilità sicura tra l'agente guest e la macchina del servizio di gestione. Vedere [Configurare l'agente guest in modo che consideri attendibile un server..](#)

Procedura

- 1 Passare alla pagina **Programmi di installazione degli agenti guest e software** dell'appliance vRealize Automation:

<https://vrealize-automation-appliance-FQDN/software>

- 2 In **Programmi di installazione degli agenti guest**, scaricare e salvare il file eseguibile a 32 o 64 bit nella directory principale dell'unità C:.

Nota Esiste un'alternativa della riga di comando a questa procedura per l'installazione dell'agente guest. Invece di scaricare i file eseguibili, è possibile passare ai **programmi di installazione del software Windows** nella pagina dei programmi di installazione dell'agente software e guest. Da qui è possibile scaricare ed eseguire lo script di PowerShell `prepare_vra_template.ps1`:

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

- 3 Estrarre i file dell'agente guest di Windows avviando il file eseguibile.

L'estrazione crea la cartella `C:\VRMGuestAgent` e aggiunge i file.

Non rinominare C:\VRMGuestAgent.

- 4 Configurare l'agente guest per la comunicazione con il servizio di gestione.
 - a Aprire un prompt dei comandi con privilegi elevati.
 - b Passare a C:\VRMGuestAgent.
 - c Inserire il file PEM del servizio di gestione attendibile nella directory C:\VRMGuestAgent\ per configurare l'agente guest in modo che consideri attendibile la macchina del servizio di gestione.
 - d Eseguire `win service -i -h Manager_Service_Hostname_fqdn:portnumber -p ssl`.

Il numero di porta predefinito per il servizio di gestione è 443.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e la porta relativi al bilanciamento del carico del servizio di gestione. Ad esempio <code>win service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> .
Senza bilanciamento del carico	Specificare il nome di dominio completo e la porta relativi alla macchina del servizio di gestione. Ad esempio <code>win service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> .
Se si prepara un'immagine di macchina Amazon	È necessario specificare che si sta utilizzando Amazon. Ad esempio <code>win service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

Risultati

Il nome del servizio Windows è VCACGuestAgentService. Il registro di installazione VCAC-GuestAgentService.log si trova in C:\VRMGuestAgent.

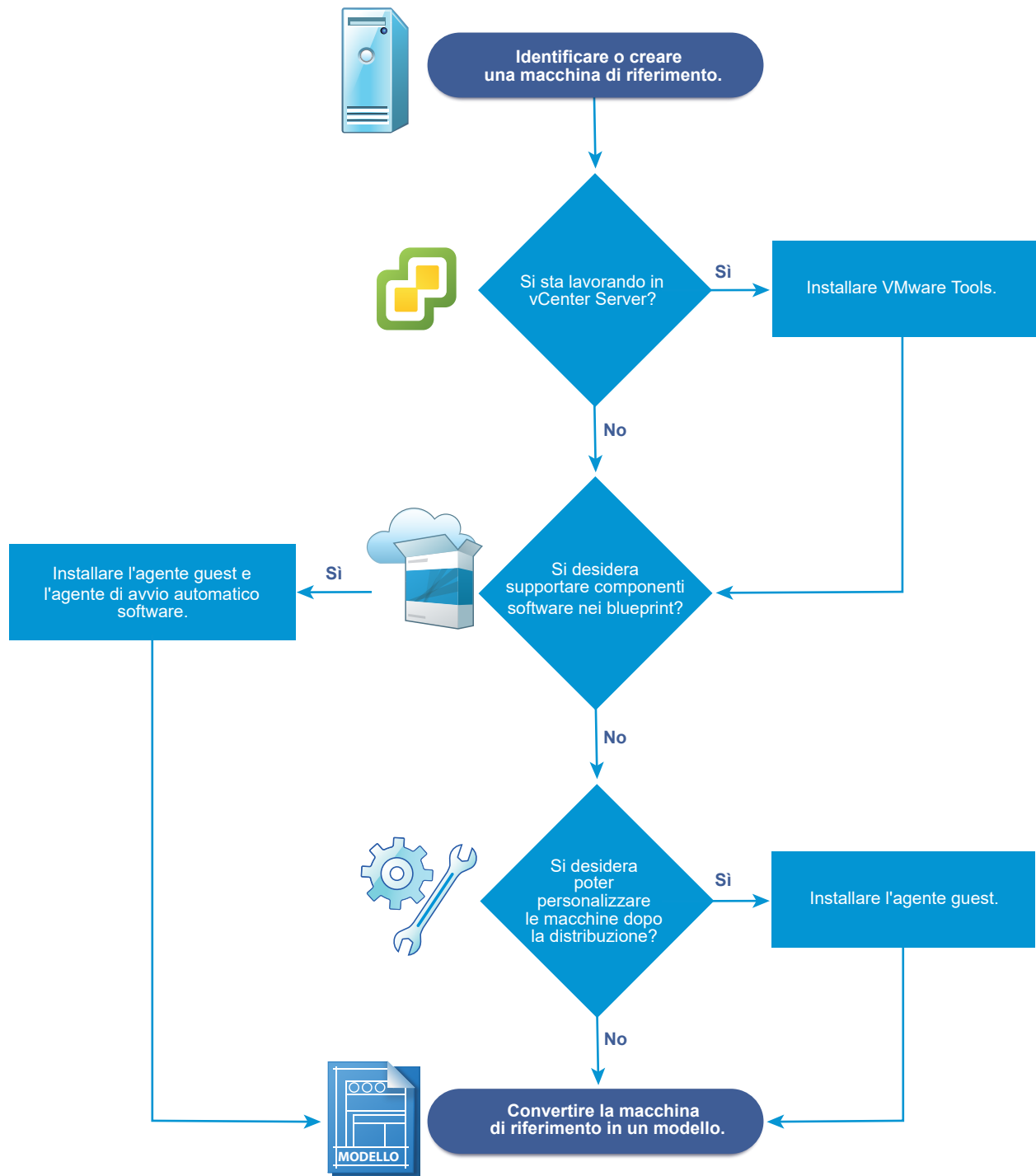
Operazioni successive

Convertire la macchina di riferimento in un modello per la clonazione, un'immagine di macchina Amazon o uno snapshot in modo che gli architetti di IaaS possano utilizzare tale modello quando creano i blueprint.

Elenco di controllo per la preparazione al provisioning tramite clonazione

È necessario eseguire alcune operazioni di preparazione esterne a vRealize Automation per creare il modello e gli oggetti di personalizzazione utilizzati per clonare macchine virtuali Linux e Windows.

La clonazione viene eseguita a partire da un modello creato da una macchina di riferimento.



Se si sta eseguendo il provisioning di una macchina Windows mediante clonazione, gli unici modi per unire la macchina fornita in provisioning a un dominio di Active Directory sono utilizzare la specifica di personalizzazione da vCenter Server o includere un profilo di sistema operativo guest nel proprio modello SCVMM. Le macchine fornite in provisioning mediante clonazione non possono essere collocate in un contenitore di Active Directory durante il provisioning. Questa operazione dovrà essere eseguita manualmente dopo il provisioning.

Tabella 1-8. Elenco di controllo per la preparazione al provisioning tramite clonazione

Attività	Posizione	Dettagli
<input type="checkbox"/> Identificare o creare la macchina di riferimento.	Hypervisor	Consultare la documentazione fornita dal proprio hypervisor.
<input type="checkbox"/> (Facoltativo) Se si desidera clonare il modello per supportare componenti Software, installare l'agente guest di vRealize Automation e l'agente di avvio automatico del software sulla macchina di riferimento.	Macchina di riferimento	<p>Per le macchine di riferimento Windows, vedere Preparazione di una macchina di riferimento Windows per il supporto di Software.</p> <p>Per le macchine di riferimento Linux, vedere Preparazione di una macchina di riferimento Linux per il supporto di Software.</p>
<input type="checkbox"/> (Facoltativo) Se non è necessario clonare il modello per supportare componenti Software ma si desidera poter personalizzare le macchine distribuite, installare l'agente guest di vRealize Automation sulla macchina di riferimento.	Macchina di riferimento	Vedere Utilizzo dell'agente guest di vRealize Automation nel provisioning .
<input type="checkbox"/> Se si lavora in un ambiente vCenter Server, installare VMware Tools sulla macchina di riferimento.	vCenter Server	Vedere la documentazione di VMware Tools.
<input type="checkbox"/> Utilizzare la macchina di riferimento per creare un modello per la clonazione.	Hypervisor	<p>La macchina di riferimento può essere accesa o spenta. Se si sta clonando in vCenter Server, è possibile utilizzare una macchina di riferimento direttamente senza creare un modello.</p> <p>Consultare la documentazione fornita dal proprio hypervisor.</p>
<input type="checkbox"/> Creare l'oggetto di personalizzazione per configurare macchine clonate applicando le informazioni dell'Utilità di preparazione del sistema o una personalizzazione Linux.	Hypervisor	<p>Se si sta clonando per Linux è possibile installare l'agente guest di Linux e fornire script di personalizzazione esterni, evitando così di creare un oggetto di personalizzazione. Se si sta clonando con vCenter Server, è necessario fornire la specifica di personalizzazione come oggetto di personalizzazione.</p> <p>Consultare la documentazione fornita dal proprio hypervisor.</p>
<input type="checkbox"/> Raccogliere le informazioni necessarie per creare blueprint che clonano il modello.	Catturare le informazioni e trasferirle agli architetti di IaaS.	Vedere Foglio di lavoro per il provisioning virtuale tramite clonazione .

Foglio di lavoro per il provisioning virtuale tramite clonazione

Completare il foglio di lavoro di trasferimento delle conoscenze per acquisire informazioni su modello, personalizzazioni e proprietà personalizzate necessarie per creare blueprint clone per i modelli preparati nell'ambiente. Non tutte le informazioni sono necessarie per ogni

implementazione. Utilizzare questo foglio di lavoro come guida oppure copiare e incollare le tabelle del foglio di lavoro in uno strumento di elaborazione testo per modificarle.

Informazioni su modello e prenotazione richieste

Tabella 1-9. Foglio di lavoro con informazioni su modello e prenotazione

Informazioni richieste	Valore personale	Dettagli
Nome modello		
Prenotazioni in cui il modello è disponibile o criteri di prenotazione da applicare		Per evitare errori durante il provisioning, assicurarsi che il modello sia disponibile in tutte le prenotazioni o creare criteri di prenotazione che possano essere utilizzati dagli architetti dei blueprint per limitare il blueprint alle prenotazioni in cui il modello è disponibile.
(Solo vSphere) Tipo di clonazione richiesta per questo modello		<ul style="list-style-type: none"> ■ Clona ■ Clone collegato ■ NetApp FlexClone
Nome specifico della personalizzazione (obbligatorio per la clonazione con indirizzi IP statici)		<p>Non è possibile eseguire la personalizzazione di macchine Windows senza una specifica di personalizzazione di vSphere.</p> <p>Vedere Aggiunta di una macchina Linux a un dominio Active Directory di Windows.</p>
(Solo SCVMM) Nome ISO		
(Solo SCVMM) Disco rigido virtuale		
(Solo SCVMM) Profilo hardware da collegare alle macchine con provisioning		

Gruppi di proprietà richiesti

È possibile completare le sezioni relative alle informazioni sulle proprietà personalizzate del foglio di lavoro oppure creare gruppi di proprietà e chiedere agli architetti di aggiungere i gruppi di proprietà ai loro blueprint anziché numerose singole proprietà personalizzate.

Sistema operativo vCenter Server richiesto

È necessario fornire la proprietà personalizzata del sistema operativo guest per il provisioning di vCenter Server.

Tabella 1-10. Sistema operativo di vCenter Server

Proprietà personalizzata	Valore personale	Descrizione
VMware.VirtualCenter.OperatingSystem		Specifica la versione del sistema operativo guest di vCenter Server (VirtualMachineGuestOsIdentifier) con cui vCenter Server crea la macchina. Questa versione del sistema operativo deve corrispondere alla versione del sistema operativo da installare sulla macchina fornita in provisioning. Gli amministratori possono creare gruppi di proprietà utilizzando uno di diversi set di proprietà, ad esempio VMware[OS_Version]Properties, che sono predefiniti per includere i valori di VMware.VirtualCenter.OperatingSystem corretti. Questa proprietà è valida per il provisioning virtuale.

Informazioni sugli script di Visual Basic

Se vRealize Automation è stato configurato per l'esecuzione dei propri script Visual Basic personalizzati come passaggi aggiuntivi durante il ciclo di vita della macchina, è necessario includere informazioni sugli script nel blueprint.

Nota un amministratore di struttura può creare un gruppo di proprietà utilizzando i set di proprietà ExternalPreProvisioningVbScript ed ExternalPostProvisioningVbScript per fornire questa informazioni richiesta. In questo modo sarà più semplice per gli architetti dei blueprint includere correttamente queste informazioni nei propri blueprint.

Tabella 1-11. Informazioni sugli script di Visual Basic

Proprietà personalizzata	Valore personale	Descrizione
ExternalPreProvisioningVbScript		Eseguire uno script prima del provisioning. Immettere il percorso completo dello script includendo il nome del file e l'estensione. <i>%System Drive%Programmi (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs.</i>
ExternalPostProvisioningVbScript		Eseguire uno script al termine del provisioning. Immettere il percorso completo dello script includendo il nome del file e l'estensione. <i>%System Drive%Programmi (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</i>

Informazioni sugli script di personalizzazione dell'agente guest di Linux

Se il modello Linux è stato configurato in modo da utilizzare l'agente guest per l'esecuzione degli script di personalizzazione, è necessario includere informazioni sugli script nel blueprint.

Tabella 1-12. Foglio di lavoro con informazioni sugli script di personalizzazione dell'agente guest di Linux

Proprietà personalizzata	Valore personale	Descrizione
Linux.ExternalScript.Name		Specifica il nome di uno script di personalizzazione opzionale, ad esempio config.sh, che l'agente guest di Linux esegue dopo l'installazione del sistema operativo. Questa proprietà è disponibile per macchine Linux clonate da modelli su cui è installato l'agente Linux. Se si specifica uno script esterno, è necessario inoltre definire la sua posizione utilizzando le proprietà Linux.ExternalScript.LocationType e Linux.ExternalScript.Path.
Linux.ExternalScript.LocationType		Specifica il tipo di posizione dello script di personalizzazione denominato nella proprietà Linux.ExternalScript.Name. Questo può essere local oppure nfs. È necessario anche specificare la posizione dello script utilizzando la proprietà Linux.ExternalScript.Path. Se il tipo di posizione è nfs, utilizzare anche la proprietà Linux.ExternalScript.Server.
Linux.ExternalScript.Server		Specifica il nome del server NFS, ad esempio lab-ad.lab.local, in cui collocare lo script di personalizzazione esterno di Linux denominato in Linux.ExternalScript.Name.
Linux.ExternalScript.Path		Specifica il percorso locale dello script di personalizzazione Linux o il percorso di esportazione nella personalizzazione di Linux sul server NFS. Il valore deve iniziare con una barra e non includere il nome del file, ad esempio /scripts/linux/config.sh.

Altre proprietà personalizzate dell'agente guest

Se l'agente guest è stato installato nella propria macchina di riferimento, è possibile utilizzare le proprietà personalizzate per personalizzare ulteriormente le macchine in seguito alla distribuzione.

Tabella 1-13. Foglio di calcolo delle proprietà personalizzate per la personalizzazione delle macchine clonate con un agente guest

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.Admin.AddOwnerToAdmins		Impostare su True (predefinito) per aggiungere il proprietario della macchina, specificato dalla proprietà VirtualMachine.Admin.Owner, al gruppo di amministratori locale della macchina.
VirtualMachine.Admin.AllowLogin		Impostare su True (predefinito) per aggiungere il proprietario della macchina al gruppo di utenti desktop remoti locale, come specificato dalla proprietà VirtualMachine.Admin.Owner.
VirtualMachine.Admin.UseGuestAgent		Se l'agente guest è installato come servizio su un modello per la clonazione, impostare su True sul blueprint della macchina per abilitare il servizio dell'agente guest sulle macchine clonate da quel modello. Quando la macchina viene avviata, viene avviato anche il servizio dell'agente guest. Impostare su False per disattivare l'agente guest. Se impostato su False, il workflow di clonazione avanzato non utilizzerà l'agente guest per le attività del sistema operativo guest, riducendo la sua funzionalità a VMwareCloneWorkflow. Se non specificato o se impostato su un valore diverso da False, il workflow di clonazione avanzato invierà elementi di lavoro all'agente guest.
VirtualMachine.DiskN.Active		Impostare su True (predefinito) per specificare che il disco <i>N</i> della macchina è attivo. Impostare su False per specificare che il disco <i>N</i> della macchina non è attivo.

Tabella 1-13. Foglio di calcolo delle proprietà personalizzate per la personalizzazione delle macchine clonate con un agente guest (continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.DiskN.Label		Specifica l'etichetta del disco <i>N</i> di una macchina. L'etichetta del disco può contenere al massimo 32 caratteri. La numerazione dei dischi deve essere sequenziale. Quando utilizzato con un agente guest, specifica l'etichetta del disco <i>N</i> di una macchina all'interno del sistema operativo guest.
VirtualMachine.DiskN.Letter		Specifica la lettera di unità o il punto di montaggio del disco <i>N</i> di una macchina. L'impostazione predefinita è C. Ad esempio, per specificare la lettera D per Disk 1, definire la proprietà personalizzata nel modo seguente VirtualMachine.Disk1.Letter e immettere il valore D. La numerazione dei dischi deve essere sequenziale. Quando utilizzato in associazione a un agente guest, questo valore specifica la lettera di unità o il punto di montaggio sotto cui viene montato un disco aggiuntivo <i>N</i> dall'agente guest nel sistema operativo guest.
VirtualMachine.Admin.CustomizeGuestOSDelay		Specifica il tempo di attesa che deve trascorrere dopo il completamento della personalizzazione e prima che inizi la personalizzazione del sistema operativo guest. Il valore deve essere nel formato HH:MM:SS. Se il valore non è impostato, il valore predefinito è un minuto (00:01:00). Se si sceglie di non includere questa proprietà personalizzata, il provisioning terminerà con esito negativo se la macchina virtuale si riavvierà prima che gli elementi di lavoro dell'agente guest siano stati completati.
VirtualMachine.Customize.WaitComplete		Impostare su True per evitare che il workflow di provisioning invii gli elementi di lavoro all'agente guest prima che siano state completate tutte le personalizzazioni. Impostare su False per consentire la creazione degli elementi di lavoro prima del completamento della personalizzazione.

Tabella 1-13. Foglio di calcolo delle proprietà personalizzate per la personalizzazione delle macchine clonate con un agente guest (continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.SoftwareN.Name		Specifica il nome descrittivo di un'applicazione software <i>N</i> o script per l'installazione o l'esecuzione durante il provisioning. Questa è una proprietà facoltativa e a solo scopo informativo. Non ha una funzione reale per il workflow di clonazione avanzato o per l'agente guest, ma è utile per una selezione personalizzata del software in un'interfaccia utente o per la creazione di report sull'uso del software.
VirtualMachine.SoftwareN.ScriptPath		Specifica il percorso completo dello script d'installazione di un'applicazione. Il percorso deve essere un percorso assoluto valido, così come visto dal sistema operativo guest, e deve includere il nome del file dello script. È possibile passare i valori delle proprietà personalizzate come parametri allo script inserendo <i>{CustomPropertyName}</i> nella stringa del percorso. Se ad esempio si ha una proprietà personalizzata chiamata <i>ActivationKey</i> il cui valore è 1234, il percorso dello script è <i>D:\InstallApp.bat -key {ActivationKey}</i> . L'agente guest esegue il comando <i>D:\InstallApp.bat -key 1234</i> . Il file dello script può quindi essere programmato per accettare e utilizzare questo valore.
VirtualMachine.SoftwareN.ISOName		Specifica il percorso e il nome del file ISO relativo alla radice del datastore. Il formato è <i>/folder_name/subfolder_name/file_name.iso</i> . Se il valore non viene specificato, l'immagine ISO non viene montata.
VirtualMachine.SoftwareN.ISOLocation		Specifica il percorso di storage che contiene il file dell'immagine ISO che deve essere utilizzato dall'applicazione o dallo script. Formattare il percorso così come appare sulla prenotazione dell'host, ad esempio <i>netapp-1:it_nfs_1</i> . Se il valore non viene specificato, l'immagine ISO non viene montata.

Proprietà personalizzate di rete

È possibile specificare la configurazione di dispositivi di rete specifici su una macchina utilizzando le proprietà personalizzate.

Le proprietà personalizzate comuni correlate alle reti sono elencate nella seguente tabella. Per ulteriori proprietà personalizzate correlate, vedere *Proprietà personalizzate per i blueprint di cloni* e *Proprietà personalizzate per il networking* in *Guida di riferimento alle proprietà personalizzate*.

Tabella 1-14. Proprietà personalizzate per la configurazione del networking

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.NetworkN.Address		Specifica l'indirizzo IP del dispositivo di rete <i>N</i> in una macchina fornita in provisioning con un indirizzo IP statico.
VirtualMachine.NetworkN.MacAddressType		<p>Indica se l'indirizzo MAC del dispositivo di rete <i>N</i> è generato o definito dall'utente (statico). La proprietà è disponibile per la clonazione.</p> <p>Il valore predefinito è generated. Se il valore è static, è necessario utilizzare anche</p> <p>VirtualMachine.NetworkN.MacAddress per specificare l'indirizzo MAC.</p> <p>L'uso delle proprietà personalizzate VirtualMachine.NetworkN è specifico per blueprint singoli e macchine singole. Quando viene richiesta una macchina, l'allocazione di rete e indirizzo IP viene eseguita prima che la macchina venga assegnata a una prenotazione. Poiché l'allocazione dei blueprint in una prenotazione specifica non è garantita, non utilizzare questa proprietà su una prenotazione. Questa proprietà non è supportata per NAT su richiesta o reti instradate su richiesta</p>

Tabella 1-14. Proprietà personalizzate per la configurazione del networking (continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.NetworkN.MacAddress		<p>Specifica l'indirizzo MAC di un dispositivo di rete N. La proprietà è disponibile per la clonazione.</p> <p>Se il valore di VirtualMachine.NetworkN.MacAddressType è generated, la proprietà contiene l'indirizzo generato.</p> <p>Se il valore di VirtualMachine.NetworkN.MacAddressType è static, la proprietà specifica l'indirizzo MAC. Per le macchine virtuali fornite in provisioning sugli host del server ESX, l'indirizzo deve essere incluso nell'intervallo specificato da VMware. Per informazioni dettagliate, consultare la documentazione di vSphere.</p> <p>L'uso delle proprietà personalizzate VirtualMachine.NetworkN è specifico per blueprint singoli e macchine singole. Quando viene richiesta una macchina, l'allocazione di rete e indirizzo IP viene eseguita prima che la macchina venga assegnata a una prenotazione.</p> <p>Poiché l'allocazione dei blueprint in una prenotazione specifica non è garantita, non utilizzare questa proprietà su una prenotazione.</p> <p>Questa proprietà non è supportata per NAT su richiesta o reti instradate su richiesta</p>

Tabella 1-14. Proprietà personalizzate per la configurazione del networking (continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.NetworkN.Name		<p>Specifica il nome della rete a cui connettersi, ad esempio il dispositivo di rete <i>N</i> a cui la macchina è collegata. Equivale a una scheda di rete (NIC).</p> <p>Per impostazione predefinita, viene assegnata una rete dai percorsi di rete disponibili sulla prenotazione su cui viene eseguito il provisioning della macchina. Vedere anche <code>VirtualMachine.NetworkN.AddressType</code>.</p> <p>È possibile assicurarsi che un dispositivo di rete sia collegato a una rete specifica impostando il valore di questa proprietà sul nome di una rete su una prenotazione disponibile. Ad esempio, se si forniscono proprietà per $N = 0$ e 1, si ottengono due schede di rete e il rispettivo valore assegnato, purché la rete sia selezionata nella prenotazione associata.</p> <p>L'uso delle proprietà personalizzate <code>VirtualMachine.NetworkN</code> è specifico per blueprint e macchine. Quando viene richiesta una macchina, l'allocazione di rete e indirizzo IP viene eseguita prima che la macchina venga assegnata a una prenotazione. Poiché l'allocazione dei blueprint in una prenotazione specifica non è garantita, non utilizzare questa proprietà su una prenotazione. Questa proprietà non è supportata per NAT su richiesta o reti instradate su richiesta.</p> <p>Per un esempio di come utilizzare questa proprietà personalizzata per impostare <code>VirtualMachine.Network0.Name</code> in modo dinamico in base alla selezione di un utente da un elenco di reti disponibili predefinite, vedere il post di blog Adding a Network Selection Drop-Down in vRA 7.</p>

Tabella 1-14. Proprietà personalizzate per la configurazione del networking (continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.NetworkN.PortID		<p>Specifica l'ID della porta da utilizzare per il dispositivo di rete <i>N</i> quando si utilizza un gruppo dvPort con un vSphere Distributed Switch.</p> <p>L'uso delle proprietà personalizzate VirtualMachine.NetworkN è specifico per blueprint singoli e macchine singole. Quando viene richiesta una macchina, l'allocazione di rete e indirizzo IP viene eseguita prima che la macchina venga assegnata a una prenotazione. Poiché l'allocazione dei blueprint in una prenotazione specifica non è garantita, non utilizzare questa proprietà su una prenotazione. Questa proprietà non è supportata per NAT su richiesta o reti instradate su richiesta</p>
VirtualMachine.NetworkN.NetworkProfileName		<p>Specifica il nome di un profilo di rete da cui assegnare un indirizzo IP statico al dispositivo di rete <i>N</i> o da cui ottenere l'intervallo degli indirizzi IP statici che possono essere assegnati a un dispositivo di rete <i>N</i> di una macchina clonata, dove <i>N</i>=0 per il primo dispositivo, 1 per il secondo e così via.</p> <p>Il profilo di rete a cui la proprietà punta viene utilizzato per allocare un indirizzo IP. La proprietà determina la rete a cui la macchina si connette, in base alla prenotazione.</p>

Tabella 1-14. Proprietà personalizzate per la configurazione del networking (continua)

Proprietà personalizzata	Valore personale	Descrizione
<ul style="list-style-type: none"> ■ VirtualMachine.NetworkN.SubnetMask ■ VirtualMachine.NetworkN.Gateway ■ VirtualMachine.NetworkN.PrimaryDns ■ VirtualMachine.NetworkN.SecondaryDns ■ VirtualMachine.NetworkN.PrimaryWins ■ VirtualMachine.NetworkN.SecondaryWins ■ VirtualMachine.NetworkN.DnsSuffix ■ VirtualMachine.NetworkN.DnsSearchSuffixes 		<p>L'apposizione di un nome consente di creare più versioni di una proprietà personalizzata. Ad esempio, le proprietà seguenti potrebbero elencare pool di bilanciamento del carico configurati per l'uso generale e macchine con requisiti di prestazioni alti, moderati e bassi:</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low <p>Configura gli attributi del profilo di rete specificato in VirtualMachine.NetworkN.NetworkProfileName.</p>
VCNS.LoadBalancerEdgePool.Names.name		<p>Specifica i pool di bilanciamento del carico di NSX a cui la macchina virtuale viene assegnata durante il provisioning. La macchina virtuale viene assegnata a tutte le porte dei servizi di tutti i pool specificati. Il valore è un nome <i>edge/pool</i> o un elenco di nomi <i>edge/pool</i> separati da virgole. Per i nomi viene fatta distinzione tra maiuscole e minuscole.</p> <p>L'apposizione di un nome consente di creare più versioni di una proprietà personalizzata. Ad esempio, le proprietà seguenti potrebbero elencare pool di bilanciamento del carico configurati per l'uso generale e macchine con requisiti di prestazioni alti, moderati e bassi:</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low

Tabella 1-14. Proprietà personalizzate per la configurazione del networking (continua)

Proprietà personalizzata	Valore personale	Descrizione
VCNS.SecurityGroup.Names.name		<p>Specifica il gruppo o i gruppi di sicurezza di NSX a cui viene assegnata la macchina virtuale durante il provisioning. Il valore è il nome di un gruppo di sicurezza o un elenco di nomi separati da virgole. Per i nomi viene fatta distinzione tra maiuscole e minuscole.</p> <p>L'apposizione di un nome consente di creare più versioni della proprietà, che possono essere utilizzate separatamente o in combinazione. Ad esempio, le proprietà seguenti possono elencare gruppi di sicurezza pensati per l'uso generale, per la forza vendite e per il supporto:</p> <ul style="list-style-type: none"> ■ VCNS.SecurityGroup.Names ■ VCNS.SecurityGroup.Names.sales ■ VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names.name		<p>Specifica il tag o i tag di sicurezza di NSX a cui viene associata la macchina virtuale durante il provisioning. Il valore è il nome di un tag di sicurezza o un elenco di nomi separati da virgole. Per i nomi viene fatta distinzione tra maiuscole e minuscole.</p> <p>L'apposizione di un nome consente di creare più versioni della proprietà, che possono essere utilizzate separatamente o in combinazione. Ad esempio, le proprietà seguenti possono elencare tag di sicurezza pensati per l'uso generale, per la forza vendite e per il supporto:</p> <ul style="list-style-type: none"> ■ VCNS.SecurityTag.Names ■ VCNS.SecurityTag.Names.sales ■ VCNS.SecurityTag.Names.support

Aggiunta di una macchina Linux a un dominio Active Directory di Windows

Esistono diversi metodi per aggiungere una macchina Linux a un dominio Active Directory di Windows quando si esegue il provisioning della macchina.

- Se si esegue il provisioning tramite clonazione, è necessario utilizzare una specifica di personalizzazione (per il provisioning di una macchina vSphere) o includere il profilo di un sistema operativo guest con un modello SCVMM. Quando si esegue il provisioning della macchina, viene aggiunta al dominio specificato.
- Se non si esegue il provisioning tramite clonazione, è possibile utilizzare l'impostazione del suffisso DNS nel profilo di rete associato del blueprint per identificare il dominio. Tuttavia, per il provisioning del clone Windows con l'assegnazione di un indirizzo IP statico, è *necessario* utilizzare una specifica di personalizzazione di vSphere.
- Se si utilizza una specifica di personalizzazione di vSphere, quando viene eseguito il provisioning delle macchine, vengono aggiunte al dominio identificato nella specifica di personalizzazione e non al dominio specificato come suffisso DNS nel profilo di rete associato del blueprint.

Le specifiche di personalizzazione di vSphere sono oggetti di vSphere che contengono un set di condizioni predefinito per le impostazioni dei sistemi operativi guest Windows e Linux. È possibile aggiungere un nome della specifica di personalizzazione al blueprint di vRealize Automation utilizzando l'impostazione **Specifica personalizzazione** nella scheda **Informazioni build** della macchina.

Per informazioni sulla creazione di specifiche di personalizzazione in vSphere, vedere gli argomenti relativi alle specifiche di personalizzazione nella [documentazione del prodotto di vSphere](#), ad esempio *Creazione e gestione delle specifiche di personalizzazione*.

Preparazione per il provisioning di vCloud Air e vCloud Director

Per preparare macchine vCloud Air e vCloud Director per il provisioning utilizzando vRealize Automation, è necessario configurare il Virtual Data Center dell'organizzazione con modelli e oggetti di personalizzazione.

Per eseguire il provisioning di risorse di vCloud Air e vCloud Director utilizzando vRealize Automation, l'organizzazione necessita di un modello da cui clonare, costituito da una o più risorse macchina.

I modelli da condividere in tutta l'organizzazione devono essere pubblici. Solo i modelli riservati sono disponibili a vRealize Automation come origini di clonazione.

Nota quando si crea un blueprint clonando da un modello, l'identificatore univoco di quel modello diviene associato al blueprint. Il modello associato viene rilevato quando il blueprint viene pubblicato nel catalogo di vRealize Automation e utilizzato nei processi di provisioning e raccolta dati. Se si elimina il modello in vCloud Air o vCloud Director, le successive operazioni di provisioning e raccolta dati di vRealize Automation non riescono perché il modello associato non esiste più. Anziché eliminare e ricreare un modello, ad esempio per caricarne una versione aggiornata, sostituire il modello utilizzando il processo di sostituzione modelli di vCloud Air e vCloud Director. Utilizzando vCloud Air o vCloud Director per sostituire il modello piuttosto che eliminarlo e ricrearlo, l'ID univoco del modello viene lasciato inalterato e provisioning e raccolta dati continueranno a funzionare senza interruzioni.

Nei punti seguenti vengono descritti a grandi linee i passaggi da eseguire prima di utilizzare vRealize Automation per creare endpoint e definire prenotazioni e blueprint. Per ulteriori informazioni su queste attività amministrative, vedere la documentazione di vCloud Air e vCloud Director.

- 1 In vCloud Air o vCloud Director, creare un modello per la clonazione e aggiungerlo al catalogo dell'organizzazione.
- 2 In vCloud Air o vCloud Director, utilizzare il modello per specificare le impostazioni personalizzate quali le password, il dominio e gli script per il sistema operativo guest su ciascuna macchina.

È possibile utilizzare vRealize Automation per sovrascrivere alcune di queste impostazioni.

La personalizzazione può variare in base al sistema operativo guest della risorsa.

- 3 In vCloud Air o vCloud Director, configurare il catalogo affinché sia condiviso con tutti all'interno dell'organizzazione.

In vCloud Air o vCloud Director, configurare l'accesso dell'amministratore account alle organizzazioni applicabili per consentire a tutti gli utenti e i gruppi dell'organizzazione di accedere al catalogo. Se non si definisce questa condivisione, i modelli del catalogo non saranno visibili a endpoint e architetti di blueprint in vRealize Automation.

- 4 Raccogliere le seguenti informazioni in modo da poterle includere nei blueprint:

- Nome del modello di vCloud Air o vCloud Director.
- Quantità di storage totale specificata per il modello.

Preparazione per il provisioning Linux Kickstart

Il provisioning Linux Kickstart utilizza un file di configurazione per automatizzare un'installazione Linux su una nuova macchina di cui è stato eseguito il provisioning. Per predisporre il provisioning, è necessario creare un'immagine ISO avviabile e un file di configurazione Kickstart o autoYaST.

L'elenco che segue è una panoramica ad alto livello dei passaggi necessari per preparare il provisioning Linux Kickstart:

- 1 Verificare che nella rete sia disponibile un server DHCP. vRealize Automation non è in grado di eseguire il provisioning Linux Kickstart delle macchine se non è disponibile il servizio DHCP.
- 2 Preparare il file di configurazione. Nel file di configurazione è necessario specificare le posizioni del server vRealize Automation e del pacchetto d'installazione dell'agente di Linux. Vedere [Preparazione del file di esempio della configurazione di Linux Kickstart](#).
- 3 Modificare `isolinux/isolinux.cfg` o `loader/isolinux.cfg` per specificare il nome e la posizione del file di configurazione e l'origine della distribuzione Linux appropriata.
- 4 Creare l'immagine ISO di avvio e salvarla nella posizione richiesta dalla piattaforma di virtualizzazione utilizzata. Consultare la documentazione fornita dal proprio hypervisor per informazioni sulla posizione richiesta.

- 5 (Facoltativo) Aggiungere gli script di personalizzazione.
 - a Per specificare gli script di personalizzazione post-installazione nel file di configurazione, vedere [Definizione di script personalizzati in un file di configurazione kickstart/autoYaST](#).
 - b Per eseguire le chiamate agli script Visual Basic nel blueprint, vedere [Elenco di controllo per l'esecuzione di script Visual Basic durante il provisioning](#).
- 6 Raccogliere le seguenti informazioni in modo che gli architetti dei blueprint possano includerle nei propri blueprint:
 - a Nome e posizione dell'immagine ISO.
 - b Per le integrazioni di vCenter Server, la versione del sistema operativo guest di vCenter Server con cui vCenter Server creerà la macchina.

Nota è possibile creare un gruppo di proprietà con la proprietà `BootIsoProperties` impostata per includere le informazioni ISO richieste. In questo modo sarà più semplice includere correttamente le informazioni nei blueprint.

Preparazione del file di esempio della configurazione di Linux Kickstart

La dotazione di vRealize Automation include file di configurazione di esempio che è possibile modificare in base alle proprie esigenze. Per rendere i file utilizzabili sono necessarie alcune modifiche.

Procedura

- 1 Aprire la pagina della console di gestione dell'appliance vRealize Automation.
Ad esempio: `https://va-hostname.domain.com`.
- 2 Fare clic sulla pagina **Guest and software agents** (Agenti guest e software) nella sezione dedicata all'installazione dei componenti di vRealize Automation della pagina.
Ad esempio: `https://va-hostname.domain.com/software/index.html`.
Si apre la pagina **Guest and Software Agent Installers** (Programmi di installazione degli agenti guest e software), con i link ai download disponibili.
- 3 Fare clic su **Linux guest agent packages** (Pacchetti agenti guest Linux) nella sezione dedicata ai programmi di installazione degli agenti guest della pagina per scaricare e salvare il file `LinuxGuestAgentPkgs.zip`.
- 4 Decomprimere il file `LinuxGuestAgentPkgs.zip` scaricato per creare la cartella `VraLinuxGuestAgent`.
- 5 Andare alla sottodirectory `VraLinuxGuestAgent` che corrisponde al sistema operativo guest da distribuire durante il provisioning.
Ad esempio: `rhel32`.
- 6 Aprire un file nella sottodirectory dei campioni che corrisponde al sistema di destinazione.
Ad esempio, `samples/sample-https-rhel6-x86.cfg`.

- 7 Sostituire tutte le istanze della stringa `host=dcac.example.net` con l'indirizzo IP o il nome di dominio completo e il numero di porta del servizio di gestione o del bilanciamento del carico del servizio di gestione.

Piattaforma	Formato richiesto
vSphere ESXi	Indirizzo IP, ad esempio: <code>--host=172.20.9.59</code>
vSphere ESX	Indirizzo IP, ad esempio: <code>--host=172.20.9.58</code>
SUSE 10	Indirizzo IP, ad esempio: <code>--host=172.20.9.57</code>
Tutte le altre	Nome di dominio completo, ad esempio: <code>--host=mycompany-host1.mycompany.local:443</code>

- 8 Individuare ogni istanza di `gugent.rpm` o `gugent.tar.gz` e sostituire l'URL `rpm.example.net` con la posizione del pacchetto dell'agente `guest`.

Ad esempio:

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- 9 Salvare il file in una posizione accessibile alle macchine di cui verrà eseguito il provisioning.

Definizione di script personalizzati in un file di configurazione kickstart/autoYaST

È possibile modificare il file di configurazione per copiare o installare script personalizzati nelle macchine di cui è stato appena eseguito il provisioning. L'agente di Linux esegue gli script nel punto del workflow specificato.

Lo script può fare riferimento a qualsiasi file `./properties.xml` nelle directory `/usr/share/gugent/site/workitem`.

Prerequisiti

- Preparazione di un file di configurazione kickstart o autoYaST. Vedere [Preparazione del file di esempio della configurazione di Linux Kickstart](#).
- Lo script deve restituire un valore diverso da zero in caso di errore per evitare che il provisioning della macchina abbia esito negativo.

Procedura

- 1 Creare o identificare lo script da utilizzare.
- 2 Salvare lo script come `NN_scriptname`.

NN è un numero di due cifre. Gli script vengono eseguiti nell'ordine dal più basso al più alto. Se due script hanno lo stesso numero, l'ordine diventa quello alfabetico in base a *scriptname*.
- 3 Rendere eseguibile lo script.
- 4 Individuare la sezione post-installazione del file di configurazione kickstart o autoYaST.

In kickstart è indicata da `%post`. In autoYaST è indicata da `post-scripts`.

- 5 Modificare la sezione di post-installazione del file di configurazione per copiare o installare lo script nella directory `/usr/share/gugent/site/workitem` scelta.

Gli script personalizzati sono eseguiti più comunemente per kickstart/autoYaST virtuali con elementi di lavoro SetupOS (per provisioning di creazione) e CustomizeOS (per provisioning di clonazione), ma è possibile eseguire script in qualsiasi punto del workflow.

Ad esempio, è possibile modificare il file di configurazione per copiare lo script `11_addusers.sh` nella directory `/usr/share/gugent/site/SetupOS` su una macchina di cui è stato appena eseguito il provisioning utilizzando il seguente comando:

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/SetupOS
```

Risultati

L'agente di Linux esegue lo script nell'ordine specificato dalla directory dell'elemento di lavoro e dal nome del file di script.

Preparazione per il provisioning SCCM

vRealize Automation avvia una macchina appena fornita in provisioning da un'immagine ISO e quindi passa il controllo alla sequenza di attività SCCM specificate.

Il provisioning SCCM è supportato per la distribuzione di sistemi operativi Windows. Linux non è supportato. Distribuzione di software e aggiornamenti non sono supportati.

Per impostazione predefinita, una macchina SCCM è configurata per verificare l'appartenenza alla raccolta applicabile ogni 10 secondi dopo il provisioning. In alcuni casi, questo intervallo può causare problemi con il processo di registrazione. Sono disponibili due proprietà che consentono di personalizzare il processo di verifica. La prima proprietà è denominata `SCCM_refresh_collection_setting`. Per impostazione predefinita, questa proprietà è impostata su `true` per verificare che la macchina esegua un controllo dell'appartenenza. Se appropriato, è possibile impostarla su `false` per configurare la macchina in modo che ignori il controllo dell'appartenenza. La seconda proprietà è denominata `SCCM_machine_membership_check_interval`. Come indicato, il valore predefinito è 10 secondi, ma è possibile impostarlo su un valore diverso per aumentare la finestra di riesecuzione nel caso in cui si verifichino problemi di registrazione. Entrambe queste proprietà si trovano nelle impostazioni globali di IaaS in **Infrastruttura > Amministrazione > Impostazioni globali**.

L'elenco che segue è una panoramica ad alto livello dei passaggi necessari per preparare SCCM per il provisioning:

- 1 La comunicazione con SCCM richiede il nome NetBIOS del server SCCM.

Collaborare con l'amministratore di rete per garantire che almeno un Distributed Execution Manager (DEM) sia in grado di risolvere il nome di dominio completo del server SCCM con il proprio nome NetBIOS.

Non è necessario posizionare i DEM direttamente sulla stessa rete del server SCCM, ma i DEM devono essere in grado di raggiungere il server SCCM su IP.

- 2 Creare un pacchetto software che includa l'agente guest di vRealize Automation. Vedere [Creazione di un pacchetto software per il provisioning di SCCM](#).
- 3 In SCCM, creare la sequenza di attività desiderata per il provisioning della macchina. Il passaggio finale deve essere l'installazione del pacchetto software creato contenente l'agente guest di vRealize Automation. Per informazioni sulla creazione di sequenze di attività e sull'installazione di pacchetti software, consultare la documentazione di SCCM.
- 4 Creare un'immagine ISO di avvio Zero Touch per la sequenza di attività. Per impostazione predefinita, SCCM crea un'immagine ISO di avvio Light Touch. Per informazioni sulla configurazione di SCCM per immagini ISO Zero Touch, vedere la documentazione di SCCM.
- 5 Copiare l'immagine ISO nella posizione richiesta dalla piattaforma di virtualizzazione utilizzata. Se non si conosce la posizione appropriata, consultare la documentazione fornita a corredo con l'hypervisor.
- 6 Raccogliere le seguenti informazioni in modo che gli architetti dei blueprint possano includerle nei blueprint:
 - a Il nome della raccolta contenente la sequenza di attività.
 - b Il nome di dominio completo del server SCCM su cui risiede la raccolta contenente la sequenza.
 - c Il codice del sito del server SCCM.
 - d Credenziali di livello amministrativo per il server SCCM.
 - e (Facoltativo) Per integrazioni di SCVMM, l'immagine ISO, il disco rigido virtuale o il profilo hardware da allegare alle macchine fornite in provisioning.

Creazione di un pacchetto software per il provisioning di SCCM

Il passaggio finale nella sequenza di attività di SCCM deve essere l'installazione di un pacchetto software che includa l'agente guest di vRealize Automation.

Procedura

- 1 Aprire la pagina della console di gestione dell'appliance vRealize Automation.
Ad esempio: `https://va-hostname.domain.com`.
- 2 Fare clic sulla pagina **Guest and software agents** (Agenti guest e software) nella sezione dedicata all'installazione dei componenti di vRealize Automation della pagina.
Ad esempio: `https://va-hostname.domain.com/software/index.html`.
Si apre la pagina **Guest and Software Agent Installers** (Programmi di installazione degli agenti guest e software), con i link ai download disponibili.
- 3 Fare clic sui file degli agenti guest di Windows (**32 bit**) o (**64 bit**) nella sezione dedicata all'installazione dei componenti della pagina per scaricare e salvare il file `GuestAgentInstaller.exe` o `GuestAgentInstaller_x64.exe`.

- 4 Estrarre i file dell'agente guest Windows in una posizione accessibile da SCCM.
Verrà creata la directory C:\VRMGuestAgent. Non cambiare il nome di questa directory.
- 5 Creare un pacchetto software dal file di definizione SCCMPackageDefinitionFile.sms.
- 6 Rendere il pacchetto software disponibile nel punto di distribuzione in uso.
- 7 Selezionare il contenuto dei file dell'agente guest Windows estratti come file di origine.

Preparazione per il provisioning di WIM

Eseguire il provisioning di una macchina effettuando l'avvio in un ambiente WinPE, quindi installare un sistema operativo utilizzando l'immagine in formato WIM (Windows Imaging File Format) di una macchina di riferimento Windows esistente.

L'elenco che segue è una panoramica ad alto livello dei passaggi necessari per preparare il provisioning WIM:

- 1 Identificare o creare l'area di gestione temporanea. L'area di gestione temporanea deve essere una directory di rete che sia possibile specificare come percorso UNC o montare come unità di rete tramite
 - La macchina di riferimento.
 - Il sistema in cui si crea l'immagine WinPE.
 - L'host di virtualizzazione in cui si esegue il provisioning delle macchine.
- 2 Assicurarsi che la rete disponga di un server DHCP. vRealize Automation non può eseguire il provisioning di macchine con un'immagine WIM se non è disponibile il servizio DHCP.
- 3 Identificare o creare la macchina di riferimento nella piattaforma di virtualizzazione che si intende utilizzare per il provisioning. Per i requisiti di vRealize Automation, vedere [Requisiti della macchina di riferimento per il provisioning WIM](#). Per informazioni sulla creazione di una macchina di riferimento, consultare la documentazione fornita dall'hypervisor.
- 4 Utilizzando System Preparation Utility for Windows, preparare il sistema operativo della macchina di riferimento per la distribuzione. Vedere [Requisiti di SysPrep per la macchina di riferimento](#).
- 5 Creare l'immagine WIM della macchina di riferimento. Non includere spazi nel nome del file dell'immagine WIM, altrimenti il provisioning non riuscirà.
- 6 Creare un'immagine WinPE che contenga l'agente guest di vRealize Automation.
 - (Facoltativo) Creare tutti gli script personalizzati che si desidera utilizzare per personalizzare le macchine di cui viene eseguito il provisioning e collocarli nella directory degli elementi di lavoro appropriata.
 - Se si utilizza VirtIO per le interfacce di rete o di storage, è necessario assicurarsi che nell'immagine WinPE e nell'immagine WIM siano inclusi i driver necessari. Vedere [Preparazione per il provisioning WIM con i driver VirtIO](#).

Quando si crea l'immagine WinPE, è necessario specificare manualmente l'agente guest di vRealize Automation. Vedere [Inserimento manuale dell'agente guest in un'immagine WinPE](#).

- 7 Collocare l'immagine di WinPE nella posizione richiesta dalla piattaforma di virtualizzazione utilizzata. Se non si conosce la posizione, consultare la documentazione dell'hypervisor.
- 8 Raccogliere le informazioni seguenti da includere nel blueprint:
 - a Nome e posizione dell'immagine ISO WinPE.
 - b Il nome del file WIM, il percorso UNC del file WIM e l'indice utilizzato per estrarre l'immagine desiderata dal file WIM.
 - c Il nome utente e la password usati per mappare il percorso dell'immagine WIM a un'unità di rete sulla macchina fornita in provisioning.
 - d (Facoltativo) Se non si intende accettare la lettera predefinita K, la lettera di unità a cui è mappato il percorso dell'immagine WIM sulla macchina fornita in provisioning.
 - e Per le integrazioni di vCenter Server, la versione del sistema operativo guest di vCenter Server con cui vCenter Server creerà la macchina.
 - f (Facoltativo) Per integrazioni di SCVMM, l'immagine ISO, il disco rigido virtuale o il profilo hardware da allegare alle macchine fornite in provisioning.

Nota è possibile creare un gruppo di proprietà per includere tutte queste informazioni richieste. L'uso di un gruppo di proprietà rende più semplice includere correttamente tutte le informazioni nei blueprint.

Procedura

1 [Requisiti della macchina di riferimento per il provisioning WIM](#)

Il provisioning WIM prevede la creazione di un'immagine WIM da una macchina di riferimento. La macchina di riferimento deve soddisfare requisiti di base per consentire all'immagine WIM di operare per il provisioning in vRealize Automation.

2 [Requisiti di SysPrep per la macchina di riferimento](#)

Un file di risposte SysPrep contiene diverse impostazioni richieste utilizzate per il provisioning di WIM.

3 [Preparazione per il provisioning WIM con i driver VirtIO](#)

Se si utilizza VirtIO per le interfacce di rete o di storage, è necessario assicurarsi che nell'immagine WinPE e nell'immagine WIM siano inclusi i driver necessari. VirtIO generalmente offre prestazioni migliori nel provisioning con KVM (RHEV).

4 [Inserimento manuale dell'agente guest in un'immagine WinPE](#)

È necessario inserire manualmente l'agente guest vRealize Automation nell'immagine WinPE.

Requisiti della macchina di riferimento per il provisioning WIM

Il provisioning WIM prevede la creazione di un'immagine WIM da una macchina di riferimento. La macchina di riferimento deve soddisfare requisiti di base per consentire all'immagine WIM di operare per il provisioning in vRealize Automation.

L'elenco che segue è una panoramica ad alto livello dei passaggi necessari per preparare una macchina di riferimento:

- 1 Se il sistema operativo della macchina di riferimento è Windows Server 2008 R2, Windows Server 2012, Windows 7 o Windows 8, l'installazione predefinita crea una piccola partizione sul disco rigido di sistema in aggiunta alla partizione principale. vRealize Automation non supporta l'uso delle immagini WIM create su macchine di riferimento con più partizioni come queste. È necessario eliminare la partizione durante il processo d'installazione.
- 2 Installare NET 4.5 e Windows Automated Installation Kit (AIK) per Windows 7 (incluso WinPE 3.0) sulla macchina di riferimento.
- 3 Se il sistema operativo della macchina di riferimento è Windows Server 2003 o Windows XP, reimpostare la password di amministratore lasciandola vuota (nessuna password).
- 4 (Facoltativo) Se si desidera abilitare l'integrazione di XenDesktop, installare e configurare un Citrix Virtual Desktop Agent.
- 5 (Facoltativo) È richiesto un agente Windows Management Instrumentation (WMI) per raccogliere determinati dati da una macchina Windows gestita da vRealize Automation, ad esempio lo stato di Active Directory del proprietario di una macchina. Per garantire la corretta gestione delle macchine Windows, è necessario installare un agente WMI (generalmente sull'host del servizio di gestione) e abilitare l'agente alla raccolta dati dalle macchine Windows. Vedere *Installazione di vRealize Automation*.

Requisiti di SysPrep per la macchina di riferimento

Un file di risposte SysPrep contiene diverse impostazioni richieste utilizzate per il provisioning di WIM.

Tabella 1-15. Impostazioni richieste da SysPrep per macchine di riferimento Windows Server o Windows XP

Impostazioni di GuiUnattended	Valore
AutoLogon	Sì
AutoLogonCount	1
AutoLogonUsername	<i>username</i> (<i>username</i> e <i>password</i> sono le credenziali utilizzate per l'accesso automatico quando la macchina di cui è stato appena eseguito il provisioning si avvia nel sistema operativo guest; in genere è utilizzato Administrator).
AutoLogonPassword	<i>password</i> corrispondente ad AutoLogonUsername.

Tabella 1-16. Impostazioni di SysPrep richieste per la macchina di riferimento che non utilizzano Windows Server 2003 o Windows XP:

Impostazioni di AutoLogon	Valore
Enabled	Sì
LogonCount	1
Username	<i>username</i> (username e password sono le credenziali utilizzate per l'accesso automatico quando la macchina di cui è stato appena eseguito il provisioning si avvia nel sistema operativo guest; in genere è utilizzato Administrator).
Password	<i>password</i> (username e password sono le credenziali utilizzate per l'accesso automatico quando la macchina di cui è stato appena eseguito il provisioning si avvia nel sistema operativo guest; in genere è utilizzato Administrator).

Nota Per le macchine di riferimento che utilizzano una piattaforma Windows più recente di Windows Server 2003/Windows XP, è necessario impostare la password di autologon utilizzando la proprietà personalizzata Sysprep.GuiUnattended.AdminPassword. Un sistema comodo per eseguire questa operazione consiste nel creare un gruppo di proprietà che includa questa proprietà personalizzata, in modo che gli amministratori tenant e i manager dei gruppi di business possano includere correttamente questa informazione nei propri blueprint.

Preparazione per il provisioning WIM con i driver VirtIO

Se si utilizza VirtIO per le interfacce di rete o di storage, è necessario assicurarsi che nell'immagine WinPE e nell'immagine WIM siano inclusi i driver necessari. VirtIO generalmente offre prestazioni migliori nel provisioning con KVM (RHEV).

I driver Windows per VirtIO sono inclusi come parte di Red Hat Enterprise Virtualization, collocati nella directory `/usr/share/virtio-win` all'interno del file system del Red Hat Enterprise Virtualization Manager. I driver sono inclusi anche nei Red Hat Enterprise Virtualization Guest Tools che si trovano in `/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso`.

Di seguito è illustrato il processo di alto livello per abilitare il provisioning basato su WIM con driver VirtIO:

- 1 Creare un'immagine WIM da una macchina di riferimento Windows con i driver VirtIO installati o inserire i driver in un'immagine WIM esistente.
- 2 Copiare i file dei driver VirtIO e inserire i driver in un'immagine WinPE.
- 3 Caricare l'ISO dell'immagine WinPE nei domini di storage ISO di Red Hat Enterprise Virtualization utilizzando il comando `rhev-m-iso-uploader`. Per ulteriori informazioni sulla gestione delle immagini ISO in RHEV, fare riferimento alla documentazione di Red Hat.

- 4 Creare un blueprint KVM (RHEV) per il provisioning WIM e selezionare l'opzione ISO WinPE. La proprietà personalizzata `VirtualMachine.Admin.DiskInterfaceType` deve essere inclusa con il valore **VirtIO**. Un amministratore di struttura può inserire queste informazioni in un gruppo di proprietà per includerle nei blueprint.

Le proprietà personalizzate `Image.ISO.Location` e `Image.ISO.Name` non sono utilizzate per i blueprint KVM (RHEV).

Inserimento manuale dell'agente guest in un'immagine WinPE

È necessario inserire manualmente l'agente guest vRealize Automation nell'immagine WinPE.

Prerequisiti

- Selezionare un sistema operativo Windows da cui l'area di staging preparata sia accessibile e su cui siano installati .NET 4.5 e Windows Automated Installation Kit (AIK) per Windows 7 (incluso WinPE 3.0).
- Creare un WinPE.

Procedura

1 [Installazione dell'agente guest in un WinPE](#)

È necessario copiare manualmente i file dell'agente guest nell'immagine WinPE.

2 [Configurazione del file `doagent.bat`](#)

È necessario configurare manualmente il file `doagent.bat`.

3 [Configurazione del file `doagentc.bat`](#)

È necessario configurare manualmente il file `doagentc.bat`.

4 [Configurazione dei file di proprietà dell'agente guest](#)

È necessario configurare manualmente i file delle proprietà dell'agente ospite.

Procedura

1 [Installazione dell'agente guest in un WinPE.](#)

2 [Configurazione del file `doagent.bat`.](#)

3 [Configurazione del file `doagentc.bat`.](#)

4 [Configurazione dei file di proprietà dell'agente guest.](#)

Installazione dell'agente guest in un WinPE

È necessario copiare manualmente i file dell'agente guest nell'immagine WinPE.

Prerequisiti

- Selezionare un sistema operativo Windows da cui l'area di staging preparata sia accessibile e su cui siano installati .NET 4.5 e Windows Automated Installation Kit (AIK) per Windows 7 (incluso WinPE 3.0).

- Creare un WinPE.

Procedura

- ◆ Scaricare e installare l'agente guest di vRealize Automation da https://vRealize_VA_Hostname_fqdn/software/index.html.
 - a Scaricare *GugentZip_version* nell'unità C della macchina di riferimento.
Selezionare *GuestAgentInstaller.exe* (32 bit) o *GuestAgentInstaller_x64.exe* (64 bit) a seconda del sistema operativo di cui si dispone.
 - b Fare clic con il pulsante destro del mouse sul file e scegliere **Proprietà**.
 - c Fare clic su **Generale**.
 - d Fare clic su **Sblocca**.
 - e Estrarre i file in C:\.

Verrà creata la directory C:\VRMGuestAgent. Non cambiare il nome di questa directory.

Operazioni successive

[Configurazione del file doagent.bat.](#)

Configurazione del file doagent.bat

È necessario configurare manualmente il file `doagent.bat`.

Prerequisiti

[Installazione dell'agente guest in un WinPE.](#)

Procedura

- 1 Passare alla directory `VRMGuestAgent` all'interno dell'immagine WinPE.
Ad esempio: `C:\Programmi (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Fare una copia del file `doagent-template.bat` e cambiargli il nome in `doagent.bat`.
- 3 Aprire `doagent.bat` in editor di testo.

- 4 Sostituire tutte le ricorrenze della stringa `#Dcac Hostname#` con il nome di dominio completo e il numero di porta dell'host del servizio di gestione di IaaS.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e la porta del bilanciamento del carico relativo al servizio di gestione di IaaS. Ad esempio, <code>manager_service_LB.mycompany.com:443</code>
Senza bilanciamento del carico	Specificare il nome di dominio completo e la porta della macchina su cui è installato il servizio di gestione di IaaS. Ad esempio, <code>manager_service.mycompany.com:443</code>

- 5 Sostituire tutte le ricorrenze della stringa `#Protocol#` con la stringa `/ssl`.
- 6 Sostituire tutte le ricorrenze della stringa `#Comment#` con `REM` (`REM` deve essere seguita da uno spazio finale).
- 7 (Facoltativo) Se si utilizzano certificati autofirmati, rimuovere il commento dal comando `openssl`.

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

- 8 Salvare e chiudere il file.
- 9 Modificare lo script `Startnet.cmd` per WinPE per includere `doagentc.bat` come script personalizzato.

Operazioni successive

[Configurazione del file doagentc.bat.](#)

Configurazione del file doagentc.bat

È necessario configurare manualmente il file `doagentc.bat`.

Prerequisiti

[Configurazione del file doagentc.bat.](#)

Procedura

- 1 Passare alla directory `VRMGuestAgent` all'interno dell'immagine WinPE.
Ad esempio: `C:\Programmi (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Fare una copia del file `doagentsvc-template.bat` e cambiargli il nome in `doagentc.bat`.
- 3 Aprire `doagentc.bat` in editor di testo.
- 4 Rimuovere tutte le ricorrenze della stringa `#Comment#`.

- 5 Sostituire tutte le ricorrenze della stringa `#Dcac Hostname#` con il nome di dominio completo e il numero di porta dell'host del servizio di gestione.

La porta predefinita del servizio di gestione è 443.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	Specificare il nome di dominio completo e la porta del bilanciamento del carico relativo al servizio di gestione. Ad esempio, <code>load_balancer_manager_service.mycompany.com:443</code>
Senza bilanciamento del carico	Specificare il nome di dominio completo e la porta relativi al servizio di gestione. Ad esempio, <code>manager_service.mycompany.com:443</code>

- 6 Sostituire tutte le ricorrenze della stringa `#errorlevel#` con il carattere 1.
- 7 Sostituire tutte le ricorrenze della stringa `#Protocol#` con la stringa `/ssl`.
- 8 Salvare e chiudere il file.

Operazioni successive

[Configurazione dei file di proprietà dell'agente guest.](#)

Configurazione dei file di proprietà dell'agente guest

È necessario configurare manualmente i file delle proprietà dell'agente ospite.

Prerequisiti

[Configurazione del file `doagentc.bat`.](#)

Procedura

- 1 Passare alla directory `VRMGuestAgent` all'interno dell'immagine WinPE.
Ad esempio: `C:\Programmi (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
- 2 Fare una copia del file `gugent.properties` e cambiargli il nome in `gugent.properties.template`.
- 3 Fare una copia del file `gugent.properties.template` e cambiargli il nome in `gugentc.properties`.
- 4 Aprire `gugent.properties` in editor di testo.
- 5 Sostituire tutte le ricorrenze della stringa `GuestAgent.log` con la stringa `X:/VRMGuestAgent/GuestAgent.log`.
- 6 Salvare e chiudere il file.
- 7 Aprire `gugentc.properties` in editor di testo.
- 8 Sostituire tutte le ricorrenze della stringa `GuestAgent.log` con la stringa `C:/VRMGuestAgent/GuestAgent.log`.

9 Salvare e chiudere il file.

Preparazione per il provisioning dell'immagine delle macchine virtuali

Prima del provisioning di istanze con OpenStack, è necessario che nel provider OpenStack siano configurate le immagini e le caratteristiche delle macchine virtuali.

Immagini delle macchine virtuali

Quando si creano blueprint per risorse OpenStack, è possibile selezionare l'immagine di una macchina virtuale da un elenco di immagini disponibili.

Le immagini delle macchine virtuali sono modelli contenenti una configurazione software, che include un sistema operativo. Le immagini delle macchine virtuali sono gestite dal provider di OpenStack e vengono importate durante la raccolta dati.

Se successivamente un'immagine utilizzata in un blueprint viene eliminata dal provider di OpenStack, essa viene anche rimossa dal blueprint. Se da un blueprint vengono rimosse tutte le immagini, il blueprint verrà disattivato e non potrà essere utilizzato per le richieste di macchine finché non lo si modificherà per aggiungere almeno un'immagine.

Caratteristiche di OpenStack

È possibile selezionare una o più caratteristiche quando si creano blueprint di OpenStack.

Le caratteristiche di OpenStack sono modelli hardware virtuali che definiscono le specifiche delle risorse macchine relative a istanze fornite in provisioning in OpenStack. Le caratteristiche sono gestite dal provider di OpenStack e vengono importate durante la raccolta dati.

Preparazione per il provisioning dell'immagine della macchina Amazon

Preparare le immagini e i tipi di istanza della macchina Amazon da sottoporre a provisioning in vRealize Automation.

Le immagini delle macchine Amazon

È possibile selezionare un'immagine della macchina Amazon in un elenco di immagini disponibili al momento della creazione di blueprint di macchine Amazon.

Le immagini delle macchine Amazon sono modelli contenenti una configurazione software, che include un sistema operativo. Sono gestite da account di Amazon Web Services. vRealize Automation gestisce i tipi di istanze disponibili per il provisioning.

Nella regione Amazon devono essere disponibili l'immagine della macchina Amazon e il tipo di istanza. Non tutti i tipi di istanze sono disponibili in tutte le regioni.

È possibile selezionare l'immagine di una macchina Amazon fornita da Amazon Web Services, una community di utenti, o il sito di AWS Marketplace. È possibile anche creare e, facoltativamente, condividere le proprie immagini di macchine Amazon. Una singola immagine di macchina Amazon può essere utilizzata per avviare una o molte istanze.

Le considerazioni elencate di seguito si applicano alle immagini delle macchine Amazon negli account di Amazon Web Services da cui si esegue il provisioning delle macchine cloud:

- Ogni blueprint deve specificare l'immagine di una macchina Amazon.

Un'immagine di macchina Amazon privata è disponibile per un account specifico e tutte le sue regioni. Un'immagine di macchina Amazon pubblica è disponibile per tutti gli account, ma solo per una regione specifica di ciascun account.

- Quando viene creato un blueprint, l'immagine della macchina Amazon specificata viene selezionata dalle regioni di cui sono stati raccolti dati. Se sono disponibili più account di Amazon Web Services, il manager del gruppo di business deve possedere i diritti per tutte le immagini di macchine Amazon private. La regione dell'immagine della macchina Amazon e la posizione dell'utente specificata restringono la richiesta di provisioning alle prenotazioni corrispondenti alla regione e alla posizione.
- Utilizzare le prenotazioni e i criteri per distribuire le immagini delle macchine Amazon nei propri account di Amazon Web Services. Utilizzare i criteri per restringere il provisioning da un blueprint a un set di prenotazioni particolare.
- vRealize Automation non può creare account utente su una macchina cloud. La prima volta che il proprietario di una macchina si connette a una macchina cloud, deve accedere come amministratore e aggiungere le proprie credenziali utente di vRealize Automation, o deve farlo un amministratore al suo posto. Il proprietario può accedere utilizzando le proprie credenziali di utente vRealize Automation.

Se l'immagine della macchina Amazon genera la password di amministratore a ogni avvio, la password è mostrata nella pagina Edit Machine Record. In caso contrario, è possibile trovare la password nell'account di Amazon Web Services. È possibile configurare tutte le immagini delle macchine Amazon per generare la password di amministratore a ogni avvio. È possibile anche fornire informazioni sulla password di amministratore per supportare utenti che eseguono il provisioning di macchine per altri utenti.

- Per consentire delle richieste di Microsoft Windows Management Instrumentation (WMI) su macchine cloud con provisioning in account Amazon Web Services, abilitare un agente di Microsoft Windows Remote Management (WinRM) al fine di raccogliere dati da macchine Windows gestite da vRealize Automation. Vedere *Installazione di vRealize Automation*.
- Un'immagine di macchina Amazon privata può essere visualizzata in diversi tenant.

Per informazioni correlate, consultare gli argomenti riguardanti *Amazon Machine Images (AMI)* nella documentazione di Amazon.

I tipi di istanze di Amazon

Un architetto IaaS seleziona uno o più tipi di istanze di Amazon durante la creazione dei blueprint Amazon EC2. Un amministratore IaaS può aggiungere o rimuovere i tipi di istanze per controllare le opzioni disponibili per gli architetti.

Un'istanza Amazon EC2 è un server virtuale che può eseguire applicazioni in Amazon Web Services. Le istanze vengono create dall'immagine di una macchina Amazon e scegliendo un tipo di istanza appropriato.

Per eseguire il provisioning di una macchina in un account Amazon Web Services, all'immagine di Amazon specificata viene applicato un tipo di istanza. I tipi di istanze disponibili vengono elencati quando gli architetti creano il blueprint Amazon EC2. Gli architetti selezionano uno o più tipi di istanze, che a questo punto diventano opzioni disponibili per l'utente quando richiede il provisioning di una macchina. I tipi di istanza devono essere supportati nella regione designata.

Per informazioni correlate, consultare gli argomenti riguardanti *la selezione dei tipi di istanze e i dettagli relativi alle istanze Amazon EC2* nella documentazione di Amazon.

Aggiunta di un tipo di istanza Amazon

vRealize Automation include diversi tipi di istanza da utilizzare con i blueprint Amazon. Un amministratore può aggiungere e rimuovere i tipi di istanza.

I tipi di istanza della macchina gestiti dagli amministratori IaaS sono disponibili per gli architetti dei blueprint durante la creazione o la modifica di un blueprint Amazon. Le immagini e i tipi di istanza delle macchine Amazon vengono rese disponibili tramite il prodotto Amazon Web Services.

Prerequisiti

Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Fare clic su **Infrastruttura > Amministrazione > Tipi di istanze**.
- 2 Fare clic su **Nuovo**.
- 3 Aggiungere un nuovo tipo di istanza, specificando i parametri seguenti.

Le informazioni sui tipi di istanza di Amazon disponibili e sui valori delle impostazioni che è possibile specificare per questi parametri sono contenute nella documentazione di Amazon Web Services in *Tipi di istanze di Amazon EC2 - Amazon Web Services (AWS)* all'indirizzo <https://aws.amazon.com/it/ec2/> e in *Tipi di istanze* all'indirizzo <http://aws.amazon.com/it/documentation/>.

- Nome
- Nome API
- Nome tipo
- Nome prestazioni I/O
- CPU
- Memoria (GB)
- Storage (GB)
- Unità di elaborazione

4 Fare clic sull'icona **Salva** (.

Risultati

Quando gli architetti di IaaS creano i blueprint di Amazon Web Services, possono utilizzare i tipi di istanze personalizzati.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Scenario: preparazione di risorse vSphere per il provisioning di macchine

Un amministratore di vSphere, che ha tra i suoi compiti quello della creazione di modelli per vRealize Automation, utilizzerà il client Web di vSphere per preparare la clonazione di macchine CentOS in vRealize Automation.

Si desidera convertire una macchina di riferimento CentOS esistente in un modello di vSphere in modo da consentire anche agli architetti di creare blueprint per la clonazione di macchine CentOS in vRealize Automation. Per evitare qualsiasi conflitto che può derivare dalla distribuzione di più macchine virtuali con impostazioni identiche, è preferibile creare anche una specifica di personalizzazione generale, utilizzabile anche dagli architetti, per creare blueprint di cloni per modelli Linux.

Prerequisiti

Identificare o creare una macchina di riferimento Linux CentOS con i VMware Tools installati. Includere almeno una scheda di rete per fornire connettività a Internet.

Procedura

1 [Scenario: conversione della macchina di riferimento CentOS in un modello per Rainpole](#)

Utilizzando il vSphere Client, è possibile convertire la macchina di riferimento CentOS esistente in un modello vSphere a cui gli architetti di IaaS di vRealize Automation possono fare riferimento come base per i propri blueprint di cloni.

2 [Scenario: creazione di una specifica di personalizzazione per la clonazione di macchine Linux](#)

Utilizzando vSphere Client, è possibile creare una specifica di personalizzazione standard utilizzabile dagli architetti di IaaS di vRealize Automation quando creano blueprint di cloni per macchine Linux.

Scenario: conversione della macchina di riferimento CentOS in un modello per Rainpole

Utilizzando il vSphere Client, è possibile convertire la macchina di riferimento CentOS esistente in un modello vSphere a cui gli architetti di IaaS di vRealize Automation possono fare riferimento come base per i propri blueprint di cloni.

Procedura

- 1 Accedere alla macchina di riferimento come utente root e preparare la macchina per la conversione.

- a Rimuovere le regole di persistenza di udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Abilitare la macchina clonata da questo modello ad avere i propri identificatori unici.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Spegner la macchina.

```
shutdown -h now
```

- 2 Accedere al client Web di vSphere come amministratore.
- 3 Fare clic sulla scheda **Opzioni VM**.
- 4 Fare clic con il pulsante destro del mouse sulla macchina di riferimento e scegliere **Modifica impostazioni**.
- 5 Immettere **Rainpole_centos_63_x86** nella casella di testo **Nome VM**.
- 6 Anche se la macchina di riferimento ha un sistema operativo guest CentOS, selezionare **Red Hat Enterprise Linux 6 (64-bit)** dal menu a discesa **Versione sistema operativo guest**.
Se si seleziona CentOS, il modello e la specifica di personalizzazione potrebbero non funzionare come previsto.
- 7 Fare clic con il pulsante destro del mouse sulla macchina di riferimento **Rainpole_centos_63_x86** nel client Web di vSphere e scegliere **Modello > Converti in modello**.

Risultati

vCenter Server contrassegna la macchina di riferimento Rainpole_centos_63_x86 come modello e visualizza l'attività nel riquadro Attività recenti.

Operazioni successive

Per evitare qualsiasi conflitto che può derivare dalla distribuzione di più macchine virtuali con impostazioni identiche, è preferibile creare una specifica di personalizzazione generale, utilizzabile anche dagli architetti, per creare blueprint di cloni per modelli Linux.

Scenario: creazione di una specifica di personalizzazione per la clonazione di macchine Linux

Utilizzando vSphere Client, è possibile creare una specifica di personalizzazione standard utilizzabile dagli architetti di IaaS di vRealize Automation quando creano blueprint di cloni per macchine Linux.

Procedura

- 1 Dalla pagina Home, fare clic su **Gestione specifiche personalizzazione** per aprire la procedura guidata.
- 2 Fare clic sull'icona **Nuovo**.
- 3 Specificare le proprietà.
 - a Selezionare **Linux** dal menu a discesa **Sistema operativo VM destinazione**.
 - b Immettere **Linux** nella casella di testo **Nome specifica personalizzazione**.
 - c Immettere **Rainpole Linux cloning with vRealize Automation** nella casella di testo **Descrizione**.
 - d Fare clic su **Avanti**.
- 4 Impostare il nome del computer.
 - a Selezionare **Usa nome macchina virtuale**.
 - b Specificare il dominio su cui eseguire il provisioning delle macchine clonate nella casella di testo **Nome dominio**.
 - c Fare clic su **Avanti**.
- 5 Configurare le impostazioni relative all'ora locale.
- 6 Fare clic su **Avanti**.
- 7 Selezionare **Usa impostazioni di rete standard per il sistema operativo guest, inclusa l'attivazione di DHCP su tutte le interfacce di rete**.
- 8 Seguire le istruzioni presentate per inserire le informazioni richieste rimanenti.
- 9 Nella pagina **Completamento**, rivedere le selezioni e fare clic su **Fine**.

Preparazione per il provisioning Software

Utilizzare Software per distribuire le applicazioni e il middleware come parte del processo di provisioning di vRealize Automation per le macchine vSphere, vCloud Director, vCloud Air, Amazon Web Services e Microsoft Azure.

È possibile distribuire Software sulle macchine se il blueprint supporta Software e se si installa l'agente guest e l'agente bootstrap del software sulle macchine di riferimento prima di convertirle in modelli, snapshot o immagini della macchina.

Per informazioni relative all'indicazione delle porte durante la preparazione per il provisioning delle macchine, vedere il file PDF *Architettura di riferimento* nella [documentazione del prodotto di vRealize Automation](#).

Tabella 1-17. Metodi di provisioning che supportano Software

Tipo di macchina	Preparazione
vSphere	Un blueprint clone esegue il provisioning di una macchina virtuale completa e indipendente in base a un modello di macchina virtuale vCenter Server. Se si desidera che i modelli per la clonazione supportino i componenti Software, installare l'agente guest e l'agente bootstrap del software sulla macchina di riferimento mentre si prepara un modello per la clonazione. Vedere Elenco di controllo per la preparazione al provisioning tramite clonazione .
vSphere	Un blueprint di un clone collegato esegue il provisioning di una copia con ottimizzazione dello spazio di una macchina vSphere basata su uno snapshot, utilizzando una catena di dischi delta per tenere traccia delle differenze rispetto alla macchina padre. Se si desidera che i blueprint clone collegati supportino i componenti Software, installare l'agente guest e l'agente bootstrap del software sulla macchina prima di creare lo snapshot. Se la macchina snapshot è stata clonata da un modello che supporta Software, gli agenti necessari sono già installati.
vCloud Director	Un blueprint clone esegue il provisioning di una macchina virtuale completa e indipendente in base a un modello di macchina virtuale vCenter Server. Se si desidera che i modelli per la clonazione supportino i componenti Software, installare l'agente guest e l'agente bootstrap del software sulla macchina di riferimento mentre si prepara un modello per la clonazione. Vedere Elenco di controllo per la preparazione al provisioning tramite clonazione .
vCloud Air	Un blueprint clone esegue il provisioning di una macchina virtuale completa e indipendente in base a un modello di macchina virtuale vCenter Server. Se si desidera che i modelli per la clonazione supportino i componenti Software, installare l'agente guest e l'agente bootstrap del software sulla macchina di riferimento mentre si prepara un modello per la clonazione. Vedere Elenco di controllo per la preparazione al provisioning tramite clonazione .
Amazon Web Services	Le immagini delle macchine Amazon sono modelli contenenti una configurazione software, che include un sistema operativo. Se si desidera creare un'immagine di una macchina Amazon che supporti Software, connettersi a un'istanza di Amazon Web Services in esecuzione che utilizza un volume EBS per il dispositivo radice. Installare l'agente guest e l'agente bootstrap del software sulla macchina di riferimento, quindi creare un'immagine della macchina Amazon dalla propria istanza. Perché l'agente guest e l'agente bootstrap di Software funzionino sulle macchine con provisioning, è necessario configurare la connettività tra rete e VPC. Per informazioni sulla creazione di immagini AMI con supporto Amazon EBS, vedere la documentazione di Amazon Web Services.
Microsoft Azure	Per informazioni, vedere la documentazione del prodotto di Impostazioni dei componenti Software , Creazione di un blueprint per Microsoft Azure e Microsoft Azure.

Preparazione per il provisioning delle macchine con Software

Per supportare i componenti di Software, è necessario installare l'agente guest e l'agente bootstrap di Software sulla macchina di riferimento prima di convertire un modello per la clonazione, creare un'immagine della macchina Amazon oppure creare uno snapshot.

Preparazione di una macchina di riferimento Windows per il supporto di Software

Utilizzare un singolo script per installare Java Runtime Environment, l'agente guest e l'agente bootstrap Software in una macchina di riferimento Windows. Dalla macchina di riferimento, è possibile creare un modello per la clonazione, uno snapshot o un'immagine della macchina Amazon che supporti i componenti Software.

Software supporta l'esecuzione di script con Windows CMD e PowerShell 2.0.

Importante Il processo di avvio non deve essere interrotto. Configurare la macchina virtuale in modo che il processo di avvio della macchina virtuale non venga interrotto prima della richiesta di accesso. Ad esempio, verificare che nessun processo o script richieda l'interazione dell'utente all'avvio della macchina virtuale.

Prerequisiti

- Identificare o creare una macchina di riferimento Windows.
- Stabilire l'attendibilità sicura tra la macchina di riferimento e l'host del servizio di gestione di IaaS. Vedere [Configurare l'agente guest in modo che consideri attendibile un server..](#)
- Se si prevede di accedere in remoto alla macchina per la risoluzione dei problemi o per altri motivi, installare i servizi RDS (Remote Desktop Services).
- Rimuovere gli elementi della configurazione di rete dai relativi file di configurazione.

Procedura

- 1 Accedere al server di riferimento Windows come amministratore.
- 2 Aprire un browser alla pagina di download del software nell'appliance vRealize Automation.
`https://vrealize-automation-appliance-FQDN/software`
- 3 Salvare il modello ZIP nel server Windows.
`prepare_vra_template_windows.zip`
- 4 Estrarre il contenuto del file ZIP in una cartella ed eseguire il file batch.
`.\prepare_vra_template.bat`
- 5 Seguire le istruzioni visualizzate.
- 6 Al termine, arrestare la macchina virtuale Windows.

Risultati

Lo script rimuove qualsiasi guest o agente bootstrap Software precedente e installa le versioni supportate di Java Runtime Environment, dell'agente guest e dell'agente bootstrap Software.

Operazioni successive

Convertire la macchina di riferimento in un modello per la clonazione, uno snapshot o un'immagine della macchina Amazon. Ciascuno supporta i componenti Software e i progettisti di infrastrutture possono usarli quando creano blueprint.

Preparazione di una macchina di riferimento Linux per il supporto di Software

Utilizzare un singolo script per installare Java Runtime Environment, l'agente guest e l'agente bootstrap Software in una macchina di riferimento Linux. Dalla macchina di riferimento, è possibile creare un modello per la clonazione, uno snapshot o un'immagine della macchina Amazon che supporti i componenti Software.

Software supporta l'esecuzione di script con Bash.

Importante Il processo di avvio non deve essere interrotto. Configurare la macchina virtuale in modo che il processo di avvio della macchina virtuale non venga interrotto prima della richiesta di accesso. Ad esempio, verificare che nessun processo o script richieda l'interazione dell'utente all'avvio della macchina virtuale.

Prerequisiti

- Identificare o creare una macchina di riferimento Linux.
- Verificare che i seguenti comandi siano disponibili, in base al sistema Linux installato:
 - `yum` o `apt-get`
 - `wget` o `curl`
 - `python`
 - `dmidecode` come richiesto dal provider di servizi cloud
 - Requisiti comuni quali `sed`, `awk`, `perl`, `chkconfig`, `unzip` e `grep` in base alla distribuzione Linux

È inoltre possibile utilizzare un editor per controllare lo script `prepare_vra_template.sh` scaricato, che espone i comandi che utilizza.

- Se si prevede di accedere in remoto alla macchina per la risoluzione dei problemi o per altri motivi, installare OpenSSH.
- Rimuovere gli elementi della configurazione di rete dai relativi file di configurazione.

Procedura

- 1 Accedere alla macchina di riferimento come root.
- 2 Scaricare il pacchetto tar.gz del modello dall'appliance vRealize Automation.

```
wget https://vrealize-automation-appliance-FQDN/software/download/
prepare_vra_template_linux.tar.gz
```

Se l'ambiente utilizza certificati autofirmati, potrebbe essere necessaria l'opzione `--no-check-certificate`.

```
wget --no-check-certificate https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template_linux.tar.gz
```

3 Decomprimere il pacchetto.

```
tar -xvf prepare_vra_template_linux.tar.gz
```

4 Nell'output di decompressione, individuare lo script del programma di installazione e impostarlo come file eseguibile.

```
chmod +x prepare_vra_template.sh
```

5 Eseguire lo script del programma di installazione.

```
./prepare_vra_template.sh
```

Per informazioni sulle opzioni non interattive e i valori previsti, vedere la guida dello script.

```
./prepare_vra_template.sh --help
```

6 Seguire le istruzioni visualizzate.

Al completamento dell'installazione, viene visualizzato un messaggio di conferma. Se vengono visualizzati errori e registri, risolvere gli errori ed eseguire di nuovo lo script.

7 Al termine, arrestare la macchina virtuale Linux.

Risultati

Lo script rimuove qualsiasi guest o agente bootstrap Software precedente e installa le versioni supportate di Java Runtime Environment, dell'agente guest e dell'agente bootstrap Software.

Operazioni successive

Nell'hypervisor o nel provider di cloud, convertire la macchina di riferimento in un modello per la clonazione, uno snapshot o un'immagine della macchina Amazon. Ciascuno supporta i componenti Software e i progettisti di infrastrutture possono usarli quando creano blueprint.

Aggiornamento dei modelli di macchine virtuali esistenti in vRealize Automation

Se si stanno aggiornando i modelli, le immagini delle macchine Amazon o gli snapshot per la versione più recente dell'agente di avvio automatico di Software per Windows, oppure se si sta effettuando l'aggiornamento manuale all'agente di avvio automatico di Software per Linux più recente invece di utilizzare lo script `prepare_vra_template.sh`, è necessario rimuovere qualsiasi versione esistente ed eliminare tutti i registri.

Linux

Per le macchine di riferimento Linux, l'esecuzione dello script `prepare_vra_template.sh` consente di reimpostare l'agente e di rimuovere tutti i registri prima della reinstallazione. Tuttavia, se si intende eseguire un'installazione manuale, è necessario accedere alla macchina di riferimento come utente root ed eseguire il comando per reimpostare e rimuovere gli elementi.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

Windows

Per le macchine di riferimento Windows, occorre rimuovere l'agente di avvio automatico di Software esistente e l'agente guest di vRealize Automation 6.0 o versione successiva, nonché eliminare tutti i file di registro di runtime esistenti. In una finestra di comando PowerShell, eseguire i comandi per rimuovere agente ed elementi.

```
c:\opt\vmware-appdirector\agent-bootstrap\appd_bootstrap_removal.bat
```

Preparazione di un modello di vSphere per clonare blueprint di componenti software e macchine

Un amministratore di vCenter Server desidera preparare un modello di vSphere che gli architetti di vRealize Automation possano utilizzare per clonare ad esempio macchine Linux CentOS. Per assicurarsi che il modello supporti i componenti software dei blueprint, installare l'agente guest e l'agente di avvio automatico software prima di convertire la macchina di riferimento in un modello.

Prerequisiti

- Identificare o creare una macchina di riferimento Linux CentOS con i VMware Tools installati. Includere almeno una scheda di rete per fornire connettività a Internet nel caso in cui gli architetti di blueprint non aggiungano questa funzionalità al livello dei blueprint. Per informazioni sulla creazione di istanze di macchine virtuali, vedere la documentazione di vSphere.
- È necessario essere connessi a un vCenter Server per convertire una macchina virtuale in un modello. Non è possibile creare modelli se si connette il client di vSphere direttamente a un host vSphere ESXi.

Procedura

1 [Scenario: preparazione della macchina di riferimento per le personalizzazioni dell'agente guest e i componenti software](#)

Affinché il modello possa supportare i componenti software, è necessario installare l'agente di avvio automatico software e il relativo prerequisito, l'agente guest, sulla propria macchina di riferimento. Gli agenti assicurano che gli architetti di vRealize Automation che utilizzano il modello possano includere i componenti software nei loro blueprint.

2 Scenario: conversione della macchina di riferimento CentOS in un modello

Dopo aver installato l'agente guest e l'agente di bootstrap software sulla macchina di riferimento, si procede convertendo la macchina di riferimento in un modello utilizzabile dagli architetti di vRealize Automation per creare blueprint di macchine clone.

3 Scenario: creazione di una specifica di personalizzazione per la clonazione di vSphere

Creare una specifica di personalizzazione che gli architetti dei blueprint potranno utilizzare con il proprio modello `cpb_centos_63_x84`.

Risultati

È stato creato un modello e una specifica di personalizzazione dalla macchina di riferimento che gli architetti di blueprint possono utilizzare per creare blueprint di vRealize Automation che clonano macchine Linux CentOS. Grazie all'installazione dell'agente di avvio automatico di Software e dell'agente guest sulla macchina di riferimento, gli architetti possono utilizzare il modello per creare blueprint di voci di catalogo elaborati che includono componenti Software o altre personalizzazioni di agenti guest, come l'esecuzione di script o la formattazione di dischi. Grazie all'installazione di VMware Tools, gli architetti e gli amministratori di catalogo possono permettere agli utenti di eseguire azioni sulle macchine quali riconfigurazioni, snapshot e riavvii.

Operazioni successive

Dopo aver configurato utenti, gruppi e risorse di vRealize Automation, è possibile utilizzare il modello e la specifica di personalizzazione per creare un blueprint di macchine per la clonazione. Vedere [Configurazione del blueprint di una macchina](#).

Scenario: preparazione della macchina di riferimento per le personalizzazioni dell'agente guest e i componenti software

Affinché il modello possa supportare i componenti software, è necessario installare l'agente di avvio automatico software e il relativo prerequisito, l'agente guest, sulla propria macchina di riferimento. Gli agenti assicurano che gli architetti di vRealize Automation che utilizzano il modello possano includere i componenti software nei loro blueprint.

Per semplificare il processo, scaricare ed eseguire uno script di vRealize Automation che installa entrambi gli agenti invece di scaricare e installare pacchetti separati.

Lo script inoltre si connette all'istanza del servizio di gestione e scarica il certificato SSL necessario per stabilire la relazione di fiducia tra il servizio di gestione e le macchine distribuite dal modello. Si tenga presente che scaricare il certificato tramite lo script è tuttavia meno sicuro rispetto alla procedura che prevede di richiedere manualmente il certificato SSL del servizio di gestione e installarlo sulla macchina di riferimento in `/usr/share/gugent/cert.pem`.

Procedura

- 1 Aprire un browser alla pagina del software dell'appliance vRealize Automation.

<https://vrealize-automation-appliance-FQDN/software>

- 2 In Linux Software Installers, scaricare il file tar compresso con GZip.

```
prepare_vra_template_linux.tar.gz
```

- 3 Trasferire il file tar in una directory temporanea nella macchina di riferimento Linux.

Per trasferire il file, è possibile eseguire uno strumento come WinSCP o utilizzare qualsiasi altro metodo con cui si ha familiarità.

- 4 Accedere come root al prompt dei comandi nella macchina di riferimento Linux.

Per aprire un terminale, è possibile avviare Remote Console sulla macchina da vRealize Automation oppure utilizzare qualsiasi altro metodo con cui si ha familiarità.

- 5 Dalla directory temporanea, estrarre il file tar.

```
gunzip prepare_vra_template_linux.tar.gz
```

- 6 Estrarre il contenuto del file tar.

```
tar xvf prepare_vra_template_linux.tar
```

- 7 Passare alla directory dello script.

```
cd prepare_vra_template_linux
```

- 8 Eseguire lo script e seguire le istruzioni visualizzate.

```
./prepare_vra_template.sh
```

Per informazioni non interattive sulle opzioni e i valori, immettere ./prepare_vra_template.sh --help.

Risultati

Al termine dell'installazione viene visualizzato un messaggio di conferma. Se vengono visualizzati messaggi e registri di errore, correggere i problemi ed eseguire di nuovo lo script.

Scenario: conversione della macchina di riferimento CentOS in un modello

Dopo aver installato l'agente guest e l'agente di bootstrap software sulla macchina di riferimento, si procede convertendo la macchina di riferimento in un modello utilizzabile dagli architetti di vRealize Automation per creare blueprint di macchine clone.

Dopo aver convertito la macchina di riferimento in un modello, non sarà possibile modificare o accendere il modello senza prima averlo riconvertito in una macchina virtuale.

Procedura

- 1 Accedere alla macchina di riferimento come utente root e preparare la macchina per la conversione.

- a Rimuovere le regole di persistenza di udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- b Abilitare la macchina clonata da questo modello ad avere i propri identificatori unici.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- c Se la macchina di riferimento è stata riavviata o riconfigurata dopo l'installazione dell'agente di avvio automatico software, reimpostare l'agente.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- d Spegner la macchina.

```
shutdown -h now
```

- 2 Accedere al client Web di vSphere come amministratore.
- 3 Fare clic con il pulsante destro del mouse sulla macchina di riferimento e scegliere **Modifica impostazioni**.
- 4 Immettere **cpb_centos_63_x84** nella casella di testo **Nome macchina virtuale**.
- 5 Anche se la macchina di riferimento ha un sistema operativo guest CentOS, selezionare **Red Hat Enterprise Linux 6 (64-bit)** dal menu a discesa **Versione sistema operativo guest**.
Se si seleziona CentOS, il modello e la specifica di personalizzazione potrebbero non funzionare come previsto.
- 6 Fare clic con il pulsante destro del mouse sulla macchina di riferimento nel client Web di vSphere e scegliere **Modello > Converti in modello**.

Risultati

vCenter Server contrassegna la macchina di riferimento cpb_centos_63_x84 come modello e visualizza l'attività nel riquadro Attività recenti. Se l'ambiente vSphere è già stato trasferito sotto la gestione di vRealize Automation, il modello viene rilevato nel corso della successiva raccolta dati automatica. Se vRealize Automation non è stato ancora configurato, il modello viene riconosciuto durante il processo di configurazione.

Scenario: creazione di una specifica di personalizzazione per la clonazione di vSphere

Creare una specifica di personalizzazione che gli architetti dei blueprint potranno utilizzare con il proprio modello cpb_centos_63_x84.

Procedura

- 1 Accedere al client Web di vSphere come amministratore.
- 2 Dalla pagina Home, fare clic su **Gestione specifiche personalizzazione** per aprire la procedura guidata.
- 3 Fare clic sull'icona **Nuovo**.
- 4 Fare clic sull'icona **Nuovo**.
- 5 Specificare le proprietà.
 - a Selezionare **Linux** dal menu a discesa **Sistema operativo VM destinazione**.
 - b Immettere **Customspecs** nella casella di testo **Nome specifica personalizzazione**.
 - c Immettere **cpb_centos_63_x84 cloning with vRealize Automation** nella casella di testo **Descrizione**.
 - d Fare clic su **Avanti**.
- 6 Impostare il nome del computer.
 - a Selezionare **Usa nome macchina virtuale**.
 - b Specificare il dominio su cui eseguire il provisioning delle macchine clonate nella casella di testo **Nome dominio**.
 - c Fare clic su **Avanti**.
- 7 Configurare le impostazioni relative all'ora locale.
- 8 Fare clic su **Avanti**.
- 9 Selezionare **Usa impostazioni di rete standard per il sistema operativo guest, inclusa l'attivazione di DHCP su tutte le interfacce di rete**.
 Amministratori di struttura e architetti dell'infrastruttura possono gestire le impostazioni di rete relative alle macchine di cui è stato eseguito il provisioning creando e utilizzando profili di rete in vRealize Automation.
- 10 Seguire le istruzioni presentate per inserire le informazioni richieste rimanenti.
- 11 Nella pagina **Completamento**, rivedere le selezioni e fare clic su **Fine**.

Risultati

Scenario: preparazione per l'importazione di Dukes Bank per il blueprint dell'applicazione campione di vSphere

Un amministratore di vCenter Server procede alla preparazione di un modello Linux CentOS 6.x di vSphere e di una specifica di personalizzazione da utilizzare per il provisioning dell'applicazione campione Dukes Bank di vRealize Automation.

Per assicurarsi che il modello supporti i componenti software dell'applicazione campione, installare l'agente guest e l'agente di avvio automatico software sulla macchina di riferimento Linux prima di convertirla in un modello e creare una specifica di personalizzazione. Per disattivare SELinux sulla macchina di riferimento per assicurarsi che il modello supporti l'implementazione specifica di MySQL utilizzata nell'applicazione campione Dukes Bank.

Prerequisiti

- Identificare o creare una macchina di riferimento Linux CentOS 6.x con i VMware Tools installati. Per informazioni sulla creazione di istanze di macchine virtuali, vedere la documentazione di vSphere.
- È necessario essere connessi a un vCenter Server per convertire una macchina virtuale in un modello. Non è possibile creare modelli se si connette il client di vSphere direttamente a un host vSphere ESXi.

Procedura

1 Scenario: preparazione della macchina di riferimento per l'applicazione campione Dukes Bank di vSphere

Il supporto del modello per l'applicazione campione Dukes Bank richiede l'installazione sia dell'agente guest che dell'agente di avvio automatico software sulla macchina di riferimento, per consentire a vRealize Automation di eseguire il provisioning dei componenti software. Per semplificare il processo, scaricare ed eseguire uno script di vRealize Automation che installa sia l'agente guest che l'agente di avvio automatico software invece di scaricare e installare separatamente i pacchetti.

2 Scenario: conversione della macchina di riferimento in un modello per l'applicazione campione Dukes Bank di vSphere

Dopo aver installato l'agente guest e l'agente di avvio automatico software nella macchina di riferimento, disattivare SELinux per assicurarsi che il modello supporti l'implementazione specifica di MySQL utilizzata nell'applicazione campione Dukes Bank. È possibile convertire la macchina di riferimento in un modello che è possibile utilizzare per il provisioning dell'applicazione campione Dukes Bank di vSphere.

3 Scenario: creazione di una specifica personalizzata per la clonazione delle macchine dell'applicazione campione Dukes Bank di vSphere

È necessario creare una specifica di personalizzazione da utilizzare con il modello della macchina di Dukes Bank.

Risultati

È stato creato un modello e una specifica di personalizzazione dalla macchina di riferimento con il supporto per l'applicazione campione Dukes Bank di vRealize Automation.

Scenario: preparazione della macchina di riferimento per l'applicazione campione Dukes Bank di vSphere

Il supporto del modello per l'applicazione campione Dukes Bank richiede l'installazione sia dell'agente guest che dell'agente di avvio automatico software sulla macchina di riferimento, per consentire a vRealize Automation di eseguire il provisioning dei componenti software. Per semplificare il processo, scaricare ed eseguire uno script di vRealize Automation che installa sia l'agente guest che l'agente di avvio automatico software invece di scaricare e installare separatamente i pacchetti.

Procedura

- 1 Accedere alla macchina di riferimento come utente root.
- 2 Scaricare lo script di installazione dall'appliance vRealize Automation.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Se l'ambiente utilizza certificati autofirmati, potrebbe essere necessario utilizzare l'opzione di `wget --no-check-certificate`. Ad esempio:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

- 3 Rendere eseguibile lo script `prepare_vra_template.sh`.

```
chmod +x prepare_vra_template.sh
```

- 4 Eseguire lo script d'installazione `prepare_vra_template.sh`.

```
./prepare_vra_template.sh
```

È possibile eseguire il comando `./prepare_vra_template.sh --help` per informazioni sulle opzioni non interattive e sui valori previsti.

- 5 Seguire le istruzioni presentate per completare l'installazione.

Il completamento dell'installazione viene segnalato da un messaggio di conferma. Se compaiono messaggi di errore e registri nella console, risolvere gli errori ed eseguire nuovamente lo script d'installazione.

Risultati

L'installazione dell'agente di avvio automatico software e del suo prerequisito, ovvero dell'agente guest, consente all'applicazione campione Dukes Bank di eseguire correttamente il provisioning dei componenti software. Lo script inoltre connette all'istanza del servizio di gestione e scarica il certificato SSL necessario per stabilire la relazione di fiducia tra il servizio di gestione e le macchine distribuite dal modello. Questo approccio è meno sicuro rispetto all'ottenimento del certificato SSL del servizio di gestione e alla sua installazione manuale nella macchina di riferimento in `/usr/share/gugent/cert.pem` ed è possibile sostituire subito manualmente questo certificato se la sicurezza è un requisito importante.

Scenario: conversione della macchina di riferimento in un modello per l'applicazione campione Dukes Bank di vSphere

Dopo aver installato l'agente guest e l'agente di avvio automatico software nella macchina di riferimento, disattivare SELinux per assicurarsi che il modello supporti l'implementazione specifica di MySQL utilizzata nell'applicazione campione Dukes Bank. È possibile convertire la macchina di riferimento in un modello che è possibile utilizzare per il provisioning dell'applicazione campione Dukes Bank di vSphere.

Dopo aver convertito la macchina di riferimento in un modello, non sarà possibile modificare o accendere il modello senza prima averlo riconvertito in una macchina virtuale.

Procedura

- 1 Accedere alla macchina di riferimento come utente root.

- a Modificare il file `/etc/selinux/config` disattivare SELinux.

```
SELINUX=disabled
```

Se non si disattiva SELinux, il componente software MySQL dell'applicazione campione Duke's Bank potrebbe non funzionare come previsto.

- b Rimuovere le regole di persistenza di udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- c Abilitare la macchina clonata da questo modello ad avere i propri identificatori unici.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- d Se la macchina di riferimento è stata riavviata o riconfigurata dopo l'installazione dell'agente di avvio automatico software, reimpostare l'agente.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- e Spegnerla la macchina.

```
shutdown -h now
```

- 2 Accedere al client Web di vSphere come amministratore.
- 3 Fare clic con il pulsante destro del mouse sulla macchina di riferimento e scegliere **Modifica impostazioni**.
- 4 Immettere **dukes_bank_template** nella casella di testo **Nome VM**.
- 5 Se la macchina di riferimento ha un sistema operativo guest CentOS, selezionare **Red Hat Enterprise Linux 6 (64-bit)** dal menu a discesa **Versione sistema operativo guest**.

Se si seleziona CentOS, il modello e la specifica di personalizzazione potrebbero non funzionare come previsto.

- 6 Fare clic su **OK**.
- 7 Fare clic con il pulsante destro del mouse sulla macchina di riferimento nel client Web di vSphere e scegliere **Modello > Converti in modello**.

Risultati

vCenter Server contrassegna la macchina di riferimento dukes_bank_template come modello e visualizza l'attività nel riquadro Attività recenti. Se l'ambiente vSphere è già stato trasferito sotto la gestione di vRealize Automation, il modello viene rilevato nel corso della successiva raccolta dati automatica. Se vRealize Automation non è stato ancora configurato, il modello viene riconosciuto durante il processo di configurazione.

Scenario: creazione di una specifica personalizzata per la clonazione delle macchine dell'applicazione campione Dukes Bank di vSphere

È necessario creare una specifica di personalizzazione da utilizzare con il modello della macchina di Dukes Bank.

Procedura

- 1 Accedere al client Web di vSphere come amministratore.
- 2 Dalla pagina Home, fare clic su **Gestione specifiche personalizzazione** per aprire la procedura guidata.
- 3 Fare clic sull'icona **Nuovo**.
- 4 Specificare le proprietà.
 - a Selezionare **Linux** dal menu a discesa **Sistema operativo VM destinazione**.
 - b Immettere **Customspecs_sample** nella casella di testo **Nome specifica personalizzazione**.
 - c Immettere **Dukes Bank customization spec** nella casella di testo **Descrizione**.
 - d Fare clic su **Avanti**.
- 5 Impostare il nome del computer.
 - a Selezionare **Usa nome macchina virtuale**.
 - b Specificare il dominio cui eseguire il provisioning dell'applicazione campione Dukes Bank nella casella di testo **Nome dominio**.
 - c Fare clic su **Avanti**.
- 6 Configurare le impostazioni relative all'ora locale.
- 7 Fare clic su **Avanti**.

8 Selezionare **Usa impostazioni di rete standard per il sistema operativo guest, inclusa l'attivazione di DHCP su tutte le interfacce di rete.**

Amministratori di struttura e architetti dell'infrastruttura possono gestire le impostazioni di rete relative alle macchine di cui è stato eseguito il provisioning creando e utilizzando profili di rete in vRealize Automation.

9 Seguire le istruzioni presentate per inserire le informazioni richieste rimanenti.

10 Nella pagina **Completamento**, rivedere le selezioni e fare clic su **Fine**.

Risultati

È stato creato un modello e una specifica di personalizzazione che è possibile utilizzare per il provisioning dell'applicazione campione Dukes Bank.

Operazioni successive

- 1 Creare un profilo di rete esterna per fornire un gateway e un intervallo di indirizzi IP. Vedere [Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti](#).
- 2 Mappare il profilo di rete esterno sulla prenotazione vSphere. Vedere [Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer](#). L'applicazione campione non può eseguire correttamente il provisioning senza un profilo di rete esterna.
- 3 Importare l'applicazione campione Dukes Bank nell'ambiente. Vedere [Scenario: importazione di Dukes Bank per l'applicazione campione di vSphere e configurazione dell'ambiente](#).

Preparazione di tenant e risorse per il provisioning dei blueprint

2

È possibile configurare ambienti tenant multipli, ognuno con i propri gruppi di utenti e accesso univoco alle risorse poste sotto la gestione di vRealize Automation.

Questo capitolo include i seguenti argomenti:

- [Configurazione delle impostazioni del tenant](#)
- [Configurazione delle risorse](#)
- [Preferenze utente per notifiche e delegati](#)

Configurazione delle impostazioni del tenant

Gli amministratori tenant configurano le impostazioni del tenant, ad esempio l'autenticazione utente, e gestiscono i ruoli utente e i gruppi di business. Gli amministratori di sistema e gli amministratori tenant configurano opzioni quali i server email per la gestione delle notifiche e il branding per la console di vRealize Automation.

È possibile utilizzare l'Elenco di controllo per la configurazione delle impostazioni del tenant per avere un quadro generale della sequenza di passaggi necessari per configurare le impostazioni del tenant.

Tabella 2-1. Elenco di controllo per la configurazione delle impostazioni del tenant

Attività	Ruolo di vRealize Automation	Dettagli
<input type="checkbox"/> Creare account utente locali e assegnare un amministratore tenant.	Amministratore di sistema	Configurazione dell'accesso al tenant predefinito
<input type="checkbox"/> Configurare Gestione directory per regolare le impostazioni per il controllo degli accessi e la gestione delle identità del tenant.	Amministratore tenant	Scelta delle opzioni di configurazione di Gestione directory
<input type="checkbox"/> Creare gruppi di business e gruppi personalizzati e concedere diritti di accesso utente alla console di vRealize Automation.	Amministratore tenant	Configurazione dei ruoli di utenti e gruppi
<input type="checkbox"/> (Facoltativo) Creare tenant aggiuntivi in modo che gli utenti possano accedere alle applicazioni e alle risorse appropriate di cui hanno bisogno per completare le proprie assegnazioni di lavoro.	Amministratore di sistema	Creazione di tenant aggiuntivi

Tabella 2-1. Elenco di controllo per la configurazione delle impostazioni del tenant (continua)

Attività	Ruolo di vRealize Automation	Dettagli
❑ (Facoltativo) Configurare un branding personalizzato per le pagine dell'applicazione e di accesso del tenant della console di vRealize Automation.	<ul style="list-style-type: none"> ■ Amministratore e di sistema ■ Amministratore e tenant 	Configurazione del branding personalizzato
❑ (Facoltativo) Configurare vRealize Automation per inviare notifiche agli utenti quando si verificano eventi specifici.	<ul style="list-style-type: none"> ■ Amministratore e di sistema ■ Amministratore e tenant 	Elenco di controllo per la configurazione delle notifiche
❑ (Facoltativo) Configurare vRealize Orchestrator per il supporto di XaaS e di altre opzioni di estensibilità.	<ul style="list-style-type: none"> ■ Amministratore e di sistema ■ Amministratore e tenant 	Configurazione di vRealize Orchestrator
❑ (Facoltativo) Creare un file di protocollo di desktop remoto personalizzato che verrà utilizzato dagli architetti IaaS nei blueprint per configurare le impostazioni RDP.	Amministratore di sistema	Creazione di un file RDP personalizzato per il supporto di connessioni RDP per le macchine di cui è stato eseguito il provisioning
❑ (Facoltativo) Definire posizioni dei data center che gli amministratori di struttura e gli architetti IaaS possono utilizzare per consentire agli utenti di selezionare una posizione appropriata per il provisioning al momento della richiesta delle macchine.	Amministratore di sistema	Per un esempio di aggiunta di posizioni dei data center, vedere Scenario: aggiunta di posizioni di data center per distribuzioni tra più regioni .

Scelta delle opzioni di configurazione di Gestione directory

È possibile utilizzare le funzionalità di Gestione directory di vRealize Automation per configurare un collegamento ad Active Directory in base ai propri requisiti di autenticazione utente.

Gestione directory offre molte opzioni che consentono un'elevata personalizzazione dell'autenticazione utente.

Tabella 2-2. Scelta delle opzioni di configurazione di Gestione directory

Opzione di configurazione	Procedura
Configurazione di un collegamento ad Active Directory.	<ol style="list-style-type: none"> 1 Configurazione di un collegamento ad Active Directory. Vedere Configurazione di un collegamento Active Directory su LDAP/IWA. 2 Se vRealize Automation è stato configurato per l'alta disponibilità, vedere Configurazione di Gestione directory per l'alta disponibilità.
(Facoltativo) Aumentare la sicurezza di un collegamento di directory basato su ID utente e password tramite la configurazione dell'integrazione bi-direzionale con i servizi ADFS (Active Directory Federated Services).	Configurazione di una relazione di trust bidirezionale tra vRealize Automation e Active Directory
(Facoltativo) Aggiungere utenti e gruppi a un collegamento ad Active Directory esistente.	Aggiunta di utenti o gruppi a una connessione Active Directory .

Tabella 2-2. Scelta delle opzioni di configurazione di Gestione directory (continua)

Opzione di configurazione	Procedura
(Facoltativo) Modificare il criterio predefinito per applicare regole personalizzate per un collegamento ad Active Directory.	Gestione del criterio di accesso utente.
(Facoltativo) Configurare gli intervalli di rete per limitare gli indirizzi IP tramite cui gli utenti possono accedere al sistema, gestire le restrizioni dell'accesso (timeout, numero di tentativi di accesso prima del blocco).	Aggiunta o modifica di un intervallo di rete.

Panoramica di Gestione directory

Gli amministratori tenant possono configurare le impostazioni di gestione delle identità del tenant e di controllo degli accessi utilizzando le opzioni di Gestione directory nella console delle applicazioni di vRealize Automation.

Dalla scheda **Amministrazione > Gestione directory** è possibile gestire le seguenti impostazioni.

Tabella 2-3. Impostazioni di Gestione directory

Impostazione	Descrizione
Directory	<p>La pagina Directory consente di creare e gestire i collegamenti ad Active Directory per supportare le autorizzazioni e l'autenticazione degli utenti dei tenant di vRealize Automation. L'utente crea una o più directory e quindi le sincronizza con la distribuzione di Active Directory. Questa pagina visualizza il numero di gruppi e utenti che vengono sincronizzati nella directory, nonché la data e l'ora dell'ultima sincronizzazione. È possibile fare clic su Sincronizza per avviare manualmente la sincronizzazione della directory.</p> <p>Vedere Utilizzo di Gestione directory per creare un collegamento ad Active Directory.</p> <p>Quando si fa clic su una directory e quindi sul pulsante Impostazioni di sincronizzazione, è possibile modificare le impostazioni di sincronizzazione, esplorare la pagina Provider di identità e visualizzare il registro delle sincronizzazioni.</p> <p>Dalla pagina delle impostazioni di sincronizzazione delle directory è possibile pianificare la frequenza di sincronizzazione, visualizzare l'elenco dei domini associati alla directory, cambiare l'elenco degli attributi mappati, aggiornare l'elenco di utenti e gruppi sincronizzato e impostare gli obiettivi di protezione.</p>
Connettori	<p>La pagina Connettori elenca i connettori distribuiti per la rete dell'azienda. Il compito di un connettore è di sincronizzare i dati di utenti e gruppi tra Active Directory e il servizio Gestione directory e, quando utilizzato come provider di identità, di autenticare gli utenti nel servizio. Per impostazione predefinita, ogni appliance vRealize Automation contiene un connettore. Vedere Gestione di connettori e cluster di connettori.</p>
Attributi utente	<p>La pagina Attributi utente elenca gli attributi utente predefiniti sincronizzati nella directory e permette di aggiungere altri attributi che possono essere mappati con quelli di Active Directory. Vedere Selezione degli attributi per la sincronizzazione con la directory.</p>
Intervalli di rete	<p>Questa pagina elenca gli intervalli di rete configurati per il sistema. È possibile configurare un intervallo di rete per consentire l'accesso degli utenti tramite quegli indirizzi IP. Si possono aggiungere intervalli di rete aggiuntivi e modificare quelli esistenti. Vedere Aggiunta o modifica di un intervallo di rete.</p>

Tabella 2-3. Impostazioni di Gestione directory (continua)

Impostazione	Descrizione
Provider di identità	La pagina Provider di identità elenca i provider di identità disponibili nel sistema. I sistemi vRealize Automation contengono un connettore che funge da provider di identità predefinito ed è sufficiente per la maggior parte delle esigenze degli utenti. È possibile aggiungere istanze di provider di identità di terze parti o avere una combinazione di entrambi i tipi. Vedere Configurazione di una connessione a un provider di identità di terze parti .
Criteri	La pagina Criteri elenca il criterio di accesso predefinito e tutti gli altri criteri di accesso alle applicazioni Web creati. I criteri sono un insieme di regole che definiscono quali sono i criteri da soddisfare affinché gli utenti possano accedere ai rispettivi portali di applicazioni o avviare applicazioni Web abilitate per essi. È consigliabile che il criterio predefinito sia adatto alla maggior parte delle distribuzioni di vRealize Automation, ma è possibile modificarlo se necessario. Vedere Gestione del criterio di accesso utente .

Concetti importanti relativi ad Active Directory

Per comprendere alcuni concetti correlati ad Active Directory, è fondamentale comprendere come Directories Management si integra con gli ambienti Active Directory.

Connettore

Il connettore, un componente del servizio, esegue le funzioni indicate di seguito.

- Sincronizza i dati di utenti e gruppi tra Active Directory e il servizio.
- Quando viene utilizzato come provider di identità, autentica gli utenti nel servizio.

Il connettore è il provider di identità predefinito. Per i metodi di autenticazione supportati dal connettore, vedere la guida *VMware Identity Manager Administration*. È anche possibile utilizzare provider di identità di terze parti che supportano il protocollo SAML 2.0. Utilizzare un provider di identità di terze parti per un tipo di autenticazione non supportato dal connettore o per un tipo di autenticazione supportato dal connettore, se il provider di identità di terze parti è preferibile in base ai propri criteri di sicurezza aziendale.

Nota anche se si utilizzano provider di identità di terze parti, è necessario configurare il connettore per la sincronizzazione dei dati di utenti e gruppi.

Directory

Il servizio Directories Management include il proprio concetto di directory, che utilizza gli attributi e i parametri di Active Directory per definire gli utenti e i gruppi. L'utente crea una o più directory e quindi le sincronizza con la distribuzione di Active Directory. È possibile creare nel servizio i tipi di directory indicati di seguito.

- Active Directory su LDAP. Creare questo tipo di directory se si desidera connettersi a un singolo ambiente di dominio Active Directory. Per il tipo di directory Active Directory su LDAP, il connettore esegue il binding ad Active Directory utilizzando l'autenticazione di binding semplice.

- Active Directory, Autenticazione integrata di Windows. Creare questo tipo di directory se si desidera connettersi a un ambiente Active Directory con più domini o foreste. Il connettore esegue il binding ad Active Directory utilizzando Autenticazione integrata di Windows.

Il tipo e il numero di directory create variano in base all'ambiente Active Directory, ad esempio dominio singolo o più domini, e al tipo di attendibilità utilizzata tra i domini. Nella maggior parte degli ambienti viene creata una directory.

Il servizio non dispone di accesso diretto ad Active Directory. Solo il connettore dispone di accesso diretto ad Active Directory. Pertanto, ogni directory creata nel servizio viene associata ad un'istanza del connettore.

Worker

Quando si associa una directory ad un'istanza del connettore, il connettore crea una partizione per la directory associata denominata Worker. A un'istanza del connettore possono essere associati più Worker. Ogni Worker agisce come un provider di identità. Per ogni Worker è necessario definire e configurare i metodi di autenticazione.

Il connettore sincronizza i dati di utenti e gruppi tra Active Directory e il servizio tramite uno o più Worker.

In un'istanza del connettore non possono essere presenti due Worker del tipo Autenticazione integrata di Windows.

Ambienti Active Directory

È possibile integrare il servizio in un ambiente Active Directory composto da un singolo dominio Active Directory, più domini in una singola foresta Active Directory o più domini in più foreste Active Directory.

Ambiente con singolo dominio Active Directory

Una distribuzione di Active Directory singola consente di sincronizzare gli utenti e i gruppi di un singolo dominio Active Directory.

Vedere [Configurazione di un collegamento Active Directory su LDAP/IWA](#) . Per questo ambiente, quando si aggiunge una directory al servizio, selezionare l'opzione Active Directory su LDAP.

Ambiente con foresta Active Directory singola e multidominio

Una distribuzione con una singola foresta Active Directory e multidominio consente di sincronizzare gli utenti e i gruppi da più domini Active Directory appartenenti a un'unica foresta.

È possibile configurare il servizio per questo ambiente Active Directory come tipo di directory con autenticazione integrata di Windows e singola Active Directory oppure, in alternativa, come tipo di directory Active Directory su LDAP configurata con l'opzione di catalogo globale.

- L'opzione consigliata è creare il tipo di directory con autenticazione integrata di Windows e singola Active Directory.

Vedere [Configurazione di un collegamento Active Directory su LDAP/IWA](#) . Quando si aggiunge una directory per questo ambiente, selezionare l'opzione Active Directory (autenticazione integrata di Windows).

Ambiente Active Directory multiforesta con relazioni di trust

Una distribuzione Active Directory multiforesta con relazioni di trust consente di sincronizzare gli utenti e i gruppi da più domini Active Directory tra foreste in cui esistono relazioni di trust bidirezionale tra domini.

Vedere [Configurazione di un collegamento Active Directory su LDAP/IWA](#) . Quando si aggiunge una directory per questo ambiente, selezionare l'opzione Active Directory (autenticazione integrata di Windows).

Ambiente Active Directory multiforesta senza relazioni di trust

Una distribuzione Active Directory multiforesta senza relazioni di trust consente di sincronizzare gli utenti e i gruppi da più domini Active Directory tra foreste senza una relazione di trust tra domini. Per questo ambiente occorre creare più directory nel servizio, una per ogni foresta.

Vedere [Configurazione di un collegamento Active Directory su LDAP/IWA](#) . Il tipo di directory create nel servizio dipende dalla foresta. Per foreste con domini multipli, selezionare l'opzione Active Directory (autenticazione integrata di Windows). Per una foresta con dominio singolo, selezionare l'opzione Active Directory su LDAP.

Utilizzo di Gestione directory per creare un collegamento ad Active Directory

Dopo aver creato tenant di vRealize Automation, è necessario accedere alla console di sistema in qualità di amministratore tenant e creare un collegamento ad Active Directory per supportare l'autenticazione utente.

Sono disponibili tre opzioni di protocolli di comunicazione Active Directory quando si configura una connessione Active Directory con la gestione delle directory.

- Active Directory su LDAP - Per impostazione predefinita una connessione Active Directory su protocollo LDAP supporta la ricerca della posizione del servizio DNS.
- Active Directory (autenticazione integrata di Windows) - L'opzione Active Directory (autenticazione integrata di Windows) consente di configurare il dominio a cui unirsi. Active Directory su LDAP è adeguato per distribuzioni di domini singoli. Utilizzare Active Directory (autenticazione integrata di Windows) per tutte le distribuzioni a più domini e a più foreste.
- OpenLDAP - È possibile utilizzare la versione open source di LDAP per supportare l'autenticazione degli utenti per la gestione delle directory.

Dopo aver selezionato un protocollo di comunicazione e configurato un link Active Directory, è possibile specificare i domini da utilizzare con la configurazione Active Directory, quindi selezionare gli utenti e i gruppi da sincronizzare con la configurazione specificata.

Configurazione di un collegamento Active Directory su LDAP/IWA

È possibile configurare un collegamento Active Directory su LDAP/IWA utilizzando la funzionalità Directories Management che consente di configurare un collegamento ad Active Directory per il supporto dell'autenticazione utente di tutti i tenant e selezionare gli utenti e i gruppi da sincronizzare con la directory Directories Management.

Per informazioni e istruzioni sull'uso di OpenLDAP con Directories Management, vedere [Configurazione di una connessione alla directory OpenLDAP](#).

Per Active Directory (autenticazione integrata di Windows), quando è configurata Active Directory multiforesta e il gruppo locale di dominio contiene membri provenienti da domini di foreste diverse, assicurarsi che l'utente Binding sia aggiunto al gruppo Administrators del dominio in cui risiede il gruppo locale di dominio. Se non si soddisfano tali requisiti, questi membri non appariranno nel gruppo locale di dominio.

Nota Configurare innanzitutto le directory IWA di Active Directory per il tenant predefinito. È quindi possibile aggiungerle ad altri tenant.

Prerequisiti

- Selezionare gli attributi predefiniti obbligatori e aggiungere ulteriori attributi nella pagina Attributi utente. Vedere [Selezione degli attributi per la sincronizzazione con la directory](#).
- Elenco di gruppi e utenti Active Directory da sincronizzare da Active Directory.
- Se Active Directory richiede l'accesso su SSL o STARTTLS, il certificato CA root del controller di dominio di Active Directory è obbligatorio.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.
- 2 Fare clic su **Aggiungi directory** e selezionare **Aggiungi Active Directory su LDAP/IWA**.
- 3 Nella pagina Aggiungi directory, specificare l'indirizzo IP del server di Active Directory nella casella di testo **Nome directory**.
- 4 Selezionare il protocollo di comunicazione con Active Directory appropriato utilizzando i pulsanti di opzione sotto la casella di testo **Nome directory**.

Opzione	Descrizione
Autenticazione Windows	Selezionare Active Directory (autenticazione integrata di Windows) . Per l'autenticazione integrata di Windows in Active Directory, le informazioni obbligatorie sono l'indirizzo UPN dell'utente di binding del dominio e la relativa password.
LDAP	Selezionare Active Directory su LDAP . Per Active Directory su LDAP, le informazioni obbligatorie includono DN di base, DN di binding e password del DN di binding.

- 5 Configurare il connettore che sincronizza gli utenti di Active Directory con la directory Directories Management di VMware nella sezione Sincronizzazione directory e autenticazione.

Opzione	Descrizione
Connettore di sincronizzazione	<p>Selezionare il connettore appropriato da utilizzare per il sistema. Ogni appliance vRealize Automation contiene un connettore predefinito. Rivolgersi all'amministratore di sistema per aiuto nella scelta del connettore appropriato.</p>
Autenticazione	<p>Fare clic sul pulsante di opzione appropriato per indicare se anche il connettore selezionato deve eseguire l'autenticazione.</p> <p>Se si utilizza Active Directory (autenticazione integrata di Windows), con un provider di identità di terze parti per eseguire l'autenticazione degli utenti, fare clic su No. Dopo aver configurato la connessione ad Active Directory per sincronizzare utenti e gruppi, passare alla pagina Provider di identità per aggiungere il provider di identità per l'autenticazione.</p> <p>Per informazioni sull'utilizzo degli adattatori di autenticazione come PasswordIpddAdapter, SecurIDAdapter e RadiusAuthAdapter, vedere la <i>Guida all'amministrazione di VMware Identity Manager</i>.</p>
Attributo di ricerca directory	<p>Selezionare l'attributo dell'account appropriato contenente il nome utente. VMware consiglia di utilizzare l'attributo sAMAccount anziché userPrincipalName. Se si utilizza userPrincipalName per le operazioni di sincronizzazione, è possibile che l'integrazione con software di seconde e terze parti che richiede un nome utente non funzioni correttamente.</p> <p>Nota Se si seleziona sAMAccountName quando si utilizza un catalogo globale, indicato selezionando la casella di controllo Questa directory dispone di un catalogo globale nell'area Posizione server, gli utenti non potranno effettuare l'accesso.</p>

- 6 Immettere le informazioni appropriate nella casella di testo Posizione server se è stata selezionata l'opzione Active Directory su LDAP oppure inserire le informazioni nelle caselle di testo di Dettaglio unione al dominio se è stata selezionata l'opzione Active Directory (autenticazione integrata di Windows).

Opzione	Descrizione
Posizione server - Visualizzata quando l'opzione Active Directory su LDAP è selezionata	<p>■ Se si desidera utilizzare la ricerca DNS di Posizione servizio per individuare i domini di Active Directory, lasciare selezionata la casella di controllo La directory supporta DNS di Posizione servizio.</p> <p>Nota Se si seleziona questa opzione, non è possibile impostare l'assegnazione della porta su 636.</p> <p>Insieme alla directory viene creato un file <code>domain_krb.properties</code>, popolato automaticamente con un elenco di controller di dominio. Vedere Informazioni sulla selezione dei controller di dominio.</p> <p>Se Active Directory richiede la crittografia STARTTLS, selezionare la casella di controllo Questa directory richiede che tutte le connessioni utilizzino STARTTLS nella sezione Certificati e copiare e incollare il certificato CA root di Active Directory nel campo Certificato SSL.</p> <p>■ Se il servizio Active Directory specificato non utilizza la ricerca DNS di Posizione servizio, deselezionare la casella di controllo accanto a La directory supporta DNS di Posizione servizio nei campi Posizione server e inserire il nome host e la porta del server di Active Directory nelle caselle di testo corrispondenti.</p> <p>Selezionare la casella di controllo Questa directory dispone di un catalogo globale se l'istanza di Active Directory associata utilizza un catalogo globale. Un catalogo globale contiene una rappresentazione di tutti gli oggetti in ogni dominio in una foresta Active Directory a più domini.</p> <p>Per configurare la directory come catalogo globale, vedere la sezione relativa all'ambiente di Active Directory con foresta singola a più domini in Ambienti Active Directory.</p> <p>Se Active Directory richiede l'accesso tramite SSL, selezionare la casella di controllo Questa directory richiede che tutte le connessioni utilizzino SSL sotto l'intestazione Certificati e fornire il certificato SSL di Active Directory.</p> <p>Quando si seleziona questa opzione, viene utilizzata automaticamente la porta 636 e non può essere modificata.</p> <p>Assicurarsi che il certificato sia in formato PEM e che includa le righe BEGIN CERTIFICATE ed END CERTIFICATE.</p>
Dettaglio unione al dominio - Visualizzata quando l'opzione Active Directory (autenticazione Windows integrata) è selezionata	<p>Immettere le credenziali necessarie nelle caselle di testo Nome dominio, Nome utente amministratore di dominio e Password amministratore di dominio.</p> <p>Se Active Directory richiede la crittografia STARTTLS, selezionare la casella di controllo Questa directory richiede che tutte le connessioni utilizzino STARTTLS nella sezione Certificati e copiare e incollare il certificato CA root di Active Directory nel campo Certificato SSL.</p> <p>Assicurarsi che il certificato sia in formato PEM e che includa le righe BEGIN CERTIFICATE ed END CERTIFICATE.</p>

Opzione	Descrizione
	Se la directory ha più domini, aggiungere i certificati CA root per tutti i domini, uno alla volta.
	Nota Se Active Directory richiede STARTTLS e non si fornisce il certificato, non è possibile creare la directory.

- 7 Nella sezione Dettagli utente di binding immettere le credenziali appropriate per consentire la sincronizzazione delle directory.

Per Active Directory su LDAP:

Opzione	Descrizione
DN di base	Specificare il nome distinto di base per la ricerca. Ad esempio, cn=users,dc=corp,dc=local .
DN di binding	Specificare il nome distinto di binding. Ad esempio cn=fritz infra,cn=users,dc=corp,dc=local

Per Active Directory (autenticazione integrata di Windows):

Opzione	Descrizione
UPN utente di binding	Immettere il nome dell'entità dell'utente che può autenticarsi nel dominio. Ad esempio UserName@example.com.
Password DN di binding	Specificare la password dell'utente Binding.

- 8 Fare clic su **Prova connessione** per verificare la connessione alla directory configurata.

Questo pulsante non viene visualizzato se è stata selezionata l'opzione Active Directory (autenticazione integrata di Windows).

- 9 Fare clic su **Salva e avanti**.

Viene visualizzata la pagina Seleziona domini con l'elenco dei domini.

- 10 Esaminare e aggiornare i domini elencati per la connessione ad Active Directory.

- Per Active Directory (autenticazione integrata di Windows), selezionare i domini da associare a questa connessione ad Active Directory.
- Per Active Directory su LDAP, il dominio disponibile viene elencato con un segno di spunta.


Nota se si aggiunge un dominio trusting dopo aver creato la directory, il servizio non rileva automaticamente il nuovo dominio trusting. Per consentire al servizio di rilevare il dominio, connettore deve essere tolto e poi aggiunto nuovamente al dominio. Quando connettore si unisce nuovamente al dominio, il dominio trusting comparirà nell'elenco.

- 11 Fare clic su **Avanti**.

- 12** Verificare che i nomi degli attributi della directory di Directories Management siano mappati agli attributi di Active Directory corretti.

Se i nomi degli attributi di directory non sono mappati correttamente, selezionare l'attributo Active Directory corretto nel menu a discesa.

- 13** Fare clic su **Avanti**.

- 14** Fare clic su  per selezionare i gruppi da sincronizzare da Active Directory alla directory.

Quando si aggiunge un gruppo da Active Directory, se i membri di tale gruppo non sono inclusi nell'elenco Utenti, vengono aggiunti. Quando si sincronizza un gruppo, gli utenti che non hanno Utenti del dominio come gruppo primario in Active Directory non vengono sincronizzati.

Nota il sistema di autenticazione degli utenti di Directories Management importa i dati da Active Directory quando si aggiungono gruppi e utenti e la velocità del sistema dipende dalle caratteristiche di Active Directory. È quindi possibile che l'importazione di un numero elevato di gruppi e utenti richieda una quantità di tempo significativa. Per ridurre eventuali ritardi o problemi, aggiungere solo i gruppi e gli utenti effettivamente necessari per il funzionamento di vRealize Automation.


In caso di errori o di peggioramento delle prestazioni del sistema, chiudere tutte le applicazioni non necessarie e verificare che sia stata allocata ad Active Directory una quantità di memoria appropriata. Se i problemi persistono, aumentare la quantità di memoria allocata ad Active Directory in base alle necessità. Per sistemi con un elevato numero di utenti e gruppi, potrebbe essere necessario allocare fino a 24 GB di memoria ad Active Directory.

- 15** Fare clic su **Avanti**.

- 16** Fare clic su  per aggiungere ulteriori utenti.

I valori appropriati sono i seguenti:

- Singolo utente: **CN=username,CN=Users,OU=Users,DC=myCorp,DC=com**
- Più utenti: **OU=Users,OU=myUnit,DC=myCorp,DC=com**

Per escludere utenti, fare clic su  per creare un filtro che escluda determinati tipi di utenti. È possibile selezionare l'attributo da utilizzare per filtrare gli utenti, la regola di query e il valore.

- 17** Fare clic su **Avanti**.

- 18** Esaminare la pagina per verificare quanti utenti e gruppi sono in corso di sincronizzazione con la directory.

Se si desidera apportare modifiche agli utenti e ai gruppi, fare clic sui collegamenti Modifica.

Nota Assicurarsi di specificare DN di utenti inclusi all'interno del DN di base specificato in precedenza. Se il DN di un utente si trova al di fuori del DN di base, gli utenti di tale DN verranno sincronizzati ma non potranno effettuare l'accesso.

19 Fare clic su **Push in area di lavoro** per avviare la sincronizzazione con la directory.

Risultati

La connessione ad Active Directory è completa e gli utenti e i gruppi selezionati vengono aggiunti alla directory. Ora è possibile assegnare utenti e gruppi ai ruoli vRealize Automation appropriati selezionando **Amministrazione > Utenti e gruppi > Utenti e gruppi della directory**. Vedere [Assegnazione di ruoli a utenti e gruppi della directory](#) per ulteriori informazioni.

Operazioni successive

Se l'ambiente vRealize Automation è configurato per l'alta disponibilità, è necessario configurare Gestione directory specificamente per questa modalità. Vedere [Configurazione di Gestione directory per l'alta disponibilità](#).

- Impostare i metodi di autenticazione. Dopo la sincronizzazione di utenti e gruppi con la directory, se il connettore è utilizzato anche per l'autenticazione, è possibile impostare metodi di autenticazione aggiuntivi sul connettore. Se il provider di identità di autenticazione è di terze parti, configurare quel provider di identità nel connettore.
- Riesaminare il criterio di accesso predefinito. Il criterio di accesso predefinito è configurato per consentire l'accesso al browser Web da parte di tutte le appliance in tutti gli intervalli di rete, con un timeout di sessione impostato a otto ore, oppure l'accesso a un'app client con un timeout di sessione di 2.160 ore (90 giorni). È possibile modificare il criterio di accesso predefinito e creare nuovi criteri quando si aggiungono applicazioni Web al catalogo.
- Applicare un branding personalizzato alla console di amministrazione, alle pagine del portale degli utenti e alla schermata di accesso.

Configurazione di una connessione alla directory OpenLDAP

È possibile configurare una connessione alla directory OpenLDAP utilizzando Gestione directory.

Sebbene esistano diversi protocolli LDAP, OpenLDAP è l'unico protocollo testato e approvato per l'uso con il servizio Gestione directory di vRealize Automation.

Per l'integrazione con la directory LDAP, è necessario creare una directory di Directories Management corrispondente e sincronizzare utenti e gruppi dalla directory LDAP alla directory di Directories Management. È possibile impostare una pianificazione di sincronizzazione regolare per gli aggiornamenti successivi.

Si possono anche selezionare gli attributi LDAP che si desidera sincronizzare per gli utenti e associarli ad attributi di Directories Management.

La configurazione della directory LDAP può essere basata su schemi predefiniti, ma si possono creare anche schermi personalizzati. Inoltre si possono definire attributi personalizzati. Affinché Directories Management possa eseguire query nella directory LDAP per ottenere oggetti utente o gruppo, è necessario fornire i filtri di ricerca LDAP e i nomi degli attributi applicabili alla directory LDAP.

Nello specifico, è necessario fornire la seguenti informazioni.

- Filtri di ricerca LDAP per ottenere gruppi, utenti e l'utente di binding
- Nomi degli attributi LDAP per l'appartenenza ai gruppi, UUID e nome distinto

Nota Gestione directory utilizza la dimensione pagina predefinita 1500 per le query LDAP. Se si configura una connessione alla directory OpenLDAP, è necessario abilitare l'estensione del controllo della pagina dei risultati semplice per consentire a OpenLDAP di limitare il numero di risultati visualizzati. Il non utilizzo di questa estensione può causare errori di sincronizzazione per gruppi e utenti.

Prerequisiti

- Esaminare la configurazione nella pagina Attributi utente e aggiungere gli altri attributi che si desidera sincronizzare. L'associazione degli attributi di Directories Management con quelli della directory LDAP viene eseguita in fase di creazione della directory. Questi attributi saranno sincronizzati per gli utenti nella directory.

Nota Quando si apportano modifiche agli attributi degli utenti, considerare l'effetto sulle altre directory nel servizio. Se si pianifica di aggiungere sia Active Directory che directory LDAP, assicurarsi di non contrassegnare alcun attributo come obbligatorio, eccetto **userName**. Le impostazioni nella pagina Attributi utente si applica a tutte le directory nel servizio. Se un attributo è contrassegnato come obbligatorio, gli utenti senza l'attributo non vengono sincronizzati nel servizio di Directories Management.

- Un account utente Nome distinto di binding. L'uso di un utente Nome distinto di binding con una password che non ha scadenza è consigliato.
- Nella directory LDAP, gli UUID di utenti e gruppi devono essere in formato testo normale.
- Nella directory LDAP, per tutti gli utenti e i gruppi deve esistere un attributo di dominio.
Questo attributo viene associato all'attributo **dominio** di Directories Management quando si crea la directory di Directories Management.
- I nomi utente non devono contenere spazi. Se un nome utente contiene spazi, l'utente viene sincronizzato ma i permessi non saranno disponibili per l'utente.
- Se si utilizza l'autenticazione con certificato, per gli utenti devono essere impostati valori per gli attributi userPrincipalName e indirizzo e-mail.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.
- 2 Fare clic su **Aggiungi directory** e selezionare **Aggiungi directory LDAP**.

3 Immettere le informazioni richieste nella pagina Aggiungi directory LDAP.

Opzione	Descrizione
Nome directory	Immettere un nome per la directory Directories Management.
Sincronizzazione e autenticazione directory	<p>a Nel campo Sincronizza connettore, selezionare il connettore che si desidera utilizzare per sincronizzare gli utenti e i gruppi dalla directory LDAP alla directory Directories Management.</p> <p>Per impostazione predefinita, un componente del connettore è sempre disponibile con il servizio Directories Management. Questo connettore verrà visualizzato nell'elenco a discesa. Se si installano più appliance Directories Management per l'alta disponibilità, nell'elenco verrà visualizzato il componente del connettore di ciascuna appliance.</p> <p>Non è necessario un connettore separato per una directory LDAP. Un connettore può supportare più directory, indipendentemente dal fatto che siano Active Directory o directory LDAP.</p> <p>b Nel campo Autenticazione, scegliere Sì se si desidera utilizzare questa directory LDAP per autenticare gli utenti.</p> <p>Se si desidera utilizzare un provider di identità di terze parti per autenticare gli utenti, fare clic su No. Dopo aver aggiunto la connessione alla directory per sincronizzare utenti e gruppi, passare alla pagina Amministrazione > Gestione directory > Provider di identità per aggiungere il provider di identità di terze parti per l'autenticazione.</p> <p>c Per la maggior parte delle configurazioni, lasciare l'opzione predefinita Personalizzato selezionata nella casella di testo Attributo di ricerca directory. Nel campo Attributo di ricerca directory - Personalizzato, specificare l'attributo di directory LDAP da utilizzare per i nomi di utente e di gruppo. Questo attributo identifica in modo univoco le entità, ad esempio utenti e gruppi, del server LDAP. Ad esempio, cn.</p> <p>d Se si desidera utilizzare la ricerca della posizione del servizio DNS per Active Directory, effettuare le selezioni riportate di seguito.</p> <ul style="list-style-type: none"> ■ Nella sezione Posizione server, selezionare la casella di controllo Questa directory supporta la posizione servizio DNS. <p>Gestione directory individua e utilizza i controller di dominio ottimali. Se non si desidera utilizzare la selezione dei controller di dominio ottimizzata, saltare al passaggio e.</p> <ul style="list-style-type: none"> ■ Se Active Directory richiede la crittografia STARTTLS, selezionare la casella di spunta Questa directory richiede che tutte le connessioni utilizzino SSL nella sezione Certificati e copiare e incollare il certificato CA root di Active Directory nella casella di testo Certificato SSL. <p>Assicurarsi che il certificato sia in formato PEM e che includa le righe "BEGIN CERTIFICATE" ed "END CERTIFICATE".</p> <p>Nota Se Active Directory richiede STARTTLS e non si fornisce il certificato, non è possibile creare la directory.</p> <p>e Se non si desidera utilizzare la ricerca della posizione del servizio DNS per Active Directory, effettuare le selezioni riportate di seguito.</p> <ul style="list-style-type: none"> ■ Nella sezione Posizione server, verificare che la casella di controllo Questa directory supporta posizione servizio DNS non sia

Opzione	Descrizione
	<p>selezionata ed immettere il nome host e il numero di porta del server Active Directory. Per configurare la directory come catalogo globale, vedere la sezione relativa all'ambiente di Active Directory con foresta singola a più domini in Ambienti Active Directory.</p> <ul style="list-style-type: none"> Se Active Directory richiede l'accesso su SSL, selezionare la casella di controllo Questa directory richiede che tutte le connessioni utilizzino SSL nella sezione Certificati e copiare e incollare il certificato CA root di Active Directory nel campo Certificato SSL. <p>Assicurarsi che il certificato sia in formato PEM e che includa le righe "BEGIN CERTIFICATE" ed "END CERTIFICATE".</p> <p>Nota Se Active Directory richiede STARTTLS e non si fornisce il certificato, non è possibile creare la directory.</p>
Posizione server	<p>Immettere l'host del server e il numero di porta della directory LDAP. Per l'host del server, è possibile specificare sia il nome di dominio completo che l'indirizzo IP. Ad esempio, serverLDAP.esempio.com o 100.00.00.0.</p> <p>Se è presente un cluster di server con il bilanciamento del carico, immettere invece le informazioni sul bilanciamento.</p>
Configurazione LDAP	<p>Specificare i filtri di ricerca LDAP e gli attributi che possono essere utilizzati da Directories Management per interrogare la propria directory LDAP. I valori predefiniti sono forniti in base allo schema LDAP principale.</p> <p>Query con filtro</p> <ul style="list-style-type: none"> Gruppi: il filtro di ricerca per ottenere gli oggetti gruppo. <p>Ad esempio: (objectClass=group)</p> <ul style="list-style-type: none"> Utente bind: il filtro di ricerca per ottenere l'oggetto utente bind, ovvero l'utente che può eseguire il binding alla directory. <p>Ad esempio: (objectClass=person)</p> <ul style="list-style-type: none"> Utenti: il filtro di ricerca per ottenere gli utenti da sincronizzare. <p>Ad esempio: (&(objectClass=user)(objectCategory=person))</p> <p>Attributi</p> <ul style="list-style-type: none"> Appartenenza: questo attributo è utilizzato nella directory LDAP per definire i membri di un gruppo. <p>Ad esempio: member</p> <ul style="list-style-type: none"> UUID oggetto: l'attributo utilizzato nella directory LDAP per definire l'UUID di un utente o di un gruppo. <p>Ad esempio: entryUUID</p> <ul style="list-style-type: none"> DN (Distinguished Name): l'attributo utilizzato nella directory LDAP per il nome distinto (DN) di un utente o un gruppo. <p>Ad esempio: entryDN</p>

Opzione	Descrizione
Certificati	<p>Se la directory LDAP richiede l'accesso su SSL, selezionare la casella di controllo Questa directory richiede che tutte le connessioni utilizzino SSL. Copiare e incollare quindi il certificato CA SSL root del server di directory LDAP nella casella di testo Certificato SSL. Assicurarsi che il certificato sia in formato PEM e includere le righe "BEGIN CERTIFICATE" e "END CERTIFICATE".</p> <p>Se la directory ha più domini, aggiungere i certificati CA root di tutti i domini, uno di seguito all'altro.</p> <p>Infine, verificare che sia stato specificato il numero di porta corretto nel campo Porta server della sezione Posizione server della pagina.</p>
Dettagli utente Bind	<p>Nome distinto di base: immettere il DN da cui iniziare le ricerche. Ad esempio, cn=users,dc=example,dc=com</p> <p>Tutti gli utenti validi devono essere inclusi in Nome distinto di base. Se un determinato utente non è incluso in Nome distinto di base, tale utente non potrà accedere anche se è un membro di un gruppo incluso in Nome distinto di base.</p> <p>Nome distinto di binding: immettere il nome distinto da utilizzare per eseguire il binding alla directory LDAP. È anche possibile immettere i nomi utente, ma un nome distinto è più adatto nella maggior parte delle distribuzioni.</p> <hr/> <p>Nota È consigliato l'uso di un account utente Nome distinto di binding con una password senza scadenza.</p> <hr/> <p>Password nome distinto di binding: immettere la password per l'utente Nome distinto di binding</p>

- 4 Per eseguire il test della connessione al server di directory LDAP, fare clic su **Test della connessione**.

Se la connessione non riesce, controllare le informazioni immesse ed apportare le modifiche necessarie.

- 5 Fare clic su **Salva e avanti**.

- 6 Verificare che sia selezionato il dominio corretto nella pagina Seleziona domini, quindi fare clic su **Avanti**.

- 7 Nella pagina di associazione degli attributi, verificare che gli attributi di Directories Management siano associati agli attributi di LDAP corretti.

Questi attributi saranno sincronizzati per gli utenti.

Importante È necessario specificare un'associazione per l'attributo **dominio**.

È possibile aggiungere attributi all'elenco dalla pagina Attributi utente.

- 8 Fare clic su **Avanti**.

- 9 Fare clic sul segno **+** per selezionare i gruppi da sincronizzare dalla directory LDAP alla directory Directories Management nella pagina Selezionare i gruppi (utenti) da sincronizzare.

Se nella directory LDAP sono presenti più gruppi con lo stesso nome, sarà necessario specificare nomi univoci sulla relativa pagina.

Quando si aggiunge un gruppo da Active Directory, se i membri di tale gruppo non sono inclusi nell'elenco Utenti, vengono aggiunti. Quando si sincronizza un gruppo, gli utenti che non hanno Utenti del dominio come gruppo primario in Active Directory non vengono sincronizzati.

Per impostazione predefinita è abilitata l'opzione **Sincronizza membri del gruppo nidificati**. Quando questa opzione è abilitata, tutti gli utenti che appartengono direttamente al gruppo selezionato così come gli utenti che appartengono ai gruppi nidificati al di sotto di esso vengono sincronizzati. Tenere presente che i gruppi nidificati non vengono sincronizzati; sono sincronizzati solo gli utenti che appartengono a tali gruppi. Nella directory di Directories Management, questi utenti saranno membri del gruppo di livello superiore selezionato per la sincronizzazione. La gerarchia inferiore al gruppo selezionato viene di fatto appiattita e gli utenti provenienti da tutti i livelli compaiono in Directories Management come membri del gruppo selezionato.

Se l'opzione è disattivata, quando si specifica un gruppo da sincronizzare, tutti gli utenti che appartengono direttamente a tale gruppo saranno sincronizzati. Gli utenti che appartengono ai gruppi nidificati al di sotto di esso non saranno sincronizzati. La disabilitazione di questa opzione è utile per configurazioni di directory di grosse dimensioni dove l'attraversamento di una struttura di gruppi implica un uso intensivo di risorse e di tempo. Se si disattiva questa opzione, assicurarsi di selezionare tutti i gruppi per cui si desidera sincronizzare gli utenti.

Nota il sistema di autenticazione degli utenti di Directories Management importa i dati da Active Directory quando si aggiungono gruppi e utenti e la velocità del sistema dipende dalle caratteristiche di Active Directory. È quindi possibile che l'importazione di un numero elevato di gruppi e utenti richieda una quantità di tempo significativa. Per ridurre eventuali ritardi o problemi, aggiungere solo i gruppi e gli utenti effettivamente necessari per il funzionamento di vRealize Automation.

In caso di errori o di peggioramento delle prestazioni del sistema, chiudere tutte le applicazioni non necessarie e verificare che sia stata allocata a Gestione directory una quantità di memoria appropriata. Se i problemi persistono, aumentare la quantità di memoria allocata a Gestione directory in base alle necessità. Per i sistemi con un elevato numero di utenti e gruppi, potrebbe essere necessario allocare fino a 24 GB di memoria a Gestione directory.

- 10 Fare clic su **Avanti**.
- 11 Fare clic su **+** per aggiungere altri utenti. Ad esempio, immettere **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Qui è possibile aggiungere sia unità organizzative sia singoli utenti.

È possibile creare un filtro per escludere alcuni tipi di utenti. Selezionare l'attributo da utilizzare per filtrare gli utenti, la regola di query e il valore.

12 Fare clic su **Avanti**.

13 Esaminare la pagina per sapere quanti utenti e gruppi verranno sincronizzati nella directory e per conoscere la pianificazione delle sincronizzazioni predefinita.

Per apportare modifiche a utenti e gruppi o alla frequenza di sincronizzazione, fare clic sul collegamento **Modifica**.

14 Fare clic su **Sincronizza directory** per iniziare la sincronizzazione della directory.

Risultati

La connessione alla directory LDAP viene stabilita ed utenti e gruppi vengono sincronizzati dalla directory LDAP alla directory di Directories Management.

Ora è possibile assegnare utenti e gruppi ai ruoli vRealize Automation appropriati selezionando **Amministrazione > Utenti e gruppi > Utenti e gruppi della directory**. Vedere [Assegnazione di ruoli a utenti e gruppi della directory](#) per ulteriori informazioni.

Limitazioni dell'integrazione della directory LDAP

Sono presenti diverse limitazioni importanti correlate all'integrazione della directory LDAP nella gestione delle directory.

- È possibile integrare solo un ambiente con directory LDAP a dominio singolo.
Per integrare domini multipli da una directory LDAP è necessario creare directory Directories Management aggiuntive, una per ogni dominio.
- I seguenti metodi di autenticazione non sono supportati per le directory Directories Management di tipo directory LDAP.
 - autenticazione Kerberos
 - Autenticazione adattiva RSA
 - ADFS come provider di identità di terze parti
 - SecurID
 - Autenticazione Radius con server SMS Passcode e Vasco
- Non è possibile unire un dominio LDAP.
- Non è supportata l'integrazione con risorse View o pubblicate da Citrix per le directory Directories Management di tipo directory LDAP.
- I nomi utente non devono contenere spazi. Se un nome utente contiene spazi, l'utente viene sincronizzato ma i permessi non saranno disponibili per l'utente.

- Se si pianifica l'aggiunta di directory sia Active Directory che LDAP, assicurarsi di non contrassegnare alcun attributo come obbligatorio nella pagina Attributi utente, eccetto userName, che può essere contrassegnato come obbligatorio. Le impostazioni nella pagina Attributi utente si applica a tutte le directory nel servizio. Se un attributo è contrassegnato come obbligatorio, gli utenti senza l'attributo non vengono sincronizzati nel servizio di Directories Management.
- Se nella directory LDAP sono presenti più gruppi con lo stesso nome, è necessario specificare nomi univoci per essi nel servizio Directories Management. È possibile specificare i nomi quando si selezionano i gruppi da sincronizzare.
- Non è disponibile l'opzione per consentire agli utenti di reimpostare le password scadute.
- Il file `domain_krb.properties` non è supportato.

Configurazione di Gestione directory per l'alta disponibilità

È possibile utilizzare Gestione directory per configurare una connessione ad Active Directory ad alta disponibilità in vRealize Automation.

Ogni appliance vRealize Automation include un connettore che supporta l'autenticazione utente, anche se in genere viene configurato un solo connettore per eseguire la sincronizzazione delle directory. Non è importante quale sia il connettore scelto per la sincronizzazione. Per supportare l'alta disponibilità di Gestione directory, è necessario configurare manualmente un secondo connettore che corrisponda alla seconda appliance vRealize Automation, si connetta al provider di identità e punti alla stessa istanza di Active Directory. Con questa configurazione, se in un'appliance si verifica un errore, l'altra la sostituisce per la gestione dell'autenticazione degli utenti.

In un ambiente ad alta disponibilità, tutti i nodi devono servire lo stesso set di Active Directory, utenti, metodo di autenticazione e così via. Il metodo più diretto per implementare questa configurazione consiste nel promuovere il provider di identità nel cluster impostando l'host di bilanciamento del carico come host del provider di identità. Con questa configurazione, tutte le richieste di autenticazione vengono indirizzate al bilanciamento del carico, che a sua volta le inoltra al connettore appropriato.

Un connettore viene utilizzato anche per la sincronizzazione dell'utente. Ma un solo connettore viene configurato per eseguire la sincronizzazione della directory. Gli utenti sincronizzati vengono salvati nel database dell'appliance, che è leggibile da tutti i nodi del cluster. Se si verifica un problema con il connettore responsabile della sincronizzazione della directory, la sincronizzazione della directory verrà interrotta. Per recuperare, l'amministratore del tenant deve richiedere manualmente a un altro connettore di eseguire la sincronizzazione della directory utilizzando l'interfaccia utente di vRealize Automation. Vedere [Abilitare la sincronizzazione directory su un connettore secondario](#).

Per ulteriori informazioni sull'utilizzo dei connettori, vedere [Gestione di connettori e cluster di connettori](#).

Prerequisiti

- Configurare la distribuzione di vRealize Automation con almeno due istanze dell'appliance vRealize Automation.
- Installare vRealize Automation in modalità Enterprise operando in un singolo dominio con due istanze dell'appliance vRealize Automation.
- Installare e configurare un bilanciamento del carico appropriato per operare con la distribuzione vRealize Automation esistente.
- Configurare i tenant e Gestione directory utilizzando uno dei connettori forniti con le istanze installate dell'appliance vRealize Automation. Per informazioni sulla configurazione dei tenant, vedere [Configurazione delle impostazioni del tenant](#).

Procedura

- 1 Accedere al bilanciamento del carico della distribuzione vRealize Automation come amministratore tenant.

L'URL del bilanciamento del carico è `<load balancer address>/vcac/org/tenant_name`.
- 2 Selezionare **Amministrazione > Gestione directory > Provider di identità**.
- 3 Fare clic sul provider di identità attualmente in uso per il sistema.

Vengono visualizzati la directory e il connettore che correntemente forniscono al sistema la gestione di base delle identità.
- 4 Nella pagina delle proprietà del provider di identità, fare clic sull'elenco a discesa **Aggiungi un connettore** e selezionare il connettore corrispondente all'appliance vRealize Automation secondaria.
- 5 Immettere la password appropriata nella casella di testo **Password DN di binding** visualizzata alla selezione del connettore.
- 6 Fare clic su **Aggiungi connettore**.
- 7 Per impostazione predefinita, nella casella di testo **Nome host IdP** compare il connettore principale. Cambiare il nome host per puntare al bilanciamento del carico.

Abilitare la sincronizzazione directory su un connettore secondario

Se il connettore principale non riesce, l'autenticazione viene gestita automaticamente da un'altra istanza del connettore. In caso di esito negativo, per la sincronizzazione della directory, è necessario modificare le impostazioni della directory in Gestione directory per utilizzare l'istanza del connettore secondario appropriata. È possibile abilitare la sincronizzazione della directory solo su un connettore alla volta.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.

- 2 Selezionare la directory che era associata con l'istanza del connettore originale.

Nota Queste informazioni sono disponibili nella pagina **Directory > Connettori**.

- 3 Nella sezione Sincronizzazione e autenticazione directory della pagina Directory, selezionare un'altra istanza del connettore nell'elenco a discesa **Sincronizza connettore**.
- 4 Nella sezione Dettagli utente Bind, immettere la password dell'account bind di Active Directory nella casella di testo **Password DN di binding**.
- 5 Fare clic su **Salva**.

Configurazione di una relazione di trust bidirezionale tra vRealize Automation e Active Directory

È possibile migliorare la sicurezza di sistema di una connessione Active Directory vRealize Automation di base configurando una relazione di trust bidirezionale tra il provider di identità e Active Directory Federated Services.

Per configurare una relazione di trust bidirezionale tra vRealize Automation e Active Directory, è necessario creare una provider di identità personalizzato e aggiungere metadati di Active Directory a questo provider. Inoltre è necessari omodificare il criterio predefinito utilizzato dalla distribuzione di vRealize Automation. Infine è necessario configurare Active Directory per riconoscere il provider di identità.

Prerequisiti

- Verificare che siano stati configurati i tenant per la distribuzione vRealize Automation e un collegamento Active Directory appropriato per supportare l'autenticazione ID utente e password di base di Active Directory.
- Active Directory è installato e configurato per l'uso nella rete esistente.
- Ottenere i metadati ADFS (Active Directory Federated Services) appropriati.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Ottenere il file Federation Metadata.

È possibile scaricare questo file da <https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml>

- 2 Cercare la parola logout e modificare la posizione di tutte le istanze che puntano a <https://servername.domain/adfs/ls/logout.aspx>

Ad esempio, la seguente:

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/ "/>
```

Deve essere cambiata in:

```
SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

3 Creare un nuovo provider di identità per la distribuzione.

- a Selezionare **Amministrazione > Gestione directory > Provider di identità**.
- b Fare clic su **Aggiungi provider di identità** e completare i campi come appropriato.

Opzione	Descrizione
Nome del provider di identità	Immettere il nome del nuovo provider di identità.
Metadati del provider di identità (URL o XML)	Incollare il contenuto del file di metadati di Active Directory Federated Services qui.
Nome del criterio ID nome nella richiesta SAML (facoltativo)	Se appropriato, immettere un nome per la richiesta SAML del criterio di identità.
Utenti	Selezionare i domini per i quali si desidera assegnare privilegi di accesso agli utenti
Metadati IDP processo	Fare clic per elaborare il file di metadati aggiunto.
Rete	Selezionare gli intervalli di rete ai quali si desidera che gli utenti accedano.
Metodi di autenticazione	Immettere un nome per il metodo di autenticazione usato dal provider di identità.
Contesto SAML	Selezionare il contesto appropriato per il sistema.
Certificato della firma SAML	Fare clic sul collegamento accanto all'intestazione Metadati SAML per scaricare i metadati di Gestione directory.

- c Salvare il file dei metadati di Gestione directory come `sp.xml`.
- d Fare clic su **Aggiungi**.

4 Aggiungere un ruolo al criterio predefinito.

- a Selezionare **Amministrazione > Gestione directory > Criteri**.
- b Fare clic sul nome del criterio predefinito.
- c Fare clic sull'icona **+** nell'intestazione **Regole criterio** per aggiungere una nuova regola.

Utilizzare le opzioni della pagina **Aggiungi regola criterio** per creare una regola che specifichi i metodi di autenticazione primario e secondario appropriati da utilizzare per un intervallo di rete e un dispositivo specifici.

Ad esempio, se l'intervallo di rete è **Mie macchine** e occorre accedere ai contenuti provenienti da **Tutti i tipi di dispositivi**, per una distribuzione tipica sarà necessario autenticarsi con il metodo seguente: **Nome utente e password ADFS**.

- d Fare clic su **OK** per salvare gli aggiornamenti del criterio.
 - e Nella pagina Criterio predefinito, trascinare la nuova regola all'inizio della tabella, così da porla in precedenza rispetto alle altre regole esistenti.
- 5** Utilizzando la console di gestione di Active Directory Federated Services, o un altro strumento appropriato, impostare una relazione di trust relying party con il provider di identità di vRealize Automation.

Per impostare questa relazione di trust, è necessario importare i metadati di Gestione directory precedentemente scaricati. Consultare la documentazione di Microsoft Active Directory per ulteriori informazioni sulla configurazione di ADFS (Active Directory Federated Services) per le relazioni di trust bidirezionali. Come parte del processo, è necessario eseguire le operazioni seguenti:

- Impostare una relazione di trust relying party. Nell'impostazione di questa relazione di trust, è necessario importare il file XML dei metadati del provider di servizi del provider di identità di VMware copiato e salvato.
- Creare una regola attestazioni che trasforma gli attributi recuperati da LDAP nella regola Ottieni attributi nel formato SAML desiderato. Dopo aver creato la regola, modificarla aggiungendo il testo seguente:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"vmwareidentity.domain.com");
```

Configurazione della federazione SAML tra Directories Management e SSO2

È possibile stabilire una federazione SAML tra vRealize Automation Directories Management e i sistemi che utilizzano SSO2 per supportare il Single Sign-On.

La federazione tra Directories Management e SSO2 può essere stabilita creando una connessione SAML tra le due parti. Attualmente, l'unico flusso end-to-end supportato prevede che SSO2 agisca come provider di identità (IdP) e Directories Management come provider di servizi (SP).

Per l'autenticazione utente SSO2, lo stesso account deve esistere sia in Directories Management sia in SSO2. Almeno l'UPN (UserPrincipalName) dell'utente deve corrispondere su entrambe le estremità. Gli altri attributi possono essere differenti in quanto devono identificare l'oggetto SAML.

Per gli utenti locali in SSO2, come ad esempio `admin@vsphere.local`, è necessario che esistano account corrispondenti anche in Directories Management, dove almeno l'UPN dell'utente deve coincidere. Creare tali account manualmente o con uno script utilizzando le API di creazione di utenti locali di Directories Management.

L'impostazione di SAML tra SSO2 e Directories Management prevede la configurazione dei componenti Gestione directory e SSO.

Tabella 2-4. Configurazione dei componenti della federazione SAML

Componente	Configurazione
Gestione directory	Configurare SSO2 come provider di identità di terze parti su Directories Management e aggiornare il criterio di autenticazione predefinito. Per impostare Directories Management è possibile creare uno script automatizzato.
Componente SSO2	Configurare Directories Management come provider di servizi importando il file <code>sp.xml</code> di Directories Management . Questo file consente di configurare SSO2 per utilizzare Directories Management come provider di servizi (SP).

Prerequisiti

- Configurare i tenant per la distribuzione di vRealize Automation Vedere [Creazione di tenant aggiuntivi](#).
- Impostare un collegamento Active Directory appropriato per supportare l'autenticazione di base ad Active Directory con ID utente e password.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Scaricare i metadati del provider di identità SSO2 tramite l'interfaccia utente di SSO2.
 - a Accedere a vCenter come amministratore all'indirizzo `https://<cloudvm-hostname>/`.
 - b Fare clic sul collegamento per **accedere a vSphere Web Client**.
 - c Nel riquadro di navigazione a sinistra selezionare **Amministrazione > Single Sign-On > Configurazione**.
 - d Fare clic sul controllo **Scarica** accanto all'installazione Metadati per il provider di servizi SAML.

Dovrebbe iniziare il download del file `vsphere.local.xml`.
 - e Copiare il contenuto del file `vsphere.local.xml`.
- 2 Nella pagina Provider di identità del componente Gestione directory di vRealize Automation, creare un nuovo provider di identità.
 - a Accedere a vRealize Automation come **amministratore tenant**.
 - b Selezionare **Amministrazione > Gestione directory > Provider di identità**.

- c Fare clic su **Aggiungi provider di identità** e specificare le informazioni di configurazione.

Opzione	Azione
Nome del provider di identità	Immettere il nome del nuovo provider di identità.
Casella di testo Metadati provider di identità (URI o XML)	Incollare i contenuti del file di metadati <code>idp.xml</code> di SSO2 nella casella di testo e fare clic su Elabora metadati IDP .
Nome del criterio ID nome nella richiesta SAML (facoltativo)	Immettere <code>http://schemas.xmlsoap.org/claims/UPN</code> .
Utenti	Selezionare i domini per i quali si desidera assegnare privilegi di accesso agli utenti
Rete	Selezionare gli intervalli di rete dai quali si desidera che gli utenti abbiano privilegi di accesso. Per autenticare gli utenti da indirizzi IP, selezionare Tutti gli intervalli .
Metodi di autenticazione	Immettere il nome del metodo di autenticazione. Quindi, utilizzare il menu a discesa Contesto SAML a destra per definire la corrispondenza tra il metodo di autenticazione e <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> .
Certificato della firma SAML	Fare clic sul collegamento accanto all'intestazione Metadati SAML per scaricare i metadati di Gestione directory.

- d Salvare il file dei metadati di Gestione directory come `sp.xml`.
- e Fare clic su **Aggiungi**.
- 3** Aggiornare il relativo criterio di autenticazione utilizzando la pagina dei criteri di Gestione directory per reindirizzare l'autenticazione al provider di identità SSO2 di terze parti.
- a Selezionare **Amministrazione > Gestione directory > Criteri**.
- b Fare clic sul nome del criterio predefinito.
- c Fare clic sul metodo di autenticazione sotto l'intestazione **Regole criterio** per modificare la regola di autenticazione esistente.
- d Nella pagina Modifica regola criterio, cambiare il metodo di autenticazione da password al metodo appropriato.
- In questo caso, il metodo dovrebbe essere SSO2.
- e Fare clic su **Salva** per salvare gli aggiornamenti al criterio.
- 4** Nel riquadro di navigazione a sinistra selezionare **Amministrazione > Single Sign-On > Configurazione** e fare clic su **Aggiorna** per caricare il file `sp.xml` in vSphere.

Aggiunta di utenti o gruppi a una connessione Active Directory

È possibile aggiungere utenti o gruppi a una connessione Active Directory esistente.

Il sistema di autenticazione utenti di Gestione directory importa i dati da Active Directory quando vengono aggiunti gruppi e utenti. La velocità del trasporto dei dati dipende dai limiti di capacità di Active Directory. Questa operazione può quindi richiedere molto tempo, in base al numero di gruppi e utenti aggiunti. Per ridurre al minimo i problemi, aggiungere solo i gruppi e gli utenti necessari per un'azione di vRealize Automation. In caso di problemi, chiudere le applicazioni non necessarie e verificare che nella distribuzione sia stata allocata memoria sufficiente ad Active Directory. Se i problemi persistono, aumentare la quantità di memoria allocata ad Active Directory. Per le distribuzioni con un elevato numero di utenti e gruppi, potrebbe essere necessario allocare fino a 24 GB di memoria ad Active Directory.

Quando viene sincronizzata una distribuzione di vRealize Automation con molti utenti e gruppi, è possibile che si verifichi un ritardo prima che siano disponibili i dettagli SyncLog. Il timestamp nel file di registro può essere diverso dall'orario completo visualizzato nella console.

Se i membri di un gruppo non sono presenti nell'elenco Utenti, quando si aggiunge il gruppo da Active Directory, tali membri vengono aggiunti all'elenco. Quando si sincronizza un gruppo, gli utenti che non hanno Utenti del dominio come gruppo primario in Active Directory non vengono sincronizzati.

Nota Una volta avviata l'operazione di sincronizzazione, non è possibile annullarla.

Prerequisiti

- Connettore installato e codice di attivazione attivato. Selezionare gli attributi predefiniti obbligatori e aggiungere ulteriori attributi nella pagina Attributi utente.
- Elenco di gruppi e utenti Active Directory da sincronizzare da Active Directory.
- Per Active Directory su LDAP, le informazioni obbligatorie includono DN di base, DN di binding e password del DN di binding.
- Per l'autenticazione integrata di Windows in Active Directory, le informazioni obbligatorie sono l'indirizzo UPN dell'utente di binding del dominio e la relativa password.
- Se si accede ad Active Directory su SSL, è necessaria una copia del certificato SSL.
- Se si dispone di un'istanza di Active Directory a più foreste integrata con l'autenticazione di Windows e il gruppo locale di dominio contiene membri di foreste diverse, eseguire le operazioni seguenti. Aggiungere l'utente di binding al gruppo Amministratori del gruppo locale di dominio. In caso contrario, tali membri risulteranno mancanti dal gruppo locale di dominio.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.
- 2 Fare clic sul nome della directory desiderata.
- 3 Fare clic su **Impostazioni di sincronizzazione** per aprire la finestra di dialogo contenente le opzioni di sincronizzazione.

- 4 Fare clic sull'icona appropriata per modificare la configurazione di utenti o gruppi.

Per modificare la configurazione di gruppi:

- Per aggiungere gruppi, fare clic sull'icona **+** per aggiungere una riga per le definizioni DN del gruppo e inserire il DN del gruppo appropriato.
- Per eliminare la definizione DN di un gruppo, fare clic sull'icona **x** corrispondente.

Per modificare la configurazione di utenti:

- ◆ Per aggiungere utenti, fare clic sull'icona **+** per aggiungere una riga per la definizione DN di un utente e inserire il DN dell'utente appropriato.

Per eliminare la definizione DN di un utente, fare clic sull'icona **x** corrispondente.

- 5 Fare clic su **Salva** per salvare le modifiche senza sincronizzare immediatamente gli aggiornamenti. Fare clic su **Salva e sincronizza** per salvare le modifiche e sincronizzare immediatamente gli aggiornamenti.

Selezione degli attributi per la sincronizzazione con la directory

Quando si imposta la directory di Directories Management per la sincronizzazione con Active Directory, vengono definiti gli attributi degli utenti sincronizzati con la directory. Prima di impostare la directory, nella pagina Attributi utente è possibile specificare quali attributi predefiniti sono richiesti e, se desiderato, aggiungere attributi aggiuntivi da mettere in corrispondenza con gli attributi di Active Directory.

Quando si configura la pagina Attributi utente prima che venga creata la directory, è possibile modificare gli attributi predefiniti obbligatori rendendoli non obbligatori, contrassegnare gli attributi come obbligatori e aggiungere attributi personalizzati.

Per un elenco degli attributi mappati predefiniti, vedere [Gestione degli attributi utente sincronizzati da Active Directory](#).

Dopo aver creato la directory, è possibile modificare un attributo obbligatorio rendendolo non obbligatorio ed eliminare attributi personalizzati. Non è possibile modificare un attributo per renderlo obbligatorio.

Quando si aggiungono altri attributi per la sincronizzazione con la directory, dopo aver creato la directory, passare alla pagina Attributi mappati della directory per mappare questi attributi agli attributi di Active Directory.

Procedura

- 1 Accedere a vRealize Automation come amministratore di sistema o tenant.
- 2 Fare clic sulla scheda Amministrazione.
- 3 Selezionare **Gestione directory > Attributi utente**.
- 4 Nella sezione Attributi predefiniti esaminare l'elenco di attributi obbligatori e apportare le modifiche appropriate in modo da riflettere gli attributi obbligatori.
- 5 Nella sezione Attributi aggiungere il nome dell'attributo della directory di Directories Management all'elenco.

6 Fare clic su **Salva**.

Lo stato dell'attributo predefinito viene aggiornato e gli attributi aggiunti vengono aggiunti nell'elenco Attributi mappati della directory.

7 Dopo aver creato la directory, passare alla pagina Archivi identità e selezionare la directory.**8** Fare clic su **Impostazioni di sincronizzazione > Attributi mappati**.**9** Nel menu a discesa relativo agli attributi aggiunti, selezionare l'attributo di Active Directory con cui mappare.**10** Fare clic su **Salva**.**Risultati**

La directory viene aggiornata alla successiva sincronizzazione con Active Directory.

Aggiunta di memoria a Gestione directory

In presenza di connessioni Active Directory che contengono un gran numero di utenti o gruppi, può presentarsi la necessità di allocare memoria aggiuntiva per Directories Management.

Per impostazione predefinita, per il servizio Directories Management vengono allocati 4 GB di memoria. Una quantità del genere è sufficiente per molte piccole e medie distribuzioni. Se la connessione Active Directory utilizzata impiega un gran numero di utenti o gruppi, potrebbe essere necessario aumentare questa allocazione di memoria. Una maggiore allocazione di memoria è appropriata per sistemi con un numero di utenti maggiore di 100.000 utenti per 30 gruppi o 750 gruppi in totale. Per questi sistemi, VMwareconsiglia di aumentare a 6 GB l'allocazione di memoria di Directories Management.

La memoria di Gestione directory viene calcolata in base alla memoria totale allocata per l'appliance vRealize Automation. La tabella seguente include le allocazioni di memoria per i componenti rilevanti.

Tabella 2-5. Allocazione di memoria dell'appliance vRealize Automation

Memoria dell'appliance virtuale	Memoria servizi vRA	Memoria servizi vIDM
18 GB	3,3 GB	4 GB
24 GB	4,9 GB	6 GB
30 GB	7,4 GB	9,1 GB

Nota Le allocazioni elencate sono basate su una configurazione in cui tutti i servizi predefiniti sono abilitati e in esecuzione sull'appliance virtuale, pertanto possono variare se qualche servizio viene arrestato.

Prerequisiti

- Una connessione Active Directory appropriata che sia configurata e funzionante nella distribuzione vRealize Automation.

Procedura

- 1 Arrestare tutte le macchine in cui è in esecuzione un'appliance vRealize Automation.
- 2 Aumentare l'allocazione di memoria dell'appliance virtuale su ogni macchina.

Se si utilizza l'allocazione di memoria predefinita di 18 GB, VMware consiglia di aumentarla a 24 GB.

- 3 Riavviare le macchine in cui è in esecuzione un'appliance vRealize Automation.

Configurazione del provisioning JIT degli utenti

È possibile configurare il provisioning Just-in-Time (JIT) per supportare l'aggiunta di utenti senza eseguire la sincronizzazione da Active Directory.

Per supportare il provisioning Just-in-Time, è necessario aggiungere un provider di identità di terze parti e quindi configurare una connessione a tale provider all'interno della distribuzione di vRealize Automation per integrare Gestione directory con gli altri provider SSO tramite un protocollo SAML. Inoltre, è necessario creare una nuova directory con il nome appropriato, ad esempio Directory JIT.

Quando si abilita il provisioning Just-in-Time, è possibile aggiungere utenti Just-in-Time a un determinato gruppo personalizzato. Per supportare questa funzionalità, creare un gruppo personalizzato con i membri appropriati. Vedere [Aggiunta di utenti JIT con regole e gruppi personalizzati](#).

Nota È consigliabile non configurare il provisioning Just-in-Time nel tenant vsphere.local predefinito.

Prerequisiti

Configurare un provider di identità di terze parti appropriato per l'utilizzo con il provisioning JIT.

Procedura

1 Creare un provider di identità per il provisioning Just-in-Time.

- a Selezionare **Amministrazione > Gestione directory > Provider di identità**.
- b Fare clic su **Aggiungi provider di identità** e modificare le impostazioni dell'istanza del provider di identità.
 - Per il provisioning Just-in-Time, creare un provider di identità di terze parti.
 - Nella sezione Crea directory Just-in-Time, immettere i nomi delle directory e uno o più domini.
 - È necessario selezionare una rete per la configurazione del provider di identità di terze parti.
 - Se si utilizza un'istanza di VMware Identity Manager esterna come provider di identità di terze parti e si usa `userPrincipalName` per eseguire l'autenticazione degli utenti, è necessario modificare la configurazione della mappatura dell'ID nome per `userPrincipalName` dal valore predefinito di `x509SubjectName` a `unspecified`.

Vedere [Configurazione di una connessione a un provider di identità di terze parti](#) per ulteriori informazioni sulla creazione dei provider di identità.

2 Configurare SAML nel provider di identità Just-in-Time.

- a Copiare i metadati del provider di identità dal provider di identità.
- b In vRealize Automation, selezionare il provider di identità e incollare i metadati del provider di identità nella casella di testo **Metadati provider di identità (URL o XML)**.
- c Fare clic su **Salva**.
- d Nel menu a discesa **Criterio ID nome nella richiesta SAML (facoltativo)**, selezionare il formato appropriato.

Ad esempio, se si utilizza l'indirizzo email come identificatore univoco dell'utente, selezionare `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`.
- e Sotto l'intestazione Utenti selezionare la directory appropriata.
- f Sotto l'intestazione Rete selezionare le reti che il provider di identità deve utilizzare.
- g Specificare un nome appropriato nella casella di testo **Metodi di autenticazione**.
- h Nell'elenco a discesa **Contesto SAML**, selezionare `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`.
- i Fare clic con il pulsante destro del mouse sul collegamento **Metadati del provider di servizi** e aprirlo in una scheda del browser separata.

j Utilizzare questi metadati per configurare la connessione SAML nel provider di identità.

Se si utilizza VMware Identity Manager vedere la documentazione di VMware Identity Manager per istruzioni complete sulla configurazione di SAML.

3 Fare clic su **Aggiungi**.

La nuova directory viene creata utilizzando il nome di directory specificato.

4 Configurare il criterio di accesso di vRealize Automation.

- a Selezionare **Amministrazione > Criteri**.
- b Fare clic sull'icona + verde nella parte superiore destra della tabella delle regole dei criteri.
- c Impostare la regola del criterio da applicare agli intervalli e ai tipi di dispositivi pertinenti.
- d Selezionare il metodo di autenticazione creato durante la configurazione del provider di identità di terze parti per il provisioning JIT per il metodo di autenticazione.

Gestione degli attributi utente sincronizzati da Active Directory

La pagina Attributi utente di Gestione directory elenca gli attributi degli utenti che vengono sincronizzati tramite la connessione ad Active Directory.

Le modifiche apportate e salvate nella pagina Attributi utente vengono aggiunte alla pagina Attributi mappati nella directory di Directories Management. Le modifiche agli attributi vengono aggiornate nella directory alla successiva sincronizzazione con Active Directory.

La pagina Attributi utente elenca gli attributi di directory predefiniti che è possibile mappare con gli attributi di Active Directory. È possibile selezionare gli attributi necessari e aggiungere altri attributi di Active Directory da sincronizzare con la directory.

Tabella 2-6. Attributi di Active Directory predefiniti da sincronizzazione nella directory

Nome attributo directory	Mappatura predefinita nell'attributo di Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Aggiunge il nome di dominio completo dell'oggetto.
disabled (utente esterno disabilitato)	userAccountControl. Con flag UF_Account_Disable. Quando un account è disabilitato, gli utenti non possono accedere alle rispettive applicazioni e risorse. Le risorse per cui erano autorizzati gli utenti non vengono rimosse dall'account, così che una volta rimosso il flag dall'account, gli utenti potranno nuovamente effettuare l'accesso e accedere alle risorse autorizzate.
phone	telephoneNumber
lastName	sn
firstName	givenName

Tabella 2-6. Attributi di Active Directory predefiniti da sincronizzazione nella directory (continua)

Nome attributo directory	Mappatura predefinita nell'attributo di Active Directory
email	mail
userName	sAMAccountName

La pagina Attributi utente elenca gli attributi di directory predefiniti che è possibile mappare con gli attributi di Active Directory. È possibile selezionare gli attributi necessari e aggiungere altri attributi di Active Directory da sincronizzare con la directory.

Tabella 2-7. Attributi di Active Directory predefiniti da sincronizzazione nella directory

Nome attributo directory	Mappatura predefinita nell'attributo di Active Directory
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Aggiunge il nome di dominio completo dell'oggetto.
disabled (utente esterno disabilitato)	userAccountControl. Con flag UF_Account_Disable. Quando un account è disabilitato, gli utenti non possono accedere alle rispettive applicazioni e risorse. Le risorse per cui erano autorizzati gli utenti non vengono rimosse dall'account, così che una volta rimosso il flag dall'account, gli utenti potranno nuovamente effettuare l'accesso e accedere alle risorse autorizzate.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName

Gestione di connettori e cluster di connettori

La pagina Connettori elenca i connettori distribuiti per la rete dell'azienda. Il compito di un connettore è di sincronizzare i dati di utenti e gruppi tra Active Directory e il servizio Gestione directory e, quando utilizzato come provider di identità, di autenticare gli utenti nel servizio.

In vRealize Automation, tutte le Appliance vRealize Automation contengono i propri connettori, che sono adatti per la maggior parte delle distribuzioni.

Quando si associa una directory a un'istanza di connettore, il connettore crea una partizione per la directory associata, chiamata Worker. A un'istanza di connettore possono essere associati più Worker. Ciascun Worker agisce come provider di identità. Il connettore sincronizza i dati di utenti e gruppi tra Active Directory e il servizio attraverso uno o più Worker. È possibile definire e configurare metodi di autenticazione in base ai singoli Worker.

Dalla pagina Connettori è possibile gestire svariati aspetti di un collegamento ad Active Directory. Questa pagina contiene una tabella e diversi pulsanti che consentono di eseguire svariate attività di gestione.

- Nella colonna appropriata selezionare un Worker per visualizzare i dettagli del connettore e navigare fino alla pagina Adattatori autenticazione per controllare lo stato dei metodi di autenticazione disponibili. Per informazioni sull'autenticazione, vedere [Integrazione di prodotti di autenticazione dell'utente alternativi con Gestione directory](#).
- Nella colonna Provider di identità, selezionare il provider da visualizzare, modificare o disattivare. Vedere [Configurazione di una connessione a un provider di identità di terze parti](#).
- Nella colonna Directory associata, accedere alla directory associata a questo Worker.
- Fare clic su **Aggiungi a dominio** per aggiungere il connettore a un dominio Active Directory specifico. Ad esempio, quando si configura l'autenticazione Kerberos, è necessario unirsi a un dominio Active Directory che contiene utenti o che ha una relazione basata sulla fiducia con domini contenenti utenti.
- Quando si configura una directory con una Active Directory con autenticazione integrata di Windows, il connettore si unisce al dominio in base ai dettagli di configurazione.

Connettori in un ambiente in clustering

In una distribuzione di vRealize Automation distribuita le autorizzazioni utente richieste vengono eseguite da tutti i connettori disponibili, mentre un unico connettore designato gestisce la sincronizzazione dell'intera configurazione. La sincronizzazione in genere prevede aggiunte, eliminazioni o modifiche nella configurazione utente e avviene automaticamente appena diventano disponibili tutti i connettori. In alcune situazioni specifiche la sincronizzazione automatica potrebbe non verificarsi.

Per le modifiche correlate alla configurazione delle directory, ad esempio il DN di base, vRealize Automation prova a eseguire automaticamente il push degli aggiornamenti in tutti i connettori di un cluster. Un connettore che per qualche motivo sia inutilizzabile o irraggiungibile non riceverà l'aggiornamento, anche una volta ripreso il funzionamento online. Per implementare le modifiche di configurazione nei connettori che potrebbero non averle ricevute automaticamente, gli amministratori di sistema devono salvarle manualmente in tutti i connettori applicabili.

Anche per le modifiche correlate al profilo di sincronizzazione delle directory, vRealize Automation prova a eseguire automaticamente il push degli aggiornamenti in tutti i connettori. Se il connettore di sincronizzazione è operativo, l'aggiornamento viene salvato e ne viene eseguito il push in tutti i connettori di autorizzazione disponibili. Se uno o più connettori sono irraggiungibili, l'amministratore di sistema riceve un avviso che segnala che l'aggiornamento non è stato eseguito su tutti i connettori. Se il connettore di sincronizzazione non è operativo,

L'aggiornamento non riesce e si verifica un errore. Se l'amministratore di sistema imposta il connettore designato come connettore di sincronizzazione, il nuovo connettore di sincronizzazione riceve le informazioni di profilo più recenti disponibili di cui viene eseguito il push in tutti i connettori applicabili e disponibili.

Unione della macchina con un connettore a un dominio

In alcuni casi, potrebbe essere necessario unire una macchina contenente un connettore di Gestione directory a un dominio.

Per Active Directory su directory LDAP, è possibile unire un dominio dopo aver creato la directory. Per directory Active Directory (autenticazione integrata di Windows), il connettore viene automaticamente unito al dominio quando viene creata la directory. In entrambi i casi, è necessario fornire le credenziali opportune.

Per effettuare l'unione a un dominio, sono necessarie le credenziali di Active Directory, che hanno il privilegio di unire il computer a un dominio AD. In Active Directory questo è configurato con i seguenti diritti:

- Creare oggetti computer
- Eliminare oggetti computer

Quando si effettua l'unione a un dominio, in Active Directory viene creato un oggetto computer nella posizione predefinita.

Se l'utente non dispone dei diritti per effettuare l'unione a un dominio oppure se i criteri dell'azienda richiedono che l'oggetto del computer disponga di una posizione personalizzata, è necessario chiedere all'amministratore di creare l'oggetto e di unire la macchina con il connettore al dominio.

Procedura

- 1 Chiedere all'amministratore di Active Directory di creare l'oggetto del computer in Active Directory, in una posizione determinata dai criteri dell'azienda. È necessario fornire il nome dell'host del connettore. Assicurarsi di fornire il nome di dominio completo, ad esempio `server.example.com`.

È possibile trovare il nome dell'host nella colonna Nome host della pagina Connettori, all'interno della console di amministrazione. Selezionare **Amministrazione > Gestione directory > Connettori**.

- 2 Una volta creato l'oggetto del computer, fare clic sul comando di **unione del dominio** nella pagina Connettori per unire il dominio utilizzando qualsiasi account dell'utente di dominio disponibile in Gestione directory.

Informazioni sulla selezione dei controller di dominio

Gestione directory conserva un elenco dinamico di controller di dominio che non richiedono alcuna configurazione utente.

Gestione directory provvede periodicamente ad aggiornare, individuare nuovamente e riordinare i controller di dominio in base al ping LDAP e li archivia in un file `domain_krb.properties` e in un file `krb5.conf` personalizzato. Il controller di dominio migliore è elencato per primo e viene quindi utilizzato per tutti gli scopi, come le operazioni di autenticazione e sincronizzazione. Se il controller di dominio non risponde entro 10 ms, l'elenco dei controller di dominio viene nuovamente aggiornato. Ciò consente a Gestione directory di utilizzare in modo coerente i controller di dominio ottimali, anche quando si verificano errori dei controller di dominio.

Gestione dei criteri di accesso

I criteri di Directories Management sono un insieme di regole che definiscono quali sono i criteri da soddisfare affinché gli utenti possano accedere al proprio portale di app o avviare applicazioni Web specificate.

È possibile creare una regola come parte di un criterio. Ogni regola di un criterio può specificare le seguenti informazioni.

- L'intervallo di rete da cui è consentito l'accesso degli utenti, ad esempio dall'interno o dall'esterno della rete dell'azienda.
- Il tipo di dispositivo che può accedere tramite questo criterio.
- L'ordine di applicazione dei metodi di autenticazione abilitati.
- Il numero di ore di validità dell'autenticazione.
- Messaggio di accesso negato personalizzato.

Nota i criteri non controllano la durata di una sessione di applicazione Web. Essi controllano quanto tempo hanno gli utenti per avviare un'applicazione Web.

Il servizio Directories Management include un criterio di predefinito che è possibile modificare. Questo criterio controlla l'accesso al servizio nel suo complesso. Vedere [Applicazione del criterio di accesso predefinito](#). Per controllare l'accesso a specifiche applicazioni Web, è possibile creare criteri aggiuntivi. Se non si applica un criterio a un'applicazione Web, viene applicato il criterio predefinito.

Configurazione delle impostazioni dei criteri di accesso

Un criterio contiene una o più regole di accesso. Ciascuna regola è costituita da impostazioni che è possibile configurare per gestire l'accesso degli utenti ai propri portali di applicazioni nel loro insieme o solo ad applicazioni Web specificate.

Intervallo di rete

Per ogni regola, si determina la base degli utenti specificando un intervallo di rete. Un intervallo di rete è costituito da uno o più intervalli IP. Gli intervalli di rete vengono creati dalla scheda Gestione accesso e identità della pagina Impostazione > Intervalli di rete prima di configurare i set dei criteri di accesso.

Tipo di dispositivo

Selezionare il tipo di dispositivo gestito dalla regola. I tipi di client sono browser Web, l'app Identity Manager Client, iOS, Android e Tutti i tipi di dispositivi.

Aggiungi gruppi

È possibile applicare criteri diversi per l'autenticazione in base all'appartenenza al gruppo degli utenti. Per fare in modo che gruppi di utenti possano accedere tramite un flusso di autenticazione specifico, è possibile aggiungere gruppi alla regola dei criteri di accesso. È possibile sincronizzare i gruppi dalla directory aziendale o da gruppi locali creati nella console dell'amministratore. I nomi dei gruppi devono essere univoci all'interno dello stesso dominio.

Per utilizzare gruppi nelle regole dei criteri di accesso, configurare un nuovo criterio da Gestione directory > pagina Criteri e selezionare i gruppi desiderati per il criterio. Il criterio deve essere mappato nella pagina Attributi utente e poi sincronizzato con la directory.

Quando i gruppi vengono utilizzati in una regola dei criteri di accesso, l'esperienza di accesso dell'utente cambia. Anziché richiedere agli utenti di selezionare il proprio dominio e immettere le credenziali, viene visualizzata una pagina che richiede agli utenti di immettere il proprio identificatore univoco. Directories Management individua l'utente nel database interno, in base all'identificatore univoco, e visualizza la pagina di autenticazione configurata nella regola.

Se non viene selezionato alcun gruppo, la regola dei criteri di accesso viene applicata a tutti gli utenti. Quando si configurano regole dei criteri di accesso che includono regole basate sui gruppi e una regola per tutti gli utenti, assicurarsi che la regola designata per tutti gli utenti sia l'ultima elencata nella sezione Regole criterio del criterio.

Consultare la documentazione di VMware Identity Manager sull'esperienza di accesso utilizzando l'identificatore univoco per ulteriori informazioni sull'applicazione delle regole agli utenti.

Metodi di autenticazione

Impostare la priorità dei metodi di autenticazione per la regola dei criteri. I metodi di autenticazione vengono applicati nell'ordine in cui sono elencati. Viene selezionata la prima istanza del provider di identità che soddisfa la configurazione del metodo di autenticazione e dell'intervallo di rete nel criterio e la richiesta di autenticazione dell'utente viene inoltrata all'istanza del provider di identità per l'autenticazione. Se l'autenticazione non riesce, viene selezionato il metodo di autenticazione successivo nell'elenco. Se si utilizza l'autenticazione Certificato, questo metodo deve essere il primo metodo di autenticazione nell'elenco.

È possibile configurare le regole dei criteri di accesso in modo che gli utenti debbano passare le credenziali tramite due metodi di autenticazione per poter eseguire l'accesso. Se uno o entrambi i metodi di autenticazione restituiscono un errore e sono configurati anche i metodi di fallback, agli utenti viene richiesto di immettere le proprie credenziali per i successivi metodi di autenticazione configurati. I due scenari seguenti descrivono come funziona il concatenamento delle autenticazioni.

- Nel primo scenario la regola dei criteri di accesso viene configurata in modo da richiedere agli utenti di autenticarsi con la propria password e con le credenziali Kerberos. L'autenticazione di fallback viene impostata per richiedere la password e le credenziali RADIUS per

l'autenticazione. Un utente immette la password correttamente, ma non riesce a immettere le credenziali di autenticazione Kerberos corrette. Poiché l'utente ha immesso la password corretta, la richiesta di autenticazione di fallback si riferisce solo alle credenziali RADIUS. L'utente non deve immettere di nuovo la password.

- Nel secondo scenario la regola dei criteri di accesso viene configurata in modo da richiedere agli utenti di autenticarsi con la propria password e con le credenziali Kerberos. L'autenticazione di fallback è impostata per richiedere le credenziali RSA SecurID e RADIUS per l'autenticazione. Un utente immette la password correttamente, ma non riesce a immettere le credenziali di autenticazione Kerberos corrette. La richiesta di autenticazione di fallback si riferisce sia alle credenziali RSA SecurID sia alle credenziali RADIUS per l'autenticazione.

Durata della sessione di autenticazione

Per ogni regola è possibile impostare il periodo di validità dell'autenticazione. Il valore determina la quantità di tempo massima di cui gli utenti dispongono dopo l'ultimo evento di autenticazione per accedere al proprio portale o per avviare un'applicazione Web specifica. Ad esempio, il valore 4 nella regola di un'applicazione Web offre agli utenti quattro ore per avviare l'applicazione Web, a meno che non inizializzino un altro evento di autenticazione che estende il tempo.

Messaggio di errore personalizzato di accesso negato

Quando gli utenti tentano di accedere, invano, a causa di credenziali non valide, errore di configurazione o di sistema, viene visualizzato un messaggio di accesso negato. Il messaggio predefinito è

Accesso negato non essendo stato trovato alcun metodo di autenticazione valido.

È possibile creare un messaggio d'errore personalizzato per ogni regola di criterio di accesso che sovrascrive il messaggio predefinito. Il messaggio personalizzato può comprendere testo e un collegamento a un messaggio che invita a eseguire un'azione. Ad esempio nelle regole per un criterio per i dispositivi mobili che si desidera gestire, se un utente tenta di accedere da un dispositivo non registrato, potrebbe apparire il seguente messaggio d'errore personalizzato:

Registrare il dispositivo per accedere alle risorse aziendali facendo clic sul collegamento alla fine di questo messaggio. Se il dispositivo è già registrato, contattare il supporto per assistenza.

Esempio di criterio predefinito

Il criterio seguente è un esempio di come sia possibile configurare il criterio predefinito per controllare l'accesso al portale delle app. Vedere [Gestione del criterio di accesso utente](#).

Le regole dei criteri vengono valutate nell'ordine in cui sono elencate. È possibile modificare l'ordine del criterio trascinando e rilasciando la regola nella sezione Regole dei criteri.

Nel caso di utilizzo seguente l'esempio di criterio è valido per tutte le applicazioni.

CRITERIO PREDEFINITO

* Nome del criterio: default_access_policy_set

Descrizione: Default access policy set

Applicabile a: Tutte le applicazioni

Regole del criterio

È possibile creare un elenco di regole per accedere a queste applicazioni Web. Per ciascuna regola selezionare l'intervallo di rete IP, il tipo di dispositivi cui è consentito accedere all'applicazione, i metodi e l'ordine di autenticazione e il numero massimo di ore per cui gli utenti possono utilizzare l'applicazione prima di autenticarsi nuovamente.

Intervallo di rete	Tipo di dispositivo	Metodo di autenticazione	Nuova autenticazione	
TUTTI GLI INTERVALLI	Browser Web	Password	8 Ore	✗ +
TUTTI GLI INTERVALLI	Applicazione client Identity Manager	Password	2160 Ore	✗ +

- Per la rete interna (Intervallo di rete interna), vengono configurati due metodi di autenticazione per la regola, Kerberos e autenticazione tramite password come metodo di fallback. Per accedere al portale delle app da una rete interna, il servizio prova innanzitutto ad autenticare gli utenti con l'autenticazione Kerberos, poiché si tratta del primo metodo di autenticazione elencato nella regola. Se l'operazione non riesce, agli utenti viene chiesto di immettere la propria password di Active Directory. Gli utenti accedono utilizzando un browser e possono accedere ai propri portali utente per una sessione di otto ore.
 - Per l'accesso dalla rete esterna (Tutti gli intervalli), è configurato un solo metodo di autenticazione, ovvero RSA SecurID. Per accedere al portale delle app da una rete esterna, gli utenti devono accedere con SecurID. Gli utenti accedono utilizzando un browser e possono accedere ai propri portali delle app per una sessione di quattro ore.
- Quando un utente tenta di accedere a una risorsa, tranne che per le applicazioni Web coperte da un criterio specifico delle applicazioni Web, viene applicato il criterio di accesso al portale predefinito.

Ad esempio, l'intervallo di tempo per la riautenticazione di queste risorse corrisponde all'intervallo di tempo per la riautenticazione della regola del criterio di accesso predefinita. Se l'intervallo di tempo per un utente che accede al portale delle app è otto ore in base alla regola del criterio di accesso predefinita, quando l'utente tenta di avviare una risorsa durante la sessione, l'applicazione viene avviata senza richiedere la riautenticazione dell'utente.

Configurazione di un criterio di accesso basato sul gruppo

È possibile configurare un criterio di accesso basato sul gruppo per controllare i privilegi di accesso in base alle assegnazioni ai gruppi.

Gestione directory contiene i criteri di accesso predefiniti che supportano tutti i gruppi e tutti gli intervalli di rete. È possibile modificare questi criteri in modo che siano più restrittivi oppure creare nuovi criteri per supportare criteri di accesso diversi.

Procedura

1 Aggiungere gruppi al criterio desiderato.

- a Selezionare **Amministrazione > Gestione directory > Criteri**.
- b È possibile aprire il criterio di accesso predefinito o crearne uno nuovo.
- c Modificare la regola del criterio configurata con un tipo di dispositivo del browser Web.

Per modificare un criterio, fare clic sul metodo di autenticazione. Per impostazione predefinita, sono presenti due regole dei criteri che si applicano a tutti gli indirizzi IP e tutti gli utenti.

Viene aperta la pagina Modifica regola del criterio per il criterio selezionato. È possibile modificare vari parametri, come intervallo di rete, tipo di dispositivo, metodi di autenticazione e altri parametri della regola del criterio.

- d Fare clic su **Modifica gruppi** nella pagina Modifica regola del criterio per visualizzare tutti i gruppi disponibili per l'uso con il criterio.

In questa pagina sono visualizzati tutti i gruppi associati al tenant.

- e Selezionare i gruppi da associare al criterio.
- f Fare clic su **OK**.

I gruppi selezionati vengono visualizzati nella pagina Modifica regola del criterio.

- g Fare clic su **OK** nella pagina Modifica regola del criterio per salvare le modifiche apportate alla regola del criterio.

Viene visualizzata la pagina Criteri, che indica il numero di gruppi selezionati per il criterio.

- h Fare clic su **Salva** nella pagina Criteri.

2 Configurare un intervallo di rete per il criterio di gruppo.

- a Selezionare **Amministrazione > Gestione directory > Intervalli di rete**.

Per impostazione predefinita, esiste un'impostazione predefinita di All Ranges valida per tutti gli indirizzi IP di tutti gli intervalli di rete. È possibile creare un nuovo intervallo di rete o modificarne uno esistente.

- b Fare clic su **Aggiungi intervallo di rete**.

Viene aperta la pagina Modifica intervallo di rete.

- c Immettere un **Nome** per il nuovo intervallo di rete e aggiungere una **Descrizione**, se necessario.

Risultati

Quando gli utenti accedono a vRealize Automation, devono selezionare il dominio e immettere un nome utente e una password validi. Se nel criterio applicabile viene specificato un gruppo, gli utenti validi devono comunque immettere un nome utente e password.


Gestione di criteri specifici di applicazioni Web

Quando si aggiungono applicazioni Web al catalogo, è possibile creare criteri di accesso specifici di applicazioni Web. Per un'applicazione Web è ad esempio possibile creare un criterio con regole che specifichi gli indirizzi IP che possono accedere all'applicazione, nonché quali metodi di autenticazione possono utilizzare e per quanto tempo finché non verrà richiesta una nuova autenticazione.

Il seguente criterio specifico di applicazione Web è un esempio di criterio che si può creare per controllare gli accessi ad applicazioni Web specificate.

Esempio 1: criterio specifico di applicazione Web rigido

In questo esempio viene creato e applicato un nuovo criterio a un'applicazione Web sensibile.



Sensitive Web Application
 To be applied to Web application that should have limited access.

Elimina criterio

Nome del criterio*

Descrizione

Applicabile a

Selezionare nel catalogo le applicazioni per cui questo criterio è valido.

Modifica applicazioni

Regole del criterio

È possibile creare un elenco di regole per accedere a queste applicazioni. Per ogni regola, selezionare l'intervallo di rete IP, il tipo di dispositivi che possono accedere alle applicazioni, l'ordine di autenticazione e dei metodi, nonché il numero massimo di ore per cui gli utenti possono utilizzare l'applicazione prima di dover eseguire nuovamente l'autenticazione.

Intervallo di rete	Tipo di dispositivo	Metodo di autent...	Nuova autentic...	Gruppi	
Internal Network	Browser Web	Prima, provare: Kerberos e altri 1 fallback...	8 Ore	Tutti gli utenti	✖ +
TUTTI GLI INTERVALLI	Browser Web	SecurId	4 Ore	Tutti gli utenti	✖ +

Salva

Annulla

- 1 Per accedere al servizio dall'esterno della rete dell'impresa, l'utente deve accedere con RSA SecurID. L'utente accede utilizzando un browser e può quindi accedere al portale delle applicazioni per una sessione di quattro ore, secondo quanto definito nella regola di accesso predefinita.
- 2 Dopo quattro ore, l'utente tenta di avviare un'applicazione Web con il criterio delle applicazioni Web sensibili applicato.
- 3 Il servizio controlla le regole nel criterio e lo applica nell'intervallo di rete TUTTI GLI INTERVALLI, dato che la richiesta dell'utente proviene da un browser Web e dall'intervallo di rete TUTTI GLI INTERVALLI.

L'utente accede utilizzando il metodo di autenticazione RSA SecurID, ma la sessione è appena scaduta. L'utente viene reindirizzato per eseguire nuovamente l'autenticazione. La nuova autenticazione fornisce all'utente un'altra sessione di quattro ore e la possibilità di avviare l'applicazione. Per le successive quattro ore l'utente può continuare ad avviare l'applicazione senza doversi riautenticare.

Esempio 2: criterio specifico di applicazione Web più rigido

Per applicare una regola ancora più rigida ad applicazioni Web più sensibili, è possibile richiedere la riautenticazione con SecureId su qualsiasi dispositivo dopo 1 ora. Il seguente esempio illustra come viene implementato questo tipo di regola del criterio di accesso:

- 1 L'utente accede dall'interno della rete dell'azienda utilizzando il metodo di autenticazione con password.

A questo punto, l'utente ha accesso al portale delle applicazioni per otto ore, come definito nell'Esempio 1.

- 2 L'utente tenta immediatamente di avviare un'applicazione Web con la regola del criterio dell'Esempio 2 applicata, la quale richiede l'autenticazione RSA SecurID.
- 3 L'utente viene reindirizzato a un provider di identità che fornisce l'autenticazione RSA SecurID.
- 4 Dopo il corretto accesso dell'utente, il servizio avvia l'applicazione e salva l'evento di autenticazione.

L'utente può continuare ad avviare l'applicazione per un'ora, ma trascorso questo tempo gli verrà richiesto di riautenticarsi, come definito dalla regola del criterio.

Gestione del criterio di accesso utente

vRealize Automation rende disponibile un criterio di accesso utente predefinito, utilizzabile così com'è o modificabile secondo le proprie esigenze, che consente di gestire l'accesso del tenant alle applicazioni.

vRealize Automation rende disponibile un criterio di accesso utente predefinito e non è possibile aggiungere nuovi criteri. È possibile modificare il criterio esistente per aggiungere regole.

Prerequisiti

- Selezionare o configurare i provider di identità appropriati per la distribuzione. Vedere [Configurazione di una connessione a un provider di identità di terze parti](#).
- Configurare gli intervalli di rete appropriati per la distribuzione. Vedere [Aggiunta o modifica di un intervallo di rete](#).
- Configurare i metodi di autenticazione appropriati per la distribuzione. Vedere [Integrazione di prodotti di autenticazione dell'utente alternativi con Gestione directory](#).
- Se si prevede di modificare il criterio predefinito (per controllare l'accesso degli utenti al servizio nel suo insieme), configurarlo prima di creare il criterio specifico per l'applicazione Web.

- Aggiungere applicazioni Web al catalogo. Le applicazioni Web devono essere elencate nella pagina Catalogo prima di poter aggiungere un criterio.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Criteri**.
- 2 Fare clic su **Modifica criterio** per aggiungere un nuovo criterio.
- 3 Aggiungere un nome e una descrizione per il criterio nelle rispettive caselle di testo.
- 4 Nella sezione Si applica a, fare clic su **Seleziona** e, nella pagina visualizzata, selezionare le applicazioni Web associate a questo criterio.
- 5 Nella sezione Regole criterio, fare clic su **+** per aggiungere una regola.
Viene visualizzata la pagina Aggiungi una regola del criterio.
 - a Selezionare l'intervallo di rete a cui applicare la regola.
 - b Selezionare il tipo di dispositivo che può accedere alle applicazioni Web per questa regola.
 - c Selezionare i metodi di autenticazione da utilizzare nell'ordine con cui devono essere applicati.
 - d Specificare il numero di ore di apertura di una sessione dell'applicazione Web.
 - e Fare clic su **Salva**.
- 6 Configurare le eventuali regole aggiuntive desiderate.
- 7 Fare clic su **Salva**.

Configurazione di connessioni di provider di identità aggiuntive

È possibile configurare connessioni di provider di identità aggiuntive in base alle esigenze per supportare diversi scenari di gestione delle identità, inclusi i provider di identità integrati aggiuntivi e i provider di identità di terze parti.

È possibile creare tre tipi di connessioni di provider di identità utilizzando Gestione directory.

- Crea provider di identità di terze parti: utilizzare questo elemento per creare una connessione a un provider di identità di terze parti esterno. Assicurarsi che siano soddisfatte le condizioni seguenti prima di aggiungere un'istanza del provider di identità di terze parti.
 - Verificare che le istanze di terze parti siano conformi con SAML 2.0 e che il servizio possa raggiungere l'istanza di terze parti.
 - Ottenere le informazioni sui metadati di terze parti appropriate da aggiungere durante la configurazione del provider di identità nella console di amministrazione. Le informazioni sui metadati ottenute dall'istanza di terze parti corrispondono all'URL dei metadati o ai metadati effettivi.

- Crea provider di identità Workspace: quando si abilita un connettore per l'autenticazione degli utenti durante la configurazione di Gestione directory, viene creato un provider di identità Workspace come provider di identità e viene abilitata l'autenticazione tramite password. È possibile configurare provider di identità Workspace aggiuntivi con bilanciamenti del carico diversi.
- Crea provider di identità integrato: i provider di identità integrati utilizzano i meccanismi di Gestione directory interni per supportare l'autenticazione. È possibile configurare i provider di identità integrati per l'utilizzo di metodi di autenticazione che non richiedano l'uso di un connettore locale. Quando si configura il provider integrato, si associano i metodi di autenticazione da utilizzare con il provider.
- **Configurazione di una connessione a un provider di identità di terze parti**
vRealize Automation viene fornito con un'istanza di connessione al provider di identità predefinita. Gli utenti possono creare ulteriori connessioni a provider di identità per supportare il provisioning utente just-in-time o altre configurazioni personalizzate.
- **Configurazione di provider di identità Workspace aggiuntivi**
Quando si configura un connettore di Gestione directory per l'autenticazione degli utenti, viene creato un provider di identità Workspace e viene abilitata l'autenticazione tramite password.
- **Configurazione della connessione di un provider di identità integrato**
È possibile configurare più provider di identità integrati e associarli a metodi di autenticazione.

Configurazione di una connessione a un provider di identità di terze parti

vRealize Automation viene fornito con un'istanza di connessione al provider di identità predefinita. Gli utenti possono creare ulteriori connessioni a provider di identità per supportare il provisioning utente just-in-time o altre configurazioni personalizzate.

vRealize Automation viene fornito con un provider di identità predefinito. Nella maggior parte dei casi, il provider predefinito è sufficiente per soddisfare le esigenze dei clienti. Se si utilizza una soluzione di gestione delle identità di livello enterprise, è possibile configurare un provider di identità personalizzato per reindirizzare gli utenti alla propria soluzione esistente.

Quando si utilizza un provider delle identità personalizzato, Gestione directory utilizza i metadata SAML del provider per stabilire con il provider una relazione basata sulla fiducia. Una volta stabilita questa relazione, Gestione directory mappa gli utenti dall'asserzione SAML all'elenco di utenti vRealize Automation interni basato sull'ID del nome del soggetto.

Prerequisiti

- Configurare gli intervalli di rete che si desidera indirizzare a questa istanza di provider di identità per l'autenticazione. Vedere [Aggiunta o modifica di un intervallo di rete](#).
- Accedere al documento dei metadati di terze parti, che può corrispondere all'URL dei metadati o ai metadati effettivi.

- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Provider di identità**.

In questa pagina vengono visualizzati tutti i provider di identità configurati.

- 2 Fare clic su **Aggiungi provider di identità**.

Viene visualizzato un menu con le opzioni relative al provider di identità.

- 3 Selezionare **Crea IDP di terze parti**.

- 4 Immettere le informazioni appropriate per configurare il provider di identità.

Opzione	Descrizione
Nome del provider di identità	Immettere un nome per l'istanza del provider di identità.
Metadati SAML	<p>Aggiungere il documento dei metadati basati su XML IdP di terze parti per stabilire una relazione di fiducia con il provider di identità.</p> <ol style="list-style-type: none"> 1 Immettere l'URL dei metadati SAML o il contenuto XML nella casella di testo. 2 Fare clic su Elabora metadati IdP. I formati NameID supportati da IdP vengono estratti dai metadati e aggiunti alla tabella Formato ID nome. 3 Nella colonna del valore ID del nome selezionare l'attributo utente del servizio da mappare ai formati degli ID visualizzati. È possibile aggiungere formati di ID di nome di terze parti personalizzati e mapparli ai valori degli attributi utente nel servizio. 4 (Facoltativo) Selezionare il formato della stringa dell'identificatore di risposta NameIDPolicy.
Utenti	Selezionare le directory Directories Management degli utenti che possono autenticarsi utilizzando questo provider di identità.
Provisioning utente Just-in-Time	<p>Selezionare le opzioni appropriate per supportare il provisioning just-in-time utilizzando un provider di identità di terze parti idoneo.</p> <p>In Nome directory immettere il nome della directory da utilizzare per il provisioning just-in-time.</p> <p>Immettere uno o più Domini esistenti nel provider di identità esterno che verrà utilizzato per il provisioning just-in-time.</p>
Rete	<p>Sono elencati gli intervalli di rete esistenti configurati nel servizio.</p> <p>Selezionare, in base ai rispettivi indirizzi IP, gli intervalli di rete degli utenti che si desidera indirizzare a questa istanza di provider di identità per l'autenticazione.</p>
Metodi di autenticazione	<p>Aggiungere i metodi di autenticazione supportati dal provider di identità di terze parti.</p> <p>Selezionare la classe del contesto di autenticazione SAML che supporta il metodo di autenticazione.</p>

Opzione	Descrizione
Certificato della firma SAML	Fare clic su Metadati del provider di servizi (SP) per visualizzare l'URL dei metadati del provider di servizi SAML Directories Management. Copiare e salvare l'URL. Questo URL viene configurato quando si modifica l'asserzione SAML nel provider di identità di terze parti per mappare gli utenti di Directories Management.
Nome host	Se viene visualizzato il campo Nome host , immettere il nome host al quale il provider di identità viene reindirizzato per l'autenticazione. Se si utilizza una porta non standard diversa dalla porta 443, è possibile impostare questo valore nel formato Nome host:Porta. Ad esempio, myco.example.com:8443.

5 Fare clic su **Aggiungi**.

Operazioni successive

- Copiare e salvare i metadati del provider di servizi Directories Management necessario per configurare l'istanza del provider di identità di terze parti. Questi metadati sono disponibili nella sezione Certificato di firma SAML della pagina Provider di identità.
- Aggiungere il metodo di autenticazione del provider di identità al criterio predefinito dei servizi.

Per informazioni sull'aggiunta e la personalizzazione delle risorse aggiunte al catalogo, vedere la guida *Setting Up Resources in Directories Management*.

Configurazione di provider di identità Workspace aggiuntivi

Quando si configura un connettore di Gestione directory per l'autenticazione degli utenti, viene creato un provider di identità Workspace e viene abilitata l'autenticazione tramite password.

È possibile configurare connettori aggiuntivi in modo che funzionino con più bilanciamenti del carico. Quando la distribuzione contiene più bilanciamenti del carico, è possibile configurare un provider di identità Workspace aggiuntivo per l'autenticazione in ogni configurazione del bilanciamento del carico.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Provider di identità**.

In questa pagina vengono visualizzati tutti i provider di identità configurati.

- 2 Fare clic su **Aggiungi provider di identità**.

Viene visualizzato un menu con le opzioni relative al provider di identità.

- 3 Selezionare **Crea provider di identità Workspace**.

4 Immettere le informazioni appropriate per configurare il provider di identità.

Opzione	Descrizione
Nome del provider di identità	Immettere il nome per l'istanza del provider di identità integrato.
Utenti	Selezionare gli utenti di cui eseguire l'autenticazione. Vengono elencate le directory configurate.
Utenti	Selezionare i gruppi di utenti che possono eseguire l'autenticazione utilizzando questo provider di identità Workspace.
Rete	Sono elencati gli intervalli di rete esistenti configurati nel servizio. Selezionare l'intervallo di rete per gli utenti in base agli indirizzi IP che si desidera indirizzare a questa istanza del provider di identità per l'autenticazione.
Metodi di autenticazione	Vengono visualizzati i metodi di autenticazione configurati per il servizio. Selezionare le caselle di controllo relative ai metodi di autenticazione da associare a questo provider di identità. Per la conformità del dispositivo e la password, con AirWatch e AirWatch Connector, assicurarsi che l'opzione sia abilitata nella pagina di configurazione di AirWatch.

5 Fare clic su **Aggiungi**.

Configurazione della connessione di un provider di identità integrato

È possibile configurare più provider di identità integrati e associarli a metodi di autenticazione.

Prerequisiti

Se si utilizza l'autenticazione Kerberos integrata, scaricare il certificato dell'emittente KDC da utilizzare nella configurazione del profilo di gestione del dispositivo iOS in AirWatch.

Procedura

1 Selezionare **Amministrazione > Gestione directory > Provider di identità**.

In questa pagina vengono visualizzati tutti i provider di identità configurati.

2 Fare clic su **Aggiungi provider di identità**.

Viene visualizzato un menu con le opzioni relative al provider di identità.

3 Selezionare **Crea provider di identità integrato**.

4 Immettere le informazioni appropriate per configurare il provider di identità.

Opzione	Descrizione
Nome del provider di identità	Immettere il nome per l'istanza del provider di identità integrato.
Utenti	Selezionare gli utenti di cui eseguire l'autenticazione. Vengono elencate le directory configurate.

Opzione	Descrizione
Rete	Sono elencati gli intervalli di rete esistenti configurati nel servizio. Selezionare l'intervallo di rete per gli utenti in base agli indirizzi IP che si desidera indirizzare a questa istanza del provider di identità per l'autenticazione.
Metodi di autenticazione	<p>Vengono visualizzati i metodi di autenticazione configurati per il servizio. Selezionare le caselle di controllo relative ai metodi di autenticazione da associare a questo provider di identità.</p> <p>Per la conformità del dispositivo e la password, con AirWatch e AirWatch Connector, assicurarsi che sia abilitata l'opzione appropriata nella pagina di configurazione di AirWatch.</p>

5 Fare clic su **Aggiungi**.

Integrazione di prodotti di autenticazione dell'utente alternativi con Gestione directory

Generalmente, durante la configurazione iniziale di Gestione directory, si utilizzano i connettori forniti con l'infrastruttura esistente di vRealize Automation per creare una connessione Active Directory per la gestione e l'autenticazione basata su ID utente e password. In alternativa, è possibile integrare Gestione directory con altre soluzioni di autenticazione come Kerberos o RSA SecurID.

L'istanza del provider di identità può essere l'istanza del Directories Managementconnettore, istanze di provider di identità di terze parti o una combinazione di entrambe.

L'istanza del provider di identità utilizzata con il servizio Directories Management crea un'autorità di federazione nella rete che comunica con il servizio utilizzando le asserzioni SAML 2.0.

Quando si distribuisce inizialmente il servizio Directories Management, il connettore è il primo provider di identità iniziale per il servizio. L'infrastruttura Active Directory esistente viene utilizzata per l'autenticazione e la gestione degli utenti.

Sono supportati i metodi di autenticazione descritti di seguito. È possibile configurare questi metodi di autenticazione dalla console di amministrazione.

Tabella 2-8. Tipi di autenticazione utente supportati da Gestione directory

Tipi di autenticazione	Descrizione
Password (distribuzione in loco)	Senza alcuna configurazione supplementare dopo la configurazione di Active Directory, Directories Management supporta l'autenticazione tramite password di Active Directory. Questo metodo autentica gli utenti direttamente con Active Directory.
Kerberos per desktop	L'autenticazione Kerberos offre agli utenti di dominio accesso Single Sign-On ai propri portali di applicazioni. Gli utenti non devono più eseguire l'accesso ogni volta che accedono alla rete.

Tabella 2-8. Tipi di autenticazione utente supportati da Gestione directory (continua)

Tipi di autenticazione	Descrizione
Certificato (distribuzione in loco)	<p>È possibile configurare l'autenticazione basata su certificato per consentire ai client di autenticarsi con i certificati sul desktop e sui dispositivi mobili o di utilizzare una scheda smart card per l'autenticazione.</p> <p>L'autenticazione basata su certificato si basa sui dati a disposizione dell'utente e sulle sue conoscenze. Un certificato X.509 utilizza lo standard PKI (Public Key Infrastructure) per verificare che una chiave pubblica contenuta nel certificato appartenga all'utente.</p>
RSA SecurID (distribuzione in loco)	<p>Quando si configura l'autenticazione RSA SecurID, Directories Management viene configurato come agente di autenticazione nel server RSA SecurID.</p> <p>L'autenticazione RSA SecurID richiede che gli utenti utilizzino un sistema di autenticazione basato su token. RSA SecurID è un metodo di autenticazione per gli utenti che accedono a Directories Management dall'esterno della rete aziendale.</p>
RADIUS (distribuzione in loco)	<p>L'autenticazione RADIUS offre opzioni di autenticazione a due fattori. Richiede la configurazione del server RADIUS che è accessibile per il servizio Directories Management. Quando gli utenti eseguono l'accesso con il proprio nome utente e il proprio passcode, al server RADIUS viene inviata una richiesta di accesso per l'autenticazione.</p>
Autenticazione adattiva RSA (distribuzione in loco)	<p>L'autenticazione RSA offre un'autenticazione a più fattori di livello superiore rispetto all'autenticazione basata solo sul nome utente e sulla password di Active Directory. Quando l'autenticazione adattiva RSA è abilitata, gli indicatori di rischio specificati nel criterio di rischio vengono impostati nell'applicazione RSA Policy Management. La configurazione dell'autenticazione adattiva del servizio Directories Management viene utilizzata per determinare le richieste di autenticazione necessarie.</p>
Mobile SSO (per iOS)	<p>Mobile SSO per l'autenticazione di iOS viene utilizzato per l'autenticazione Single Sign-On dei dispositivi iOS gestiti da AirWatch. L'autenticazione Mobile SSO (per iOS) utilizza un Key Distribution Center (KDC) che fa parte del servizio Directories Management. Prima di abilitare questo metodo di autenticazione, è necessario avviare il servizio KDC nel servizio VMware Identity Manager.</p>
Mobile SSO (per Android)	<p>Mobile SSO per l'autenticazione di Android viene utilizzato per l'autenticazione Single Sign-On dei dispositivi Android gestiti da AirWatch. Un servizio proxy è impostato tra il servizio Directories Management ed AirWatch per recuperare il certificato da AirWatch per l'autenticazione.</p>
Password (AirWatch Connector)	<p>AirWatch Cloud Connector può essere integrato con il servizio Directories Management per l'autenticazione della password degli utenti. Si configura il servizio Directories Management per sincronizzare gli utenti dalla directory di AirWatch.</p>

Gli utenti vengono autenticati in base a metodi di autenticazione, regole dei criteri di accesso predefiniti, intervalli di rete e istanza del provider di identità configurato. Dopo aver configurato i metodi di autenticazione, è necessario creare le regole dei criteri di accesso che specificano i metodi di autenticazione da utilizzare in base al tipo di dispositivo.

- **Configurazione di SecurID per Directories Management**

Quando si configura il server di RSA SecurID, è necessario aggiungere le informazioni sul servizio Directories Management come agente di autenticazione sul server di RSA SecurID e configurare le informazioni del server di RSA SecurID sul servizio Directories Management.

- **Configurazione di RADIUS per Directories Management**

È possibile configurare Directories Management in modo da richiedere agli utenti l'utilizzo dell'autenticazione RADIUS (Remote Authentication Dial-In User Service). Le informazioni sul server RADIUS vengono configurate nel servizio Directories Management.

- **Configurazione di un certificato o di un adattatore per smart card per l'uso con Gestione directory**

È possibile configurare l'autenticazione del certificato x509 per consentire ai client di autenticarsi con i certificati sul proprio desktop e sui dispositivi mobili oppure di utilizzare una scheda smart card per l'autenticazione. L'autenticazione basata sul certificato cambia a seconda che l'utente disponga di una chiave privata o di una smart card e a seconda che conosca la password per la chiave privata o il PIN della smart card. Un certificato X.509 utilizza lo standard PKI (Public Key Infrastructure) per verificare che una chiave pubblica contenuta nel certificato appartenga all'utente. Con l'autenticazione della smart card, gli utenti si connettono alla smart card tramite il computer e immettono un PIN.

- **Configurazione di un'istanza del provider di identità di terze parti per l'autenticazione degli utenti**

È possibile configurare un provider di identità di terze parti da utilizzare per autenticare gli utenti nel servizio Directories Management.

- **Gestione dei metodi di autenticazione da applicare agli utenti**

Il servizio Directories Management tenta di autenticare gli utenti in base a metodi di autenticazione, criterio di accesso predefinito, intervalli di rete e istanze di provider di identità configurati.

- **Configurazione di Kerberos per Directories Management**

Grazie all'autenticazione Kerberos, gli utenti che accedono al dominio Active Directory possono accedere al proprio portale di app senza dover immettere altre credenziali. È necessario abilitare l'autenticazione Windows per consentire al protocollo Kerberos di proteggere le interazioni tra i browser degli utenti e il servizio Directories Management. Non occorre configurare direttamente Active Directory per rendere operativo Kerberos nella propria distribuzione.

Configurazione di SecurID per Directories Management

Quando si configura il server di RSA SecurID, è necessario aggiungere le informazioni sul servizio Directories Management come agente di autenticazione sul server di RSA SecurID e configurare le informazioni del server di RSA SecurID sul servizio Directories Management.

Quando si configura SecurID per offrire sicurezza aggiuntiva, è necessario accertarsi che la rete sia correttamente configurata per la propria distribuzione di Directories Management. In modo specifico per SecurID, è necessario che sia aperta la porta giusta affinché SecurID possa autenticare gli utenti all'esterno della rete.

Dopo aver eseguito la configurazione guidata di Directories Management e configurato la connessione di Active Directory, tutte le informazioni necessarie per preparare il server di RSA SecurID sono disponibili. Dopo aver preparato il server di RSA SecurID per Directories Management, è possibile abilitare SecurID nella console di amministrazione.

■ Preparazione del server RSA SecurID

Il server RSA SecurID deve essere configurato con informazioni sull'appliance di Directories Management come agente di autenticazione. Le informazioni richieste sono il nome host e gli indirizzi IP delle interfacce di rete.

■ Configurazione dell'autenticazione RSA SecurID

Dopo aver configurato Gestione directory come agente di autenticazione sul server RSA SecurID, è necessario aggiungere le informazioni sulla configurazione RSA SecurID nel connettore.

Preparazione del server RSA SecurID

Il server RSA SecurID deve essere configurato con informazioni sull'appliance di Directories Management come agente di autenticazione. Le informazioni richieste sono il nome host e gli indirizzi IP delle interfacce di rete.

Prerequisiti

- Verificare che una delle versioni di RSA Authentication Manager seguenti sia installata e funzionante nella rete aziendale: RSA AM 6.1.2, 7.1 SP2 o versioni successive e 8.0 o versioni successive. Il server Directories Management utilizza AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), che supporta solo le versioni precedenti di RSA Authentication Manager (il server RSA SecurID). Per informazioni sull'installazione e la configurazione di RSA Authentication Manager (server RSA SecurID), vedere la documentazione relativa a RSA.

Procedura

- 1 In una versione supportata del server RSA SecurID, aggiungere Directories Management Connector come agente di autenticazione. Immettere le informazioni seguenti.

Opzione	Descrizione
Nome host	Il nome host di Directories Management.
Indirizzo IP	L'indirizzo IP di Directories Management.
Indirizzo IP alternativo	Se il traffico proveniente dal connettore passa attraverso un dispositivo NAT (Network Address Translation) per raggiungere il server RSA SecurID, immettere l'indirizzo IP privato dell'appliance.

- 2 Scaricare il file di configurazione compresso ed estrarre il file `sdconf.rec`.

Prepararsi a caricare questo file successivamente quando si configura RSA SecurID in Directories Management.

Operazioni successive

Passare alla console di amministrazione e nella pagina Configurazione della scheda Gestione identità e accessi selezionare il connettore, quindi configurare SecurID nella pagina AuthAdapters.

Configurazione dell'autenticazione RSA SecurID

Dopo aver configurato Gestione directory come agente di autenticazione sul server RSA SecurID, è necessario aggiungere le informazioni sulla configurazione RSA SecurID nel connettore.

Prerequisiti

- Verificare che RSA Authentication Manager (il server RSA SecurID) sia installato e configurato correttamente.
- Scaricare il file compresso dal server RSA SecurID ed estrarre il file di configurazione del server.

Procedura

- 1 In qualità di amministratore del tenant, passare ad **Amministrazione > Gestione directory > Connettori**.
- 2 Nella pagina Connettori selezionare il collegamento Worker del connettore che si sta configurando con RSA SecurID.
- 3 Fare clic su **Schede di autenticazione** e quindi su **SecurIDIdpAdapter**.
Si verrà reindirizzati alla pagina di accesso di Identity Manager.
- 4 Nella riga SecurIDIdpAdapter della pagina Schede di autenticazione fare clic su **Modifica**.
- 5 Configurare la pagina Scheda di autenticazione SecurID.

A tale scopo, è necessario specificare le informazioni utilizzate e i file generati sul server RSA SecurID.

Opzione	Azione
Nome	L'immissione del nome è obbligatoria. Il nome predefinito è SecurIDdpAdapter, ma è possibile modificarlo.
Abilita SecurID	Selezionare questa casella per abilitare l'autenticazione SecurID.
Numero di tentativi di autenticazione consentiti	Immettere il numero massimo di tentativi di accesso non riusciti consentiti quando si utilizza il token RSA SecurID. Il valore predefinito è cinque tentativi.
Indirizzo connettore	Immettere l'indirizzo IP dell'istanza del connettore. Il valore immesso deve corrispondere al valore utilizzato quando è stata aggiunta l'appliance del connettore come agente di autenticazione al server RSA SecurID. Se al prompt dell'indirizzo IP alternativo del server RSA SecurID è stato assegnato un valore, immettere tale valore come indirizzo IP del connettore. Se non è stato assegnato alcun indirizzo IP alternativo, immettere il valore assegnato al prompt dell'indirizzo IP.
Indirizzo IP agente	Immettere il valore assegnato al prompt dell' indirizzo IP nel server RSA SecurID.
Configurazione server	Caricare il file di configurazione del server RSA SecurID. Scaricare innanzitutto il file compresso dal server RSA SecurID ed estrarre il file di configurazione del server, che per impostazione predefinita è denominato <code>sdconf.rec</code> .
Segreto nodo	Se si lascia vuoto il campo del segreto del nodo si consente la generazione automatica del segreto del nodo. È consigliabile cancellare il file del segreto del nodo sul server RSA SecurID e non caricarlo intenzionalmente. Verificare che il file del segreto del nodo sul server RSA SecurID e sull'istanza del connettore server corrispondano sempre. Se si modifica il segreto del nodo in una posizione, modificarlo anche nell'altra posizione.

6 Fare clic su **Salva**.

Operazioni successive

Aggiungere il metodo di autenticazione al criterio di accesso predefinito. Passare ad **Amministrazione > Gestione directory > Criteri** e fare clic su **Modifica criterio predefinito** per modificare le regole del criterio predefinito e aggiungere il metodo di autenticazione SecurID alla regola nell'ordine di autenticazione corretto.

Configurazione di RADIUS per Directories Management

È possibile configurare Directories Management in modo da richiedere agli utenti l'utilizzo dell'autenticazione RADIUS (Remote Authentication Dial-In User Service). Le informazioni sul server RADIUS vengono configurate nel servizio Directories Management.

Il supporto RADIUS offre un'ampia gamma di opzioni alternative di autenticazione a due fattori basate su token. Poiché le soluzioni di autenticazione a due fattori, come RADIUS, interagiscono con i manager di autenticazione installati su server separati, è necessario che il server RADIUS sia configurato e accessibile per il servizio Identity Manager.

Quando gli utenti accedono al proprio portale My Apps e l'autenticazione RADIUS è abilitata, nel browser viene visualizzata una finestra di dialogo di accesso speciale. Gli utenti immettono il nome utente e il passcode di autenticazione RADIUS nella finestra di dialogo di accesso. Se il server RADIUS genera una verifica dell'accesso, il servizio Identity Manager visualizza una finestra di dialogo in cui viene richiesto un secondo passcode. Attualmente il supporto per le verifiche RADIUS si limita alla richiesta dell'input di testo.

Dopo che un utente ha immesso le credenziali nella finestra di dialogo, il server RADIUS può inviare al telefono cellulare dell'utente un SMS, un'email o un testo basato su un altro meccanismo fuori banda, insieme a un codice. L'utente può immettere questo testo e il codice nella finestra di dialogo di accesso per completare l'autenticazione.

Se il server RADIUS consente di importare gli utenti da Active Directory, agli utenti finali potrebbe essere innanzitutto richiesto di fornire le credenziali di Active Directory prima del nome utente e del passcode di autenticazione di RADIUS.

Preparazione del server RADIUS

Impostare il server RADIUS e quindi configurarlo per accettare richieste RADIUS provenienti dal servizio Directories Management.

Consultare la guida alla configurazione del vendor del server RADIUS utilizzato per informazioni sulla sua impostazione. Annotare le informazioni di configurazione RADIUS poiché dovranno essere utilizzate nella configurazione di RADIUS nel servizio. Per conoscere il tipo di informazioni RADIUS richieste per configurare Directories Management, vedere [Configurazione dell'autenticazione RADIUS in Gestione directory](#).

È possibile impostare un server di autenticazione Radius secondario da utilizzare per garantire l'alta disponibilità. Se il server RADIUS primario non risponde entro un tempo di server timeout configurato per l'autenticazione RADIUS, la richiesta viene reindirizzata al server secondario. Se il server primario non risponde, il server secondario riceverà tutte le richieste di autenticazione future.

Configurazione dell'autenticazione RADIUS in Gestione directory

L'abilitazione del software RADIUS viene eseguita in un server di gestione delle autenticazioni. Per l'autenticazione RADIUS, seguire la documentazione di configurazione del fornitore.

Prerequisiti

Installare e configurare il software RADIUS in un server di gestione dell'autenticazione. Per l'autenticazione RADIUS, seguire la documentazione di configurazione del fornitore.

Per configurare RADIUS nel servizio, è necessario conoscere le seguenti informazioni sul server RADIUS.

- Indirizzo IP o nome DNS del server RADIUS.
- Numeri della porta di autenticazione. La porta di autenticazione è in genere la 1812.
- Tipo di autenticazione. I tipi di autenticazione includono PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, versioni 1 e 2).

- Segreto condiviso RADIUS utilizzato per la crittografia e la decrittografia nei messaggi del protocollo RADIUS.
- Timeout e valori retry specifici necessari per l'autenticazione RADIUS.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Connettori**.
- 2 Nella pagina Connettori selezionare il collegamento Worker del connettore che si sta configurando per l'autenticazione RADIUS.
- 3 Fare clic su **Schede di autenticazione** e quindi su **RadiusAuthAdapter**.
Si verrà reindirizzati alla pagina di accesso di Identity Manager.
- 4 Fare clic su **Modifica** per configurare questi campi nella pagina Scheda di autenticazione.

Opzione	Azione
Nome	L'immissione del nome è obbligatoria. Il nome predefinito è RadiusAuthAdapter, ma è possibile modificarlo.
Abilita scheda Radius	Selezionare questa casella per abilitare l'autenticazione RADIUS.
Numero di tentativi di autenticazione consentiti	Immettere il numero massimo di tentativi di accesso non riusciti consentiti quando si utilizza RADIUS per accedere. Il valore predefinito è cinque tentativi.
Numero di tentativi di accesso al server Radius	Specificare il numero totale di tentativi. Se il server primario non risponde, il servizio attende il tempo configurato prima di riprovare.
Nome host/indirizzo server Radius	Immettere il nome host o l'indirizzo IP del server RADIUS.
Porta di autenticazione	Immettere il numero della porta di autenticazione Radius. In genere si tratta della porta 1812.
Porta di accounting	Immettere 0 come numero di porta. La porta di accounting non viene utilizzata in questa fase.
Tipo di autenticazione	Immettere il protocollo di autenticazione supportato dal server RADIUS, scegliendo tra PAP, CHAP, MSCHAP1 o MSCHAP2.
Segreto condiviso	Immettere il segreto condiviso utilizzato tra il server RADIUS e il servizio VMware Identity Manager.

Opzione	Azione
Timeout server in secondi	Immettere il timeout del server RADIUS in secondi, al termine del quale viene eseguito un nuovo tentativo se il server RADIUS non risponde.
Prefisso area di autenticazione	(Facoltativo) La posizione dell'account utente è chiamata area di autenticazione. Se si specifica una stringa per il prefisso dell'area di autenticazione, tale stringa viene posizionata all'inizio del nome utente quando il nome viene inviato al server RADIUS. Se, ad esempio, si immette jdoe come nome utente e si specifica il prefisso dell'area di autenticazione DOMAIN-A\, al server RADIUS viene inviato il nome utente DOMAIN-A\jdoe. Se non si configurano questi campi, viene inviato solo il nome utente immesso.
Suffisso area di autenticazione	(Facoltativo) Se si specifica un suffisso dell'area di autenticazione, la stringa viene posizionata alla fine del nome utente. Se, ad esempio, il suffisso è @myco.com, al server RADIUS viene inviato il nome utente jdoe@myco.com.
Suggerimento o passphrase pagina di accesso	Immettere la stringa di testo da visualizzare nel messaggio della pagina di accesso dell'utente per indicare agli utenti di immettere il passcode Radius corretto. Se, ad esempio, questo campo è configurato con Prima password AD, poi passcode SMS , il messaggio della pagina di accesso indica Immetti prima password AD, poi passcode SMS . La stringa di testo predefinita è Passcode RADIUS .

5 È possibile abilitare un server RADIUS secondario per la disponibilità elevata.

Configurare il server secondario come descritto nel passaggio 4.

6 Fare clic su **Salva**.

Operazioni successive

Aggiungere il metodo di autenticazione RADIUS al criterio di accesso predefinito. Selezionare **Amministrazione > Gestione directory > Criteri** e fare clic su **Modifica criterio predefinito** per modificare le regole del criterio predefinito e aggiungere il metodo di autenticazione RADIUS alla regola nell'ordine di autenticazione corretto.

Configurazione di un certificato o di un adattatore per smart card per l'uso con Gestione directory

È possibile configurare l'autenticazione del certificato x509 per consentire ai client di autenticarsi con i certificati sul proprio desktop e sui dispositivi mobili oppure di utilizzare una scheda smart card per l'autenticazione. L'autenticazione basata sul certificato cambia a seconda che l'utente disponga di una chiave privata o di una smart card e a seconda che conosca la password per la chiave privata o il PIN della smart card. Un certificato X.509 utilizza lo standard PKI (Public Key Infrastructure) per verificare che una chiave pubblica contenuta nel certificato appartenga all'utente. Con l'autenticazione della smart card, gli utenti si connettono alla smart card tramite il computer e immettono un PIN.

I certificati smart card vengono copiati nell'archivio dei certificati locale sul computer dell'utente. I certificati nell'archivio certificati locale sono disponibili per tutti i browser in esecuzione sul computer di questo utente, con alcune eccezioni.

Nota Quando l'autenticazione del certificato è configurata e l'appliance del servizio è impostata dietro un bilanciamento del carico, assicurarsi che il connettore sia configurato non per terminare SSL, ma per effettuare un pass-through SSL a livello del bilanciamento del carico. Questa configurazione assicura che l'handshake SSL venga eseguito tra il connettore e il client per passare il certificato al connettore. È possibile configurare connettori aggiuntivi dietro un altro bilanciamento del carico configurato con pass-through SSL e abilitare e configurare l'autenticazione basata su certificati su questi connettori.

Utilizzo del nome dell'entità utente per l'autenticazione con certificato

È possibile utilizzare la mappatura del certificato in Active Directory. Gli accessi tramite certificato e smart card utilizzano il nome dell'entità utente (UPN) di Active Directory per convalidare gli account utente. Gli account Active Directory degli utenti che tentano di eseguire l'autenticazione nel servizio Directories Management devono disporre di un nome UPN valido corrispondente al nome UPN presente nel certificato.

È possibile configurare Directories Management per l'uso di un indirizzo email con cui convalidare l'account utente se l'UPN non esiste nel certificato.

È anche possibile abilitare l'uso di un tipo di UPN alternativo.

Autorità di certificazione richiesta per l'autenticazione

Per abilitare l'accesso utilizzando l'autenticazione con certificato, i certificati radice e i certificati intermedi devono essere caricati nel di Directories Management.

I certificati vengono copiati nell'archivio certificati locale sul computer dell'utente. I certificati nell'archivio certificati locale sono disponibili a tutti i browser eseguiti sul computer dell'utente, con alcune eccezioni, e pertanto sono disponibili a un'istanza di Directories Management nel browser.

Per l'autenticazione con smart card, quando un utente avvia una connessione a un'istanza di Directories Management, il servizio Directories Management invia un elenco di autorità di certificazione (CA) attendibili al browser. Il browser analizza l'elenco di autorità di certificazione attendibili e lo confronta con i certificati utente disponibili, seleziona un certificato adatto e richiede all'utente di inserire il PIN della smart card. Se sono disponibili più certificati utente validi, il browser richiede all'utente di selezionarne uno.

Se un utente non può autenticarsi, è possibile che l'autorità di certificazione radice e l'autorità di certificazione intermedia non siano impostate correttamente, o che il servizio non sia stato riavviato dopo che le autorità di certificazione radice e intermedia sono state caricate sul server. In questi casi, il browser non può mostrare i certificati installati, l'utente non può selezionare il certificato corretto e l'autenticazione con certificato ha esito negativo.

Utilizzo del controllo della revoca del certificato

È possibile configurare il controllo della revoca del certificato per impedire l'autenticazione degli utenti il cui certificato è stato revocato. Spesso i certificati vengono revocati quando un utente abbandona un'organizzazione, perde una smart card o passa da un reparto all'altro.

Sono supportati due tipi di controllo della revoca del certificato, ovvero tramite gli elenchi di revoche di certificati (CRL) e tramite il Protocollo di stato del certificato online (OCSP). Un CRL è un elenco di certificati revocati pubblicato dall'autorità di certificazione che ha emesso i certificati. OCSP è un protocollo di convalida del certificato utilizzato per ottenere lo stato di revoca di un certificato.

È possibile configurare il controllo della revoca del certificato nella pagina Connettori > Schede di autenticazione > CertificateAuthAdapter della console di amministrazione durante la configurazione dell'autenticazione del certificato.

È possibile configurare sia l'elenco CRL che il protocollo OCSP nella stessa configurazione della scheda di autenticazione del certificato. Quando si configurano entrambi i tipi di controllo della revoca del certificato e la casella di controllo Usa CRL in caso di errore OCSP è selezionata, viene controllato prima il protocollo OCSP e, in caso di esito negativo, il controllo della revoca esegue il fallback a CRL. In caso di esito negativo di CRL, il controllo della revoca non esegue il fallback a OCSP.

Accesso con il controllo CRL

Quando si abilita la revoca del certificato, il server Directories Management legge un CRL per stabilire lo stato della revoca di un certificato utente.

Se un certificato risulta revocato, l'autenticazione tramite il certificato non riesce.

Accesso con il controllo del certificato OCSP

Quando si configura il controllo della revoca OCSP (Online Certificate Status Protocol), Directories Management invia una richiesta a un risponditore OCSP per stabilire lo stato della revoca di un certificato utente specifico. Il server Directories Management utilizza il certificato della firma OCSP per verificare che le risposte che riceve dal risponditore OCSP siano autentiche.

Se il certificato risulta revocato, l'autenticazione non riesce.

È possibile configurare l'autenticazione in modo che esegua il fallback al controllo CRL se non riceve alcuna risposta dal risponditore OCSP o se la risposta non è valida.

Configurazione dell'autenticazione dei certificati per Gestione directory

È possibile abilitare e configurare l'autenticazione dei certificati tramite la funzionalità Gestione directory della console di amministrazione di vRealize Automation.

Nota Un amministratore di sistema deve configurare un connettore esterno per la distribuzione di vRealize Automation se vengono utilizzati provider di identità terze parti come l'autenticazione della smart card o Keberos.

Prerequisiti

- Ottenere il certificato radice e i certificati intermedi dall'autorità di certificazione che ha firmato i certificati presentati dagli utenti.
- (Facoltativo) Elenco di identificatori di oggetto (OID) di criteri di certificato validi per l'autenticazione del certificato.
- Per il controllo della revoca, la posizione del file del CRL, l'URL del server OCSP.

- (Facoltativo) La posizione del file del certificato Firma risposta OCSP.
- Contenuto del modulo di consenso, se si abilita la visualizzazione di un modulo di consenso prima dell'autenticazione.

Procedura

- 1 In qualità di amministratore del tenant, passare ad **Amministrazione > Gestione directory > Connettori**.
- 2 Nella pagina Connettori, selezionare il collegamento Worker del connettore che si sta configurando.
- 3 Fare clic su **Schede di autenticazione** e quindi su **CertificateAuthAdapter**.
Si verrà reindirizzati alla pagina di accesso di Identity Manager.
- 4 Nella riga CertificateAuthAdapter fare clic su **Modifica**.
- 5 Configurare la pagina Scheda di autenticazione certificato.

Nota Un asterisco indica un campo obbligatorio. Tutti gli altri campi sono facoltativi.

Opzione	Descrizione
*Nome	L'immissione del nome è obbligatoria. Il nome predefinito è CertificateAuthAdapter, ma è possibile modificarlo.
Abilita adattatore certificato	Selezionare la casella di controllo per abilitare l'autenticazione del certificato.
*Certificati radice e intermedi dell'autorità di certificazione	Selezionare i file di certificato da caricare. È possibile selezionare più certificati radice e intermedi dell'autorità di certificazione, codificati come DER o PEM.
Certificati autorità di certificazione caricati	<p>I file di certificato caricati sono elencati nella sezione Certificati autorità di certificazione caricati del modulo.</p> <p>Per rendere disponibili i nuovi certificati, è necessario riavviare il servizio.</p> <p>Fare clic su Riavvia servizio Web per riavviare il servizio e aggiungere i certificati al servizio attendibile.</p> <p>Nota Il riavvio del servizio non comporta l'abilitazione dell'autenticazione dei certificati. Dopo aver riavviato il servizio, continuare a configurare questa pagina. Facendo clic su Salva in fondo alla pagina si abilita l'autenticazione dei certificati nel servizio.</p>
Usa email se nel certificato non esiste un UPN	Se il nome dell'entità utente (UPN) non esiste nel certificato, selezionare questa casella di controllo per utilizzare l'attributo emailAddress come estensione SAN (Subject Alternative Name, nome alternativo del soggetto) per convalidare gli account utente.
Criteri di certificato accettati	<p>Creare un elenco di identificatori di oggetto accettati nelle estensioni dei criteri di certificato.</p> <p>Immettere i numeri OID (Object ID Number) per il criterio di emissione dei certificati. Fare clic su Aggiungi un altro valore per aggiungere altri OID.</p>
Abilita revoca certificato	Selezionare la casella di controllo per abilitare il controllo della revoca del certificato. In questo modo si impedirà l'autenticazione degli utenti che hanno certificati revocati.

Opzione	Descrizione
Usa CRL dei certificati	Selezionare la casella di controllo per utilizzare l'elenco di revoche di certificati (CRL) pubblicato dall'autorità di certificazione che ha emesso i certificati per convalidare lo stato, revocato o non revocato, di un certificato.
Posizione CRL	Immettere il percorso del file server o del file locale dal quale recuperare l'elenco di revoche di certificati.
Abilita revoca OCSP	Selezionare la casella di controllo per utilizzare il protocollo di convalida del certificato OCSP (Online Certificate Status Protocol) per ottenere lo stato della revoca di un certificato.
Usa CRL in caso di errore OCSP	Se si configurano sia CRL che OCSP, è possibile selezionare questa casella di controllo per eseguire il fallback a CRL se il controllo OCSP non è disponibile.
Invia nonce OCSP	Selezionare questa casella di controllo se si desidera inviare l'identificativo univoco della richiesta OCSP nella risposta.
URL OCSP	Se la revoca OCSP è stata abilitata, immettere l'indirizzo del server OCSP per il controllo della revoca.
Certificato della firma del risponditore OCSP	Immettere il percorso del certificato OCSP del risponditore, <i>/path/to/file.cer</i> .
Abilita modulo consenso prima dell'autenticazione	Selezionare questa casella di controllo per includere una pagina per il modulo di consenso, da visualizzare prima che gli utenti accedano al portale My Apps utilizzando l'autenticazione del certificato.
Contenuto modulo consenso	Digitare in questa casella il testo visualizzato nel modulo di consenso.

6 Fare clic su **Salva**.

Operazioni successive

- Aggiungere il metodo di autenticazione dei certificati al criterio di accesso predefinito. Passare ad **Amministrazione > Gestione directory > Criteri** e fare clic su **Modifica criterio predefinito** per modificare le regole del criterio predefinito, aggiungere Certificato e impostarlo come primo metodo di autenticazione per il criterio predefinito. Certificato deve essere il primo metodo di autenticazione elencato nella regola del criterio. In caso contrario, l'autenticazione del certificato non verrà eseguita correttamente.
- Quando l'autenticazione del certificato è configurata e l'appliance del servizio è impostata dietro un bilanciamento del carico, assicurarsi che il Directories Management connettore sia configurato con un pass-through SSL a livello del bilanciamento del carico e per non terminare SSL a tale livello. Questa configurazione assicura che l'handshake SSL venga eseguito tra il connettore e il client per passare il certificato al connettore.

Configurazione di un'istanza del provider di identità di terze parti per l'autenticazione degli utenti

È possibile configurare un provider di identità di terze parti da utilizzare per autenticare gli utenti nel servizio Directories Management.

Prima di utilizzare la console di amministrazione per aggiungere l'istanza del provider di identità di terze parti, completare le attività seguenti.

- Verificare che le istanze di terze parti siano conformi con SAML 2.0 e che il servizio possa raggiungere l'istanza di terze parti.
- Ottenere le informazioni sui metadati di terze parti appropriate da aggiungere durante la configurazione del provider di identità nella console di amministrazione. Le informazioni sui metadati ottenute dall'istanza di terze parti corrispondono all'URL dei metadati o ai metadati effettivi.

Configurazione di una connessione a un provider di identità di terze parti

vRealize Automation viene fornito con un'istanza di connessione al provider di identità predefinita. Gli utenti possono creare ulteriori connessioni a provider di identità per supportare il provisioning utente just-in-time o altre configurazioni personalizzate.

vRealize Automation viene fornito con un provider di identità predefinito. Nella maggior parte dei casi, il provider predefinito è sufficiente per soddisfare le esigenze dei clienti. Se si utilizza una soluzione di gestione delle identità di livello enterprise, è possibile configurare un provider di identità personalizzato per reindirizzare gli utenti alla propria soluzione esistente.

Quando si utilizza un provider delle identità personalizzato, Gestione directory utilizza i metadati SAML del provider per stabilire con il provider una relazione basata sulla fiducia. Una volta stabilita questa relazione, Gestione directory mappa gli utenti dall'asserzione SAML all'elenco di utenti vRealize Automation interni basato sull'ID del nome del soggetto.

Prerequisiti

- Configurare gli intervalli di rete che si desidera indirizzare a questa istanza di provider di identità per l'autenticazione. Vedere [Aggiunta o modifica di un intervallo di rete](#).
- Accedere al documento dei metadati di terze parti, che può corrispondere all'URL dei metadati o ai metadati effettivi.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Provider di identità**.

In questa pagina vengono visualizzati tutti i provider di identità configurati.

- 2 Fare clic su **Aggiungi provider di identità**.

Viene visualizzato un menu con le opzioni relative al provider di identità.

- 3 Selezionare **Crea IDP di terze parti**.

4 Immettere le informazioni appropriate per configurare il provider di identità.

Opzione	Descrizione
Nome del provider di identità	Immettere un nome per l'istanza del provider di identità.
Metadati SAML	<p>Aggiungere il documento dei metadati basati su XML IdP di terze parti per stabilire una relazione di fiducia con il provider di identità.</p> <ol style="list-style-type: none"> 1 Immettere l'URL dei metadati SAML o il contenuto XML nella casella di testo. 2 Fare clic su Elabora metadati IdP. I formati NameID supportati da IdP vengono estratti dai metadati e aggiunti alla tabella Formato ID nome. 3 Nella colonna del valore ID del nome selezionare l'attributo utente del servizio da mappare ai formati degli ID visualizzati. È possibile aggiungere formati di ID di nome di terze parti personalizzati e mapparli ai valori degli attributi utente nel servizio. 4 (Facoltativo) Selezionare il formato della stringa dell'identificatore di risposta NameIDPolicy.
Utenti	Selezionare le directory Directories Management degli utenti che possono autenticarsi utilizzando questo provider di identità.
Provisioning utente Just-in-Time	<p>Selezionare le opzioni appropriate per supportare il provisioning just-in-time utilizzando un provider di identità di terze parti idoneo.</p> <p>In Nome directory immettere il nome della directory da utilizzare per il provisioning just-in-time.</p> <p>Immettere uno o più Domini esistenti nel provider di identità esterno che verrà utilizzato per il provisioning just-in-time.</p>
Rete	<p>Sono elencati gli intervalli di rete esistenti configurati nel servizio.</p> <p>Selezionare, in base ai rispettivi indirizzi IP, gli intervalli di rete degli utenti che si desidera indirizzare a questa istanza di provider di identità per l'autenticazione.</p>
Metodi di autenticazione	<p>Aggiungere i metodi di autenticazione supportati dal provider di identità di terze parti.</p> <p>Selezionare la classe del contesto di autenticazione SAML che supporta il metodo di autenticazione.</p>
Certificato della firma SAML	Fare clic su Metadati del provider di servizi (SP) per visualizzare l'URL dei metadati del provider di servizi SAML Directories Management. Copiare e salvare l'URL. Questo URL viene configurato quando si modifica l'asserzione SAML nel provider di identità di terze parti per mappare gli utenti di Directories Management.
Nome host	Se viene visualizzato il campo Nome host , immettere il nome host al quale il provider di identità viene reindirizzato per l'autenticazione. Se si utilizza una porta non standard diversa dalla porta 443, è possibile impostare questo valore nel formato Nome host:Porta. Ad esempio, myco.example.com:8443.

5 Fare clic su **Aggiungi**.

Operazioni successive

- Copiare e salvare i metadati del provider di servizi Directories Management necessario per configurare l'istanza del provider di identità di terze parti. Questi metadati sono disponibili nella sezione Certificato di firma SAML della pagina Provider di identità.
- Aggiungere il metodo di autenticazione del provider di identità al criterio predefinito dei servizi.

Per informazioni sull'aggiunta e la personalizzazione delle risorse aggiunte al catalogo, vedere la guida *Setting Up Resources in Directories Management*.

Gestione dei metodi di autenticazione da applicare agli utenti

Il servizio Directories Management tenta di autenticare gli utenti in base a metodi di autenticazione, criterio di accesso predefinito, intervalli di rete e istanze di provider di identità configurati.

Quando gli utenti effettuano l'accesso, il servizio valuta le regole del criterio di accesso predefinito per selezionare quale regola del criterio applicare. I metodi di autenticazione vengono applicati nell'ordine in cui sono elencati nella regola. Viene selezionata la prima istanza del provider di identità che soddisfa i requisiti del metodo di autenticazione e dell'intervallo di rete della regola, e la richiesta di autenticazione dell'utente viene inoltrata all'istanza del provider di identità per l'autenticazione. Se l'autenticazione ha esito negativo viene applicato il successivo metodo di autenticazione configurato nella regola.

È possibile aggiungere regole che specifichino i metodi di autenticazione da utilizzare in base al tipo di dispositivo o in base al tipo di dispositivo e a un intervallo di reti specifico. Ad esempio, è possibile configurare una regola in cui si richiede agli utenti che accedono tramite dispositivi iOS da una rete specifica di effettuare l'autenticazione tramite RSA SecurID e un'altra regola in cui si specifica che tutti i tipi di dispositivi che accedono dall'indirizzo IP della rete interna devono utilizzare la password per l'autenticazione.

Aggiunta o modifica di un intervallo di rete

È possibile gestire gli intervalli di rete per definire gli indirizzi IP dai quali gli utenti possono accedere tramite un collegamento di Active Directory. Gli intervalli di rete creati vengono aggiunti a specifiche istanze di provider di identità e regole dei criteri di accesso.

Definire intervalli di rete per la distribuzione di Directories Management in base alla propria topologia di rete.

Come intervallo predefinito viene creato un intervallo di rete, denominato TUTTI GLI INTERVALLI. Tale intervallo di rete include tutti gli indirizzi IP disponibili in Internet, da 0.0.0.0 a 255.255.255.255. Anche se la propria distribuzione presenta una singola istanza di provider di identità, è possibile modificare l'intervallo di indirizzi IP e aggiungere altri intervalli per escludere o includere indirizzi IP specifici all'intervallo di rete predefinito. È possibile creare altri intervalli di rete con indirizzi IP specifici, applicabili per uno scopo specifico.

Nota l'intervallo di rete predefinito, TUTTI GLI INTERVALLI, e la relativa descrizione, "una rete per tutti gli intervalli", sono modificabili. È possibile modificare il nome e la descrizione, nonché impostare una lingua diversa per il testo, facendo clic sul nome dell'intervallo di rete nella pagina Intervalli di rete.

Prerequisiti

- Sono stati configurati i tenant per la distribuzione vRealize Automation e un collegamento ad Active Directory appropriato per supportare l'autenticazione ID utente e password di base di Active Directory.

- Active Directory è installato e configurato per l'uso nella rete esistente.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Intervalli di rete**.
- 2 Modificare un intervallo di rete esistente o aggiungerne uno nuovo.

Opzione	Descrizione
Modifica intervallo esistente	Fare clic sul nome dell'intervallo di rete da modificare.
Aggiungi intervallo	Fare clic su Aggiungi intervallo di rete per aggiungere un nuovo intervallo.

- 3 Completare il modulo.

Elemento del modulo	Descrizione
Nome	Immettere un nome per l'intervallo di rete.
Descrizione	Immettere una descrizione per l'intervallo di rete.
Visualizza pod	L'opzione Visualizza pod viene visualizzata solo quando il modulo Visualizza è abilitato. Host URL accesso client. Immettere l'URL di accesso a Horizon Client corretto per l'intervallo di rete. Porta di accesso client. Immettere il numero della porta di accesso a Horizon Client corretto per l'intervallo di rete.
Intervalli IP	Modificare o aggiungere intervalli IP fino ad includere tutti gli indirizzi IP desiderati, escludendo quelli indesiderati.

Operazioni successive

- Associare ogni intervallo di rete a un'istanza del provider di identità.
- Associare gli intervalli di rete a una regola dei criteri di accesso appropriata. Vedere [Configurazione delle impostazioni dei criteri di accesso](#).

Selezione degli attributi per la sincronizzazione con la directory

Quando si imposta la directory di Directories Management per la sincronizzazione con Active Directory, vengono definiti gli attributi degli utenti sincronizzati con la directory. Prima di impostare la directory, nella pagina Attributi utente è possibile specificare quali attributi predefiniti sono richiesti e, se desiderato, aggiungere attributi aggiuntivi da mettere in corrispondenza con gli attributi di Active Directory.

Quando si configura la pagina Attributi utente prima che venga creata la directory, è possibile modificare gli attributi predefiniti obbligatori rendendoli non obbligatori, contrassegnare gli attributi come obbligatori e aggiungere attributi personalizzati.

Per un elenco degli attributi mappati predefiniti, vedere [Gestione degli attributi utente sincronizzati da Active Directory](#).

Dopo aver creato la directory, è possibile modificare un attributo obbligatorio rendendolo non obbligatorio ed eliminare attributi personalizzati. Non è possibile modificare un attributo per renderlo obbligatorio.

Quando si aggiungono altri attributi per la sincronizzazione con la directory, dopo aver creato la directory, passare alla pagina Attributi mappati della directory per mappare questi attributi agli attributi di Active Directory.

Procedura

- 1 Accedere a vRealize Automation come amministratore di sistema o tenant.
- 2 Fare clic sulla scheda Amministrazione.
- 3 Selezionare **Gestione directory > Attributi utente**.
- 4 Nella sezione Attributi predefiniti esaminare l'elenco di attributi obbligatori e apportare le modifiche appropriate in modo da riflettere gli attributi obbligatori.
- 5 Nella sezione Attributi aggiungere il nome dell'attributo della directory di Directories Management all'elenco.
- 6 Fare clic su **Salva**.

Lo stato dell'attributo predefinito viene aggiornato e gli attributi aggiunti vengono aggiunti nell'elenco Attributi mappati della directory.
- 7 Dopo aver creato la directory, passare alla pagina Archivi identità e selezionare la directory.
- 8 Fare clic su **Impostazioni di sincronizzazione > Attributi mappati**.
- 9 Nel menu a discesa relativo agli attributi aggiunti, selezionare l'attributo di Active Directory con cui mappare.
- 10 Fare clic su **Salva**.

Risultati

La directory viene aggiornata alla successiva sincronizzazione con Active Directory.

Applicazione del criterio di accesso predefinito

Il servizio Directories Management include un criterio di accesso predefinito che controlla l'accesso degli utenti ai loro portali di app. È possibile modificare il criterio per cambiarne le regole secondo necessità.

Quando si attivano metodi di autenticazione diversi dall'autenticazione con password, è necessario modificare il criterio predefinito per aggiungere il metodo di autenticazione attivato nelle regole del criterio.

Per ogni regola del criterio di accesso predefinito è necessario che siano soddisfatti una serie di criteri affinché gli utenti possano accedere al portale delle app. È possibile applicare un intervallo di rete, selezionare quale tipo di utente può accedere al contenuto e selezionare i metodi di autenticazione da utilizzare. Vedere [Gestione dei criteri di accesso](#).

Il numero di tentativi fatti dal servizio per completare l'accesso di un utente con un dato metodo di autenticazione varia. I servizi fanno un unico tentativo nelle autenticazioni con Kerberos o con certificato. Se il tentativo di accesso di un utente non ha esito positivo, viene provato il metodo di autenticazione successivo nella regola. Per impostazione predefinita, il numero massimo di tentativi di accesso non riusciti per l'autenticazione con password di Active Directory e RSA SecurID è impostato su cinque. Quando per un utente ci sono cinque tentativi di accesso non riusciti, il servizio tenta l'accesso dell'utente con il metodo di autenticazione successivo nell'elenco. Quando vengono esauriti tutti i metodi di autenticazione, il servizio genera un messaggio di errore.

Applicazione dei metodi di autenticazione alle regole dei criteri

Nelle regole dei criteri predefinite viene configurato solo il metodo di autenticazione tramite password. Per selezionare gli altri metodi di autenticazione configurati e impostare l'ordine in cui tali metodi vengono utilizzati per l'autenticazione, è necessario modificare le regole dei criteri.

Prerequisiti

Abilitare e configurare i metodi di autenticazione supportati dall'organizzazione. Vedere [Integrazione di prodotti di autenticazione dell'utente alternativi con Gestione directory](#)

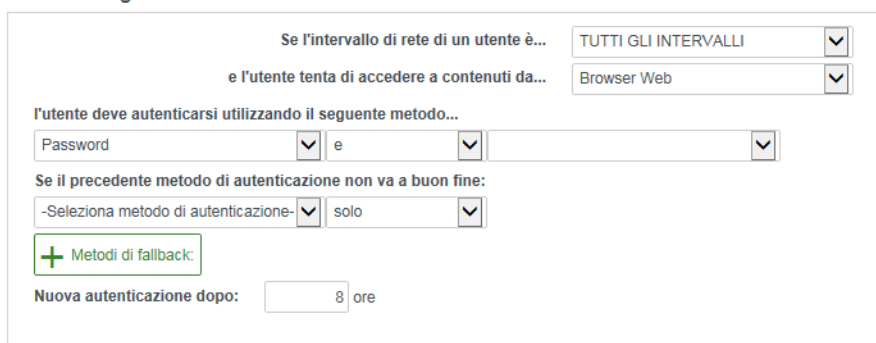
Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Criteri**.
- 2 Fare clic sul criterio di accesso predefinito da modificare.
- 3 Per modificare una regola dei criteri, fare clic sul metodo di autenticazione da modificare nella colonna Metodo di autenticazione di Regole dei criteri.

Per aggiungere una nuova regola dei criteri, fare clic sull'icona **+**.

- 4 Fare clic su **Salva** e quindi di nuovo su **Salva** nella pagina Criterio.

Modifica regola del criterio



- 5 Fare clic su **Salva** e quindi di nuovo su **Salva** nella pagina Criterio.

Configurazione di Kerberos per Directories Management

Grazie all'autenticazione Kerberos, gli utenti che accedono al dominio Active Directory possono accedere al proprio portale di app senza dover immettere altre credenziali. È necessario abilitare l'autenticazione Windows per consentire al protocollo Kerberos di proteggere le interazioni tra i

browser degli utenti e il servizio Directories Management. Non occorre configurare direttamente Active Directory per rendere operativo Kerberos nella propria distribuzione.

Al momento, le interazioni tra il browser di un utente e il servizio sono autenticate da Kerberos solo su sistemi operativi Windows. Accedendo al servizio da altri sistemi operativi si perde il vantaggio dell'autenticazione Kerberos.

■ Configurazione dell'autenticazione Kerberos

Per configurare il servizio Directories Management in modo che fornisca l'autenticazione Kerberos, è necessario accedere al dominio e abilitare tale autenticazione nel connettore Directories Management.

■ Configurazione di Internet Explorer per l'accesso all'interfaccia Web

Se Kerberos è configurato per la distribuzione e si desidera concedere agli utenti l'accesso all'interfaccia Web tramite il browser Internet Explorer, è necessario configurare tale browser.

■ Configurazione di Firefox per l'accesso all'interfaccia Web

Se Kerberos è configurato per la distribuzione e si desidera concedere agli utenti l'accesso all'interfaccia Web tramite il browser Firefox, è necessario configurare tale browser.

■ Configurazione del browser Chrome per l'accesso all'interfaccia Web

Se Kerberos è configurato per la distribuzione e si desidera concedere agli utenti l'accesso all'interfaccia Web tramite il browser Chrome, è necessario configurare tale browser.

Configurazione dell'autenticazione Kerberos

Per configurare il servizio Directories Management in modo che fornisca l'autenticazione Kerberos, è necessario accedere al dominio e abilitare tale autenticazione nel connettore Directories Management.

Prerequisiti

- Distribuire NSX Edge in vCenter e configurare un bilanciamento del carico NSX. Per informazioni sulla configurazione di un bilanciamento del carico, vedere *vRealize Automation Load Balancing*.
- Unire il proprio dominio al tenant master. È necessario eseguire questa operazione prima di creare connessioni alla directory in tenant separati.
 - a Accedere al tenant predefinito come administrator@vsphere.local.
 - b Creare un utente locale TestUser e immettere TestUser come amministratore tenant.
 - c Selezionare **Amministrazione > Gestione directory > Connettori**.
 - d Selezionare Aggiunta a un dominio in ciascun connettore dell'appliance.
 - e In Aggiunta a un dominio selezionare Dominio personalizzato e immettere il dominio a cui si desidera connettere il tenant insieme alle credenziali e all'unità organizzativa a cui connettersi.

- Configurare le connessioni alla directory per i tenant predefiniti e per i tenant non predefiniti. L'autenticazione Kerberos funziona sia con l'autenticazione integrata di Windows sia con Active Directory su LDAP. Vedere [Configurazione di un collegamento Active Directory su LDAP/IWA](#) e [Configurazione di una connessione alla directory OpenLDAP](#).
- Assicurarsi che il nome host del nodo di vRealize Automation corrisponda al dominio di Active Directory a cui si sta unendo. Ad esempio, se vRealize Automation si sta unendo a un'area di autenticazione di Active Directory denominata COMPANY.COM, il nome host deve essere node.company.com.
- Configurare un provider di identità dell'area di lavoro. Assicurarsi che tutti i nodi della distribuzione siano registrati nel provider di identità dell'area di lavoro e che il nome del bilanciamento del carico sia definito.
 - a Selezionare **Amministrazione > Gestione directory > Provider di identità**.
 - b Selezionare il collegamento del provider di identità appropriato.
Ad esempio, WorkspaceIDP_1.
 - c Fare clic sul collegamento del provider di identità e trovare il nome host del provider di identità configurato. Tenere traccia del nome perché sarà necessario quando si configurano i browser Web.
 - d Registrare tutti i nodi applicabili nel provider di identità dell'area di lavoro e immettere il nome di dominio completo del bilanciamento del carico per il nome host.
 - e Fare clic su **Salva**.
- Configurare la directory del tenant per il tenant predefinito. Vedere l'argomento relativo alla configurazione dell'accesso al tenant predefinito in *Installazione di vRealize Automation*

Procedura

- 1 In qualità di amministratore tenant, passare a **Amministrazione > Gestione directory > Connettori**.
- 2 Nella pagina Connettori, per il connettore che si sta configurando per l'autenticazione Kerberos, fare clic su **Aggiungi a dominio**.
- 3 Nella pagina Aggiungi a dominio immettere le informazioni del dominio Active Directory.

Opzione	Descrizione
Dominio	Specificare il nome di dominio completo di Active Directory. Il nome di dominio immesso deve essere lo stesso nome di dominio Windows del server del connettore.
Utente di dominio	Immettere il nome utente di un account dell'istanza di Active Directory che dispone delle autorizzazioni necessarie per aggiungere sistemi a tale dominio Active Directory.
Password di dominio	Immettere la password associata al nome utente AD. Tale password non viene archiviata in Directories Management.

Fare clic su **Salva**.

La pagina Aggiungi a dominio viene aggiornata e visualizza un messaggio per comunicare l'aggiunta dell'utente al dominio.

- 4 Nella colonna Worker del connettore fare clic su **Schede di autenticazione**.

- 5 Fare clic su **KerberosIdpAdapter**.

Si verrà reindirizzati alla pagina di accesso di Identity Manager.

- 6 Fare clic su **Modifica** nella riga KerberosIdpAdapter e configurare la pagina di autenticazione di Kerberos.

Opzione	Descrizione
Nome	L'immissione del nome è obbligatoria. Il nome predefinito è KerberosIdpAdapter, ma è possibile modificarlo.
Attributo UID di directory	Immettere l'attributo dell'account contenente il nome utente.
Abilita autenticazione di Windows	Selezionare questa opzione per estendere le interazioni di autenticazione tra i browser degli utenti e Directories Management.
Abilita NTLM	Selezionare questa opzione per abilitare l'autenticazione basata sul protocollo NTLM (NT LAN Manager) solo se l'infrastruttura di Active Directory utilizza l'autenticazione NTLM.
Abilita reindirizzamento	Selezionare questa opzione se DNS round robin e i bilanciamenti del carico non dispongono del supporto Kerberos. Le richieste di autenticazione vengono reindirizzate a Reindirizza nome host. Se questa opzione è selezionata, immettere il nome host di reindirizzamento nella casella di testo Reindirizza nome host . Generalmente si tratta del nome host del servizio.

- 7 Fare clic su **Salva**.

- 8 Configurare l'autenticazione Kerberos in tutti i nodi applicabili.

- a Selezionare **Amministrazione > Gestione directory > Connettori**.

Questa pagina mostra i connettori attualmente configurati. Per impostazione predefinita, viene configurata solo l'autenticazione con password.

- b Fare clic sul collegamento ipertestuale del Worker associato alla prima Appliance vRealize Automation.

- c Fare clic sul collegamento KerberosIdpAdapter per aprire la pagina di autenticazione.

Potrebbe essere necessario immettere la password e riavviare il collegamento KerberosIdpAdapter.

- d Specificare l'attributo UID della directory e immettere il valore predefinito sMAAccountName.

- e Selezionare le caselle di controllo **Abilita autenticazione di Windows** e **Abilita reindirizzamento**.

- f Lasciare **NTLM** deselezionato, poiché è necessario solo per i controller di dominio meno recenti.

- g Immettere il nome dell'appliance VA1 per il nome host di reindirizzamento.
- h Fare clic su **Salva**.
- 9 Configurare un criterio di accesso predefinito. La configurazione di Kerberos richiede tre criteri di accesso, ovvero Kerberos, password e password locale.
 - a Selezionare **Amministrazione > Gestione directory > Criteri**.
 - b Selezionare default_access_policy_set.
 - c Fare clic sul valore con collegamento ipertestuale Password sotto l'intestazione Metodi di autenticazione nella riga del browser Web.
 - d Fare clic sulle icone + verdi per creare nuovi metodi di autenticazione per Kerberos, password e password (directory locale).
 - e Per ogni metodo di autenticazione, selezionare TUTTI GLI INTERVALLI come intervallo di rete degli utenti e Browser Web come metodo di accesso al contenuto dell'utente.
 - f Impostare il primo metodo di autenticazione su Kerberos e il metodo di failback su Password.
 - g Fare clic su **Salva**, quindi su **OK**.

Configurazione di Internet Explorer per l'accesso all'interfaccia Web

Se Kerberos è configurato per la distribuzione e si desidera concedere agli utenti l'accesso all'interfaccia Web tramite il browser Internet Explorer, è necessario configurare tale browser.

L'autenticazione Kerberos funziona in combinazione con Directories Management nei sistemi operativi Windows.

Nota non implementare questi passaggi relativi a Kerberos su altri sistemi operativi.

Prerequisiti

Configurare il browser Internet Explorer per ogni utente oppure fornire agli utenti le istruzioni necessarie dopo aver configurato Kerberos.

Procedura

- 1 Verificare di aver eseguito l'accesso a Windows come utente del dominio.
- 2 In Internet Explorer abilitare l'accesso automatico.
 - a Selezionare **Strumenti > Opzioni Internet > Sicurezza**.
 - b Fare clic su **Livello personalizzato**.
 - c Selezionare **Accesso automatico solo nell'area Intranet**.
 - d Fare clic su **OK**.

- 3 Verificare che questa istanza dell'appliance virtuale del connettore faccia parte dell'area Intranet locale.

- a Utilizzare Internet Explorer per accedere all'URL di accesso di Directories Management all'indirizzo *https://myconnectorhost.domain/authenticate/*.
- b Individuare l'area nell'angolo in basso a destra della barra di stato della finestra del browser.

Se l'area è Intranet locale, la configurazione di Internet Explorer è stata completata.

- 4 Se l'area non è Intranet locale, aggiungere l'URL di accesso di Directories Management all'area Intranet.

- a Selezionare **Strumenti > Opzioni Internet > Sicurezza > Intranet locale > Siti**.
- b Selezionare **Rileva automaticamente rete Intranet**.

Se questa opzione non è selezionata, potrebbe essere sufficiente selezionarla per aggiungere all'area Intranet.

- c (Facoltativo) Se è stata selezionata l'opzione **Rileva automaticamente rete Intranet**, fare clic su **OK** finché tutte le finestre di dialogo non verranno chiuse.
- d Nella finestra di dialogo Intranet locale, fare clic su **Avanzate**.

Verrà visualizzata una seconda finestra di dialogo Intranet locale.

- e Immettere l'URL di Directories Management nella casella di testo **Aggiungi il sito Web all'area**.

https://myconnectorhost.domain/authenticate/

- f Fare clic su **Aggiungi > Chiudi > OK**.

- 5 Verificare che Internet Explorer sia in grado di passare l'autenticazione Windows al sito attendibile.

- a Nella finestra di dialogo Opzioni Internet fare clic sulla scheda **Avanzate**.
- b Selezionare **Abilita autenticazione di Windows integrata**.

Questa opzione diventerà effettiva solo dopo il riavvio di Internet Explorer.

- c Fare clic su **OK**.

- 6 Accedere all'interfaccia Web per verificare l'accesso.

Se l'autenticazione Kerberos riesce, l'URL di test si connette all'interfaccia Web.

Risultati

Il protocollo Kerberos protegge tutte le interazioni tra questa istanza del browser Internet Explorer e Directories Management. Gli utenti possono ora utilizzare l'accesso Single Sign-On per accedere al proprio portale My Apps.

Configurazione di Firefox per l'accesso all'interfaccia Web

Se Kerberos è configurato per la distribuzione e si desidera concedere agli utenti l'accesso all'interfaccia Web tramite il browser Firefox, è necessario configurare tale browser.

L'autenticazione Kerberos funziona in combinazione con Directories Management nei sistemi operativi Windows.

Prerequisiti

Configurare il browser Firefox per ogni utente oppure fornire agli utenti le istruzioni necessarie dopo aver configurato Kerberos.

Procedura

- 1 Nella casella di testo URL del browser Firefox immettere **about:config** per accedere alle impostazioni avanzate.
- 2 Fare clic su **Farò attenzione, prometto**.
- 3 Fare doppio clic su **network.negotiate-auth.trusted-uris** nella colonna Nome Parametro.
- 4 Immettere l'URL di Directories Management nella casella di testo.
https://myconnectorhost.domain.com
- 5 Fare clic su **OK**.
- 6 Fare doppio clic su **network.negotiate-auth.delegation-uris** nella colonna Nome Parametro.
- 7 Immettere l'URL di Directories Management nella casella di testo.
https://myconnectorhost.domain.com/authenticate/
- 8 Fare clic su **OK**.
- 9 Verificare la funzionalità di Kerberos utilizzando il browser Firefox per accedere all'URL di accesso di . Ad esempio, *https://myconnectorhost.domain.com/authenticate/*.
Se l'autenticazione Kerberos riesce, l'URL di test si connette all'interfaccia Web.

Risultati

Il protocollo Kerberos protegge tutte le interazioni tra questa istanza del browser Firefox e Directories Management. Gli utenti possono ora utilizzare l'accesso Single Sign-On per accedere al proprio portale My Apps.

Configurazione del browser Chrome per l'accesso all'interfaccia Web

Se Kerberos è configurato per la distribuzione e si desidera concedere agli utenti l'accesso all'interfaccia Web tramite il browser Chrome, è necessario configurare tale browser.

L'autenticazione Kerberos funziona in combinazione con Directories Management nei sistemi operativi Windows.

Nota non implementare questi passaggi relativi a Kerberos su altri sistemi operativi.

Prerequisiti

- Configurare Kerberos.
- Poiché Chrome utilizza la configurazione di Internet Explorer per abilitare l'autenticazione Kerberos, è necessario configurare Internet Explorer per consentire a Chrome di utilizzare la configurazione di Internet Explorer. Per informazioni su come configurare Chrome per l'autenticazione Kerberos, vedere la documentazione di Google.

Procedura

- 1 Verificare la funzionalità di Kerberos utilizzando il browser Chrome.
- 2 Accedere a Directories Management da <https://myconnectorhost.domain.com/authenticate/>.
Se l'autenticazione Kerberos riesce, l'URL di test si connette all'interfaccia Web.

Risultati

Se tutte le configurazioni relative a Kerberos sono corrette, il relativo protocollo (Kerberos) protegge tutte le interazioni tra questa istanza del browser Chrome e Directories Management. Gli utenti possono utilizzare l'accesso Single Sign-On per accedere al proprio portale My Apps.

Aggiornamento di connettori esterni per la gestione delle directory

Se si utilizza un connettore esterno con la configurazione per la gestione delle directory di vRealize Automation, è possibile che di tanto in tanto sia necessario aggiornare tale connettore.

È possibile che sia necessario aggiornare un connettore esterno quando si esegue l'aggiornamento della versione della distribuzione di vRealize Automation o se una nuova build del connettore offre una funzione che si desidera utilizzare.

La presente documentazione è valida solo per gli utenti che hanno distribuito ulteriori appliance di connettori esterni autonomi. In vRealize Automation, le appliance di connettori esterni vengono utilizzate, ad esempio, con l'autenticazione delle smart card.

Per impostazione predefinita, il connettore utilizza il sito web VMware per la procedura di aggiornamento, che richiede una connessione a Internet per l'appliance del connettore. È inoltre necessario configurare le impostazioni del server proxy per l'appliance del connettore, se applicabile.

Se l'istanza del connettore non dispone di una connessione a Internet, è possibile eseguire l'aggiornamento offline. Per un aggiornamento offline, è necessario scaricare il pacchetto di aggiornamento e impostare un server web locale in cui ospitare il file di aggiornamento.

Destinatari

Le presenti informazioni sono destinate a chiunque installi, aggiorni e configuri la gestione delle directory. Sono scritte per amministratori di sistema Windows o Linux esperti che hanno familiarità con la tecnologia delle macchine virtuali e le operazioni di data center.

Preparazione dell'aggiornamento di un connettore esterno

Per preparare l'aggiornamento di un connettore, è necessario verificare la presenza di aggiornamenti disponibili e configurare le impostazioni del server proxy dell'appliance, se applicabile.

- [Verifica della disponibilità di aggiornamenti di un connettore esterno in modalità online](#)

Se l'appliance del connettore dispone di connettività Internet, è possibile verificare la disponibilità di aggiornamenti in modalità online dall'appliance.

- [Configurazione delle impostazioni del server proxy per l'appliance del connettore esterno](#)

L'appliance del connettore accede ai server di aggiornamento VMware tramite Internet. Se la configurazione di rete consente di accedere a Internet tramite un proxy HTTP, è necessario modificare le impostazioni del proxy per l'appliance.

Verifica della disponibilità di aggiornamenti di un connettore esterno in modalità online

Se l'appliance del connettore dispone di connettività Internet, è possibile verificare la disponibilità di aggiornamenti in modalità online dall'appliance.

Procedura

- 1 Accedere all'appliance del connettore come utente root.
- 2 Eseguire il comando seguente.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- 3 Eseguire il seguente comando per verificare la disponibilità di un aggiornamento online.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

Configurazione delle impostazioni del server proxy per l'appliance del connettore esterno

L'appliance del connettore accede ai server di aggiornamento VMware tramite Internet. Se la configurazione di rete consente di accedere a Internet tramite un proxy HTTP, è necessario modificare le impostazioni del proxy per l'appliance.

Consentire al proxy di gestire solo il traffico Internet. Affinché il proxy sia configurato correttamente, impostare il parametro per il traffico interno su no-proxy nel dominio.

Nota I server proxy che richiedono autenticazione non sono supportati.

Prerequisiti

- Verificare di disporre della password root per l'appliance del connettore.
- Verificare di disporre dei dati del server proxy.

Procedura

- 1 Accedere all'appliance del connettore come utente root.

- 2 Immettere YaST nella riga di comando per eseguire la utility YaST.
- 3 Selezionare **Servizi di rete** nel riquadro a sinistra, quindi selezionare **Proxy**.
- 4 Immettere gli URL del server proxy nei campi **URP proxy HTTP** e **URL proxy HTTPS**.
- 5 Selezionare **Fine** e uscire dalla utility YaST.
- 6 Riavviare il server Tomcat sull'appliance virtuale del connettore per utilizzare le nuove impostazioni proxy.

```
service horizon-workspace restart
```

Risultati

A questo punto i server di aggiornamento di VMware sono disponibili per l'appliance del connettore.

Aggiornamento online di un connettore esterno

È possibile aggiornare online un connettore esterno per la gestione delle directory se si dispone di una connessione appropriata.

Prerequisiti

- Verificare che l'appliance del connettore sia in grado di risolvere e raggiungere vapp-updates.vmware.com sulla porta 80 su HTTP.
- Verificare la disponibilità di un aggiornamento del connettore. Eseguire il comando appropriato per verificare la disponibilità di aggiornamenti. Per ulteriori informazioni, vedere [Verifica della disponibilità di un aggiornamento online del connettore di Directories Management](#)
- Verificare che siano disponibili almeno 2 GB di spazio su disco sulla partizione root principale dell'appliance.
- Verificare che il connettore sia configurato correttamente.
- Acquisire uno snapshot dell'appliance del connettore per eseguirne il backup. Per ulteriori informazioni sull'acquisizione degli snapshot, consultare la documentazione di vSphere.
- Se è necessario un server proxy HTTP per l'accesso HTTP in uscita, configurare le impostazioni del server proxy per l'appliance del connettore. Per ulteriori informazioni, vedere [Configurazione delle impostazioni del server proxy per l'appliance del connettore di Directories Management](#)

Procedura

- 1 Accedere all'appliance del connettore come utente root.
- 2 Eseguire il comando seguente.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- 3 Eseguire il seguente comando per verificare la disponibilità di un aggiornamento online.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 4 Eseguire il seguente comando per aggiornare l'appliance.

```
/usr/local/horizon/update/updatemgr.hznupdate
```

I messaggi visualizzati durante l'aggiornamento vengono salvati nel file `update.log` nel percorso `/opt/vmware/var/log/update.log`.

- 5 Eseguire di nuovo il comando `updatemgr.hzn check` per verificare che non sia disponibile un aggiornamento più recente.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- 6 Verificare la versione dell'appliance aggiornata.

```
vami cli version --appliance
```

La nuova versione viene visualizzata.

- 7 Riavviare l'appliance del connettore.

```
reboot
```

Aggiornamento offline di un connettore esterno

Se l'appliance del connettore per la gestione delle directory esistente di vRealize Automation non è in grado di stabilire la connessione con Internet per l'aggiornamento, è possibile eseguire un aggiornamento offline. È necessario impostare un repository di aggiornamenti su un server web locale e configurare l'appliance del connettore per utilizzare il server web locale per l'aggiornamento.

Prerequisiti

- Verificare la disponibilità di un aggiornamento del connettore. Verificare la disponibilità di aggiornamenti sul sito My VMware Downloads all'indirizzo my.vmware.com.
- Verificare che siano disponibili almeno 2 GB di spazio su disco sulla partizione root principale dell'appliance.
- Verificare che il connettore sia configurato correttamente.
- Acquisire uno snapshot dell'appliance del connettore per eseguirne il backup. Per ulteriori informazioni sull'acquisizione degli snapshot, consultare la documentazione di vSphere.

- Configurare l'appliance del connettore in modo da utilizzare un server web locale in cui ospitare il file di aggiornamento. Per ulteriori informazioni, vedere Preparazione di un server web locale per l'aggiornamento offline.

Procedura

1 Preparazione di un server web locale per l'aggiornamento offline

Prima di avviare l'aggiornamento offline del connettore, preparare il server web locale creando una struttura di directory che includa una sottodirectory per l'appliance del connettore.

2 Configurazione del connettore ed esecuzione dell'aggiornamento offline

Configurare l'appliance del connettore in modo che faccia riferimento al server web locale per eseguire un aggiornamento offline. Quindi, aggiornare l'appliance.

Preparazione di un server web locale per l'aggiornamento offline

Prima di avviare l'aggiornamento offline del connettore, preparare il server web locale creando una struttura di directory che includa una sottodirectory per l'appliance del connettore.

Prerequisiti

- Scaricare il file `identity-manager-connector-NumberVersione-NumeroBuild-updaterepo.zip` da My VMware. Visitare my.vmware.com, passare alla pagina VMware Identity Manager Download e scaricare il file elencato in **VMware Identity Manager Connector offline upgrade package**.
- Se si utilizza un server web IIS, configurarlo in modo da consentire i caratteri speciali nei nomi dei file. Tali impostazioni vengono configurate nella sezione **Filtro richieste** selezionando l'opzione **Consenti escape doppi**.

Procedura

- 1 Creare una directory sul server web all'indirizzo `http://YourWebServer/VM/` e copiare il file ZIP scaricato qui.

- 2 Verificare che il server web includa i tipi mime per `.sig` (text/plain) e `.sha256` (text/plain).

Senza questi tipi mime, il server web non è in grado di verificare la disponibilità degli aggiornamenti.

- 3 Decomprimere il file.

I contenuti del file ZIP estratto sono serviti da `http://ServerWebPersonale/VM/`.

I contenuti estratti del file contengono le seguenti sottodirectory: `/manifest` e `/package-pool`.

- 4 Eseguire il comando `updateLocal.hzn` seguente per verificare che l'URL disponga di contenuti di aggiornamento validi.

```
/usr/local/horizon/update/updateLocal.hzn checkurl http://ServerWebPersonale/VM
```

Configurazione del connettore ed esecuzione dell'aggiornamento offline

Configurare l'appliance del connettore in modo che faccia riferimento al server web locale per eseguire un aggiornamento offline. Quindi, aggiornare l'appliance.

Prerequisiti

Preparare un server web locale per l'aggiornamento offline.

Procedura

- 1 Accedere all'appliance del connettore come utente root.
- 2 Eseguire il seguente comando per configurare un repository di aggiornamento che utilizzi un server web locale.

```
/usr/local/horizon/update/updatelocal.hzn seturl http://ServerWebPersonale/VM/
```

Nota Per annullare la configurazione e ripristinare la possibilità di eseguire un aggiornamento online, è possibile eseguire il seguente comando.

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

- 3 Eseguire l'aggiornamento.

- a Eseguire il comando seguente.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- b Eseguire il seguente comando per verificare la versione dell'aggiornamento disponibile.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- c Eseguire il seguente comando per aggiornare il connettore.

```
/usr/local/horizon/update/updatemgr.hznupdate
```

I messaggi visualizzati durante l'aggiornamento vengono salvati nel file `update.log` nel percorso `/opt/vmware/var/log/update.log`.

- d Eseguire di nuovo il comando `updatemgr.hzn check`.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- e Verificare la versione dell'appliance aggiornata.

```
vami cli version --appliance
```

Il comando dovrebbe mostrare la nuova versione.

- f Riavviare l'appliance del connettore.

Ad esempio, dalla riga di comando, eseguire il seguente comando.

```
reboot
```

Risultati

A questo punto, l'aggiornamento del connettore risulta completato.

Configurazione delle impostazioni dopo l'aggiornamento di un connettore esterno

Dopo l'aggiornamento a un connettore 2016.3.1.0 (o più recente) può essere necessario configurare alcune impostazioni.

Aggiungere di nuovo un dominio con autenticazione Kerberos

Se si utilizza l'autenticazione Kerberos o le directory di Active Directory (autenticazione integrata di Windows), è necessario abbandonare un dominio e aggiungerlo di nuovo in seguito. Eseguire questa operazione per tutte le appliance virtuali del connettore presenti nella distribuzione.

- 1 Selezionare **Amministrazione > Gestione directory > Connettori**
- 2 Nella pagina Connettori, per ciascun connettore utilizzato per l'autenticazione Kerberos o una directory Active Directory (autenticazione integrata di Windows), fare clic su **Esci dal dominio**.
- 3 Per aggiungere il dominio, è necessario disporre delle credenziali Active Directory e dei privilegi necessari. Vedere [Unione della macchina con un connettore a un dominio](#) per ulteriori informazioni.
- 4 Se si utilizza l'autenticazione Kerberos, abilitare di nuovo la scheda di autenticazione Kerberos. Per accedere alla pagina Schede di autenticazione, nella pagina Connettori fare clic sul collegamento appropriato nella colonna **Worker** e selezionare la scheda **Schede di autenticazione**.
- 5 Verificare che le altre schede di autenticazione utilizzate siano abilitate.

Aggiornamento della pagina Domini

Se si usa Active Directory (autenticazione integrata di Windows) o Active Directory su LDAP ed è selezionata l'opzione **La directory supporta DNS di Posizione servizio**, è necessario salvare la pagina Domini della directory.

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.

- 2 Selezionare la directory appropriata per modificarla.
- 3 Fornire la password per l'utente Nome distinto di binding, quindi fare clic su **Salva**.
- 4 Fare clic su **Sincronizza impostazioni** sulla parte sinistra della pagina, quindi selezionare la scheda **Domini**.
- 5 Fare clic su **Salva**.

DNS di Posizione servizio e controller di dominio

Nota Nei connettori 2016.3.1.0 e più recenti viene automaticamente creato e popolato un file `domain_krb.properties` con controller di dominio se viene creata una directory per cui è abilitato DNS di Posizione servizio. Quando si salva la pagina Domini dopo un aggiornamento, se è presente un file `domain_krb.properties` nella distribuzione originale, tale file verrà aggiornato con eventuali domini aggiunti successivamente e non inclusi nel file. Se nella distribuzione originale non è presente un file `domain_krb.properties`, il file viene creato e popolato automaticamente con i controller di dominio. Per ulteriori informazioni sul file `domain_krb.properties`, vedere [Informazioni sulla selezione dei controller di dominio](#).

Correzione degli errori di aggiornamento del connettore esterno

È possibile risolvere i problemi di aggiornamento del connettore esterno per la gestione delle directory di vRA consultando i registri degli errori. Se il connettore non si avvia, è possibile tornare a un'istanza precedente eseguendo il rollback a uno snapshot.

- [Consultazione dei registri degli errori di aggiornamento](#)

Risolvere gli errori che si verificano durante l'aggiornamento consultando i registri degli errori. I file di registro dell'aggiornamento si trovano nella directory `/opt/vmware/var/log`.

- [Rollback agli snapshot del connettore](#)

Se il connettore non si avvia correttamente dopo un aggiornamento e non è possibile risolvere il problema consultando i registri degli errori ed eseguendo di nuovo il comando di aggiornamento, è possibile eseguire il rollback a un'istanza precedente del connettore.

- [Raccolta di un bundle di file di registro](#)

È possibile raccogliere un bundle di file di registro da inviare al supporto di VMware. Il bundle può essere recuperato dalla pagina di configurazione del connettore.

Consultazione dei registri degli errori di aggiornamento

Risolvere gli errori che si verificano durante l'aggiornamento consultando i registri degli errori. I file di registro dell'aggiornamento si trovano nella directory `/opt/vmware/var/log`.

Se si verificano errori, il connettore potrebbe non avviarsi dopo l'aggiornamento.

Procedura

- 1 Accedere all'appliance del connettore.
- 2 Andare alla directory `/opt/vmware/var/log`.

- 3 Aprire il file `update.log` e rivedere i messaggi di errore.
- 4 Risolvere gli errori, quindi eseguire di nuovo il comando di aggiornamento. Il comando di aggiornamento riprende l'operazione dal punto in cui si era interrotto.

Nota In alternativa, è possibile ripristinare uno snapshot ed eseguire di nuovo l'aggiornamento.

Rollback agli snapshot del connettore

Se il connettore non si avvia correttamente dopo un aggiornamento e non è possibile risolvere il problema consultando i registri degli errori ed eseguendo di nuovo il comando di aggiornamento, è possibile eseguire il rollback a un'istanza precedente del connettore.

Procedura

- ◆ Ripristinare uno degli snapshot acquisiti come backup dell'istanza originale del connettore. Per ulteriori informazioni, vedere la documentazione di vSphere.

Raccolta di un bundle di file di registro

È possibile raccogliere un bundle di file di registro da inviare al supporto di VMware. Il bundle può essere recuperato dalla pagina di configurazione del connettore.

I seguenti file di registro vengono raccolti nel bundle.

Tabella 2-9. File di registro

Componente	Percorso del file di registro	Descrizione
Registri di Apache Tomcat (<code>catalina.log</code>)	<code>/opt/vmware/horizon/workspace/logs/catalina.log</code>	I messaggi dei record di Apache Tomcat che non sono registrati in altri file di registro.
Registri del configuratore (<code>configurator.log</code>)	<code>/opt/vmware/horizon/workspace/logs/configurator.log</code>	Richieste che il configuratore riceve dal client REST e dall'interfaccia Web.
Registri del connettore (<code>connector.log</code>)	<code>/opt/vmware/horizon/workspace/logs/connector.log</code>	Un record di ogni richiesta ricevuta dall'interfaccia Web. Ogni voce del registro include anche l'URL della richiesta, il formato data/ora e le eccezioni. Nessuna azione di sincronizzazione viene registrata.

Procedura

- 1 Accedere alla pagina di configurazione del connettore all'indirizzo `https://connectorURL:8443/cfg/logs`.
- 2 Fare clic su **Prepara bundle registri**.
- 3 Scaricare il bundle e inviarlo al supporto di VMware.

Scenario: configurazione di un collegamento Active Directory per un vRealize Automation ad alta disponibilità

Si supponga che un amministratore tenant voglia configurare un'Active Directory sulla connessione della directory LDAP per supportare l'autenticazione degli utenti per una distribuzione vRealize Automation ad alta disponibilità.

Ogni appliance vRealize Automation include un connettore che supporta l'autenticazione utente, anche se in genere viene configurato un solo connettore per eseguire la sincronizzazione delle directory. Non è importante quale sia il connettore scelto per la sincronizzazione. Per supportare l'alta disponibilità di Gestione directory, è necessario configurare un secondo connettore che corrisponda alla seconda appliance vRealize Automation, si connetta al provider di identità e punti alla stessa istanza di Active Directory. Con questa configurazione, se in un'appliance si verifica un errore, l'altra la sostituisce per la gestione dell'autenticazione degli utenti.

In un ambiente ad alta disponibilità, tutti i nodi devono servire lo stesso set di Active Directory, utenti, metodo di autenticazione e così via. Il metodo più diretto per implementare questa configurazione consiste nel promuovere il provider di identità nel cluster impostando l'host di bilanciamento del carico come host del provider di identità. Con questa configurazione, tutte le richieste di autenticazione vengono indirizzate al bilanciamento del carico, che a sua volta le inoltra al connettore appropriato.

Prerequisiti

- Installare una distribuzione vRealize Automation distribuita con bilanciamento del carico appropriato. Vedere *Installazione di vRealize Automation*.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Directory**.
- 2 Fare clic su **Aggiungi directory**.
- 3 Immettere le impostazioni dell'account Active Directory specifico e accettare le opzioni predefinite.

Opzione	Input di esempio
Nome directory	Aggiungere l'indirizzo IP del nome di dominio Active Directory.
Connettore di sincronizzazione	Ogni appliance vRealize Automation include un connettore. Usare uno qualsiasi dei connettori disponibili.
DN di base	Immettere il DN (Distinguished Name) del punto di inizio per le ricerche nel server della directory. Ad esempio, cn=users,dc=corp,dc=local .

Opzione	Input di esempio
DN di binding	Immettere il DN (Distinguished Name) completo, incluso il CN (Common Name), di un account utente di Active Directory che disponga di privilegi per la ricerca degli utenti. Ad esempio cn=config_admin infra,cn=users,dc=corp,dc=local.
Password DN di binding	Immettere la password di Active Directory per l'account che può effettuare la ricerca di utenti.

- 4 Fare clic su **Prova connessione** per verificare la connessione alla directory configurata.

Se la connessione non riesce, verificare le voci immesse in tutti i campi e rivolgersi all'amministratore di sistema se necessario.

- 5 Fare clic su **Salva e avanti**.

Verrà visualizzata la pagina Scegli i domini con l'elenco dei domini.

- 6 Lasciare selezionato il dominio predefinito e fare clic su **Avanti**.

- 7 Verificare che i nomi di attributo siano mappati agli attributi di Active Directory corretti. In caso contrario, selezionare l'attributo di Active Directory corretto dal menu a discesa. Fare clic su **Avanti**.

- 8 Selezionare i gruppi e gli utenti che si desidera sincronizzare.

a Fare clic sull'icona **Aggiungi** (+).

b Immettere il dominio dell'utente e fare clic su **Trova gruppi**.

Ad esempio, **cn=users,dc=corp,dc=local**.

c Selezionare la casella di controllo **Seleziona tutto**.

d Fare clic su **Seleziona**.

e Fare clic su **Avanti**.

f Fare clic su **+** per aggiungere ulteriori utenti. Ad esempio, immettere **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Per escludere alcuni utenti, fare clic su segno + per creare un filtro con cui escludere alcuni tipi di utenti. È possibile selezionare l'attributo da utilizzare per filtrare gli utenti, la regola di query e il valore.

g Fare clic su **Avanti**.

- 9 Rivedere la pagina per verificare quanti utenti e gruppi siano sincronizzati con la directory e fare clic su **Sincronizza directory**.

Il processo di sincronizzazione della directory richiede un certo di tempo ma avviene in background ed è possibile continuare a lavorare.

10 Configurare un secondo connettore per supportare l'alta disponibilità.

- a Accedere al bilanciamento del carico della distribuzione vRealize Automation come amministratore tenant.

L'URL del bilanciamento del carico è *load balancer address/vcac/org/tenant_name*.

- b Selezionare **Amministrazione > Gestione directory > Provider di identità**.

- c Fare clic sul provider di identità attualmente in uso per il sistema.

Vengono visualizzati la directory e il connettore che correntemente forniscono al sistema la gestione di base delle identità.

- d Fare clic sull'elenco a discesa **Aggiungi connettore** e selezionare il connettore corrispondente all'appliance vRealize Automation secondaria.

- e Immettere la password appropriata nella casella di testo **Password DN di binding** visualizzata alla selezione del connettore.

- f Fare clic su **Aggiungi connettore**.

- g Modificare il nome host per puntare al bilanciamento del carico.

Risultati

È stata effettuata la connessione dell'Active Directory aziendale a vRealize Automation ed è stato configurato Gestione directory per l'alta disponibilità.

Operazioni successive

Per offrire una sicurezza avanzata, è possibile configurare un'attendibilità bidirezionale tra il provider di identità e Active Directory. Vedere [Configurazione di una relazione di trust bidirezionale tra vRealize Automation e Active Directory](#).

Configurazione dei connettori esterni per smart card e dell'autenticazione del provider di identità di terze parti in vRealize Automation

Un amministratore di sistema deve configurare un connettore esterno per la distribuzione vRealize Automation utilizzando Gestione directory se vengono utilizzati provider di identità di terzi con l'autenticazione dei certificati o l'autenticazione delle smart card. Inoltre, la procedura qui riportata si applica più in generale a tutti i tipi di autenticazione di certificato.

Gestione directory supporta più provider di identità e cluster di connettori per ciascun Active Directory configurato. Per utilizzare l'autenticazione smart card o provider di identità di terze parti, è possibile impostare un unico connettore esterno oppure un cluster di connettori con un provider di identità adatto, disposto dietro un bilanciamento del carico che consente il pass-through SSL. Vedere [Gestione di connettori e cluster di connettori](#) per ulteriori informazioni.

Vedere [Aggiornamento di connettori esterni per la gestione delle directory](#) per informazioni sull'aggiornamento di un connettore esterno.

Esistono varie opzioni di configurazione dei certificati a disposizione dell'utente, che possono essere utilizzate con l'autenticazione smart card. Vedere [Configurazione di un certificato o di un adattatore per smart card per l'uso con Gestione directory](#).

Prerequisiti

- Configurare una connessione Active Directory opportuna, da utilizzare con la distribuzione di vRealize Automation.
- Scaricare il file OVA necessario alla configurazione di un connettore da [Strumenti e SDK di VMware vRealize Automation](#).
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

1 [Generazione di un token di attivazione del connettore](#)

Prima di distribuire l'appliance virtuale del connettore per utilizzare l'autenticazione della smart card, generare un codice di attivazione per il nuovo connettore dalla console di vRealize Automation. Il codice di attivazione viene utilizzato per stabilire la comunicazione tra il connettore e Gestione directory.

2 [Distribuzione del file OVA per il connettore](#)

Dopo aver scaricato il file OVA per un connettore, è possibile distribuirlo mediante VMware vSphere Client o vSphere Web Client.

3 [Configurazione delle impostazioni del connettore](#)

Dopo aver distribuito l'OVA del connettore, è necessario eseguire la procedura guidata di impostazione per attivare l'appliance e configurare le password degli amministratori.

4 [Applicazione di autorità di certificati pubblici](#)

Quando si installa Gestione directory, viene generato un certificato SSL predefinito. È possibile utilizzare il certificato predefinito a scopo di test, ma per gli ambienti di produzione è necessario generare e installare i certificati SSL commerciali.

5 [Creazione di un provider di identità per l'area di lavoro](#)

È necessario creare un provider di identità per l'area di lavoro da utilizzare come connettore esterno.

6 [Configurazione dell'autenticazione dei certificati e delle regole predefinite dei criteri di accesso](#)

È necessario configurare il connettore esterno da utilizzare con Active Directory e il dominio di vRealize Automation.

Generazione di un token di attivazione del connettore

Prima di distribuire l'appliance virtuale del connettore per utilizzare l'autenticazione della smart card, generare un codice di attivazione per il nuovo connettore dalla console di vRealize Automation. Il codice di attivazione viene utilizzato per stabilire la comunicazione tra il connettore e Gestione directory.

È possibile configurare un unico connettore o un cluster di connettori. Per utilizzare un cluster di connettori, ripetere questa procedura per ciascun componente necessario.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Connettori**.
- 2 Fare clic su **Aggiungi connettore**.
- 3 Nella casella di testo **Nome ID connettore**, digitare un nome per il nuovo connettore.
- 4 Fare clic su **Genera codice di attivazione**.
Nella casella del **codice di attivazione del connettore**, viene visualizzato il codice di attivazione relativo al connettore.
- 5 Copiare il codice di attivazione da utilizzare durante la configurazione del connettore mediante il file OVA.
- 6 Fare clic su **OK**.

Distribuzione del file OVA per il connettore

Dopo aver scaricato il file OVA per un connettore, è possibile distribuirlo mediante VMware vSphere Client o vSphere Web Client.

Distribuire il file OVA utilizzando vSphere Client o vSphere Web Client.

Prerequisiti

- Identificare i record DNS e il nome dell'host da utilizzare per la distribuzione dell'OVA per il connettore.
- Nel caso di vSphere Web Client, scegliere i browser Firefox o Chrome. Non utilizzare Internet Explorer per distribuire il file OVA.
- Scaricare il file OVA necessario alla configurazione di un connettore da [Strumenti e SDK di VMware vRealize Automation](#).

Procedura

- 1 In vSphere Client o vSphere Web Client, selezionare **File > Distribuisci modello OVF**.
- 2 Nelle pagine relative a Distribuisci modello OVF, immettere le informazioni specifiche per la distribuzione del connettore.

Pagina	Descrizione
Origine	Selezionare la posizione del pacchetto OVA oppure immettere un URL specifico.
Dettagli del modello OVA	Verificare di aver selezionato la versione corretta.

Pagina	Descrizione
Licenza	Leggere l'accordo di licenza con l'utente finale e fare clic sul pulsante per accettare .
Nome e posizione	Immettere un nome per l'appliance virtuale. Il nome deve essere univoco all'interno della cartella dell'inventario e può contenere fino a 80 caratteri. Per i nomi viene fatta distinzione tra lettere maiuscole e minuscole. Selezionare una posizione per l'appliance virtuale.
Host/Cluster	Selezionare l'host o il cluster per eseguire il modello distribuito.
Pool di risorse	Selezionare il pool di risorse.
Storage	Selezionare la posizione per archiviare i file della macchina virtuale.
Formato disco	Selezionare il formato del disco relativo ai file. Per gli ambienti di produzione, selezionare un formato Thick Provision . Utilizzare il formato Thin Provision per la valutazione e il testing.
Mappatura di rete	Mappare le reti nell'ambiente alle reti nel modello OVF.
Proprietà	<p>a Nel campo Impostazioni fuso orario, selezionare il fuso orario corretto.</p> <p>b La casella di controllo relativa al programma CEIP (Customer Experience Improvement Program) è selezionata per impostazione predefinita. I dati anonimi sulla distribuzione vengono raccolti da VMware per migliorare l'esperienza dell'utente sulla base dei requisiti espressi. Se l'utente preferisce che i dati non vengano raccolti, deselezionare la casella di controllo.</p> <p>c Nella casella di testo Nome host, immettere il nome dell'host da utilizzare. Se la casella viene lasciata vuota, la ricerca del nome dell'host viene effettuata mediante il DNS inverso.</p> <p>d Per configurare l'indirizzo IP statico per il connettore, immettere l'indirizzo di ciascuno dei seguenti elementi: gateway predefinito, DNS, indirizzo IP e netmask.</p> <p>Importante Se uno dei quattro campi relativi agli indirizzi viene lasciato vuoto, incluso Nome host, viene utilizzato il DHCP.</p> <p>Per configurare il DHCP, lasciare vuoti i campi relativi agli indirizzi.</p>
Completamento	Rivedere le selezioni e fare clic su Fine .

A seconda della velocità di rete, possono essere necessari alcuni minuti per la distribuzione. È possibile visualizzare l'avanzamento nella relativa finestra di dialogo.

- Una volta completata la distribuzione, selezionare l'appliance del , fare clic con il pulsante destro del mouse e selezionare il pulsante di **accensione > Accendi**.

L'appliance del viene inizializzata. È possibile andare nella scheda della **console** per visualizzare i dettagli. Una volta terminata l'inizializzazione dell'appliance virtuale, nello schermo della console vengono visualizzati la versione del e gli URL per accedere alla procedura guidata di impostazione del e completare la configurazione.

Operazioni successive

Utilizzare la procedura guidata di impostazione per aggiungere il codice di attivazione e le password amministrative.

Configurazione delle impostazioni del connettore

Dopo aver distribuito l'OVA del connettore, è necessario eseguire la procedura guidata di impostazione per attivare l'appliance e configurare le password degli amministratori.

Prerequisiti

- Aver generato un codice di attivazione per il connettore.
- Assicurarsi che l'appliance del connettore sia acceso e conoscere l'URL del connettore.
- Raccogliere un elenco di password da utilizzare per l'amministratore del connettore, l'account radice e l'account dell'utente SSH.

Procedura

- 1 Per eseguire la procedura guidata di impostazione, immettere l'URL del connettore visualizzato nella scheda della console dopo la distribuzione dell'OVA.
- 2 Nella pagina di benvenuto, fare clic su **Continua**.
- 3 Creare password complesse per i seguenti account di amministratori dell'appliance virtuale del connettore.

Le password complesse devono essere almeno di otto caratteri e comprendere lettere maiuscole e minuscole, nonché almeno un numero e un carattere speciale.

Opzione	Descrizione
Amministratore dell'appliance	<p>Creare la password per l'amministratore dell'appliance. Il nome utente è admin e non può essere modificato. Questo account e questa password servono ad accedere ai servizi del connettore per gestire certificati, password dell'appliance e configurazione Syslog.</p> <p>Importante La password dell'utente admin deve essere di almeno 6 caratteri.</p>
Account radice	Per installare l'appliance del connettore, è stata utilizzata una password radice predefinita di VMware. Creare una nuova password radice.
Account dell'utente SSH	Creare la password da utilizzare per l'accesso remoto all'appliance del connettore.

- 4 Fare clic su **Continua**.
- 5 Nella pagina di attivazione del connettore, incollare il codice di attivazione e fare clic su **Continua**.
- 6 Se si utilizza un certificato autofirmato nel connettore interno di vRealize Automation, è possibile ottenere il certificato corretto eseguendo il comando seguente nell'appliance vRealize Automation: `cat /etc/apache2/server-cert.pem`

Selezionare la scheda per **terminare l'SSL in un bilanciamento del carico**, quindi fare clic sul collegamento `/horizon_workspace_rootca.pem`.

Il codice di attivazione viene verificato e la comunicazione tra il servizio e l'istanza del connettore viene stabilita in modo da completare la configurazione del connettore.

Operazioni successive

All'interno del servizio, impostare l'ambiente in base alle proprie esigenze. Ad esempio, se si desidera sincronizzare due directory Autenticazione integrata di Windows ed è stato aggiunto un ulteriore connettore, creare la directory e associarla al nuovo connettore.

Applicazione di autorità di certificati pubblici

Quando si installa Gestione directory, viene generato un certificato SSL predefinito. È possibile utilizzare il certificato predefinito a scopo di test, ma per gli ambienti di produzione è necessario generare e installare i certificati SSL commerciali.

Se Gestione directory punta a un bilanciamento del carico, il certificato SSL viene applicato al bilanciamento del carico.

Quando si importa un certificato, è necessario selezionare **Contrassegna la chiave come esportabile**.

Se si genera una richiesta CSR per un certificato personalizzato, è sufficiente specificare il CN o il nome del dominio del sito dell'autorità di certificazione.

Prerequisiti

Generare una richiesta di firma del certificato e ottenere un certificato valido e firmato da un'autorità di certificazione. È possibile utilizzare anche certificati SSL firmati da un'autorità di certificazione forniti dall'organizzazione. Il formato del certificato deve essere PEM.

Procedura

- 1 Accedere alla pagina di amministrazione dell'appliance del connettore come utente amministratore all'indirizzo seguente:
`https://myconnector.mycompany:8443/cfg`
- 2 Nella console dell'amministratore, fare clic sull'opzione relativa alle **impostazioni dell'appliance**.
La configurazione dell'appliance virtuale viene selezionata per impostazione predefinita.
- 3 Fare clic sull'opzione relativa alla **gestione delle configurazioni**.
- 4 Immettere la password dell'utente amministratore del server VMware Identity Manager.
- 5 Selezionare l'opzione per **installare il certificato**.
- 6 Nella scheda per terminare l'SSL dell'**appliance Identity Manager**, selezionare **Certificato personalizzato**.

- 7** Nella casella di testo della **catena di certificati SSL**, incollare i certificati dell'host, intermedi e radice in questo ordine.

Il certificato SSL funziona solo se la catena di certificati viene specificata nell'ordine corretto. Per ciascun certificato, copiare tutto il contenuto presente tra le righe -----BEGIN CERTIFICATE----- ed -----END CERTIFICATE-----

Assicurarsi che nel certificato sia incluso il nome dell'host per il nome di dominio completo.

- 8** Incollare la chiave privata nella casella di testo Chiave privata. Copiare tutto il contenuto presente tra le righe -----BEGIN RSA PRIVATE KEY----- ed -----END RSA PRIVATE KEY-----.

- 9** Fare clic su **Salva**.

Esempio: esempi di certificati

Esempio di catena di certificati

```
-----BEGIN CERTIFICATE-----
jIQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+
...
...
...
W53+O05j5xsxzDJfWr1lqBiff/OkiYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQvt90+
...
...
...
O05j5xsxzDJfWr1lqBiff/OkiYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjIQvt9W5+C3HU17bUOwvhp/r0+
...
...
...
5j5xsxzDJfWr1lqW53+O0Biff/OkiYCPcyK1
-----END CERTIFICATE-----
```

Esempio di chiave privata

```
-----BEGIN RSA PRIVATE KEY-----
jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+
...
...
1lqBIFFW53+O05j5xsxzDJfWr/OklYCPcyK1
-----END RSA PRIVATE KEY-----
```

Creazione di un provider di identità per l'area di lavoro

È necessario creare un provider di identità per l'area di lavoro da utilizzare come connettore esterno.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Provider di identità**.
- 2 Selezionare **Aggiungi provider di identità**.
- 3 Selezionare **Crea provider di identità Workspace**.
- 4 Immettere un nome per il provider di identità nel campo **Nome del provider di identità**.
- 5 Selezionare la directory che corrisponde agli utenti di questo provider di identità.
La directory selezionata determina quali connettori sono disponibili per il provider di identità.
- 6 Selezionare il connettore o i connettori esterni configurati per l'autenticazione smart card.

Nota Se la distribuzione si trova dietro un bilanciamento del carico, immettere l'URL di quest'ultimo.

- 7 Selezionare la rete di accedere al provider di identità.
- 8 Fare clic su **Aggiungi**.

Configurazione dell'autenticazione dei certificati e delle regole predefinite dei criteri di accesso

È necessario configurare il connettore esterno da utilizzare con Active Directory e il dominio di vRealize Automation.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Connettori**.

2 Selezionare il connettore desiderato nella colonna **Worker**.

Il worker selezionato viene mostrato nella casella di testo relativa al **nome del worker**, all'interno della scheda dei **dettagli** del connettore, mentre le informazioni sul tipo di connettore vengono visualizzate nella casella di testo **Tipo di connettore**.

3 Assicurarsi che il connettore sia collegato con l'Active Directory desiderato specificando tale directory nella casella di testo della **directory associata**.**4** Immettere il nome di dominio opportuno nella casella di testo dei **domini associati**.**5** Selezionare la scheda **AuthAdapters** e abilitare CertificateAuthAdapter.**6** Configurare opportunamente l'autenticazione del certificato per la distribuzione.

Vedere [Configurazione dell'autenticazione dei certificati per Gestione directory](#).

7 Selezionare **Amministrazione > Gestione directory > Criteri**.**8** Fare clic sul pulsante di **modifica del criterio predefinito**.**9** Aggiungere il certificato alle regole dei criteri e renderlo il primo metodo di autenticazione.

Il certificato deve essere il primo metodo di autenticazione elencato nella regola del criterio. In caso contrario, l'autenticazione del certificato non verrà eseguita correttamente.

Creazione di un link di Active Directory multidominio o a più foreste

In qualità di amministratore di sistema è necessario configurare un link di Active Directory multidominio o a più foreste.

La procedura per configurare un link di Active Directory multidominio o a più foreste è fondamentalmente la stessa. Per un link a più foreste, è necessaria l'attendibilità bidirezionale tra tutti i domini applicabili.

Prerequisiti

- Installare una distribuzione vRealize Automation distribuita con bilanciamento del carico appropriato. Vedere *Installazione di vRealize Automation*.
- Accedere a vRealize Automation come **amministratore tenant**.
- Configurare i domini e le foreste di Active Directory appropriati per la distribuzione.

Procedura

1 Selezionare **Amministrazione > Gestione directory > Directory**.**2** Fare clic su **Aggiungi directory**.**3** Nella pagina Aggiungi directory, specificare un nome per il server di Active Directory nella casella di testo **Nome directory**.**4** Selezionare **Active Directory (autenticazione integrata di Windows)** sotto il titolo **Nome directory**.

- 5 Configurare il connettore che sincronizza gli utenti di Active Directory con la directory Directories Management di VMware nella sezione Sincronizzazione directory e autenticazione.

Opzione	Descrizione
Connettore di sincronizzazione	Selezionare il connettore appropriato da utilizzare per il sistema. Ogni Appliance vRealize Automation contiene un connettore predefinito. Rivolgersi all'amministratore di sistema per aiuto nella scelta del connettore appropriato.
Autenticazione	Fare clic sul pulsante di opzione appropriato per indicare se anche il connettore selezionato deve eseguire l'autenticazione.
Attributo di ricerca directory	Selezionare l'attributo dell'account appropriato contenente il nome utente.

In base alla configurazione della distribuzione, saranno disponibili uno o più connettori da utilizzare.

- 6 Immettere le credenziali necessarie per l'unione di dominio nelle caselle di testo **Nome dominio**, **Nome utente amministratore di dominio** e **Password amministratore di dominio**.

Ad esempio, inserire: **Nome dominio**: hs.trcint.com, **Nome utente amministratore di dominio**: devadmin, **Password amministratore di dominio**: xxxx.

- 7 Nella sezione **Dettagli utente di binding** immettere le credenziali appropriate di Active Directory (autenticazione integrata di Windows) per consentire la sincronizzazione delle directory.

Opzione	Descrizione
UPN utente di binding	Immettere il nome dell'entità dell'utente che può autenticarsi nel dominio. Ad esempio UserName@example.com.
Password DN di binding	Specificare la password dell'utente Binding.

- 8 Fare clic su **Salva e avanti**.

Viene visualizzata la pagina Seleziona domini con l'elenco dei domini.


- 9 Fare clic sulle caselle di controllo appropriate per selezionare i domini desiderati per la distribuzione del sistema.

- 10 Fare clic su **Avanti**.

- 11 Verificare che i nomi degli attributi della directory di Directories Management siano mappati agli attributi di Active Directory corretti.

Se i nomi degli attributi di directory sono mappati in modo errato, selezionare l'attributo Active Directory corretto nel menu a discesa.


- 12 Fare clic su **Avanti**.


- 13** Fare clic su  per selezionare i gruppi da sincronizzare da Active Directory alla directory.

Quando si aggiunge un gruppo Active Directory, i membri di tale gruppo verranno aggiunti se non sono inclusi nell'elenco Utenti.

Nota il sistema di autenticazione degli utenti di Directories Management importa i dati da Active Directory quando si aggiungono gruppi e utenti e la velocità del sistema dipende dalle caratteristiche di Active Directory. È quindi possibile che l'importazione di un numero elevato di gruppi e utenti richieda una quantità di tempo significativa. Per ridurre eventuali ritardi o problemi, aggiungere solo i gruppi e gli utenti effettivamente necessari per il funzionamento di vRealize Automation. In caso di errori o di peggioramento delle prestazioni del sistema, chiudere tutte le applicazioni non necessarie e verificare che sia stata allocata ad Active Directory una quantità di memoria appropriata. Se i problemi persistono, aumentare la quantità di memoria allocata ad Active Directory in base alle necessità. Per sistemi con un elevato numero di utenti e gruppi, potrebbe essere necessario allocare fino a 24 GB di memoria ad Active Directory.

- 14** Fare clic su **Avanti**.

- 15** Fare clic su  per aggiungere ulteriori utenti. Ad esempio, immettere **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Per escludere utenti, fare clic su  per creare un filtro che escluda determinati tipi di utenti. È possibile selezionare l'attributo da utilizzare per filtrare gli utenti, la regola di query e il valore.

- 16** Fare clic su **Avanti**.

- 17** Esaminare la pagina per verificare quanti utenti e gruppi sono in corso di sincronizzazione con la directory.

Se si desidera apportare modifiche agli utenti e ai gruppi, fare clic sui collegamenti Modifica.

- 18** Fare clic su **Push in area di lavoro** per avviare la sincronizzazione con la directory.

Operazioni successive

Configurazione dei ruoli di utenti e gruppi

Gli amministratori tenant possono creare gruppi di business e gruppi personalizzati, nonché assegnare diritti di accesso utente alla console di vRealize Automation.

Assegnazione di ruoli a utenti e gruppi della directory

Per concedere agli utenti i diritti di accesso, gli amministratori tenant assegnano ruoli a utenti o gruppi.

Per consentire agli utenti o ai gruppi di modificare e attivare una pipeline, è necessario assegnare loro le autorizzazioni richieste. Quando si assegna a utenti e gruppi il ruolo di Release Manager, si consente loro di modificare e attivare la pipeline. Quando si assegna a utenti e gruppi il ruolo di Release Engineer, si consente loro di attivare la pipeline. Per ulteriori informazioni, vedere la guida relativa all'*utilizzo di vRealize Code Stream*.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Utenti e gruppi > Utenti e gruppi della directory**.
- 2 Immettere il nome di un utente o di un gruppo nella casella **Cerca** e premere Invio.
Non utilizzare i caratteri "@", "\" e "/" nel nome. È possibile ottimizzare la ricerca specificando il nome completo dell'utente o del gruppo nella forma utente@dominio.
- 3 Fare clic sul nome dell'utente o del gruppo a cui assegnare i ruoli.
- 4 Selezionare uno o più ruoli dall'elenco **Aggiungi ruoli a questo utente**.
L'elenco **Autorità concesse dai ruoli selezionati** indica le autorità specifiche che si stanno autorizzando.
- 5 (Facoltativo) Fare clic su **Avanti** per visualizzare altre informazioni sull'utente o sul gruppo.
- 6 Nella scheda **Generale** della pagina **Dettagli utente**, scorrere l'elenco di ruoli per aggiungere l'utente.
 - a Per concedere all'utente le autorizzazioni necessarie per modificare e attivare una pipeline, selezionare la casella di controllo **Release Manager**.
 - b Per concedere all'utente le autorizzazioni necessarie per attivare una pipeline, selezionare la casella di controllo **Release Engineer**.
- 7 Fare clic su **Aggiorna**.

Risultati

Gli utenti che sono attualmente connessi a vRealize Automation devono disconnettersi e riaccedere a vRealize Automation per poter visualizzare le pagine per cui hanno ricevuto le autorizzazioni di accesso.

Operazioni successive

Facoltativamente è possibile creare gruppi personalizzati propri da utenti e gruppi nei collegamenti di Active Directory. Vedere [Creazione di un gruppo personalizzato](#).

Creazione di un gruppo personalizzato

Gli amministratori Tenant possono creare gruppi personalizzati combinando altri gruppi personalizzati, gruppi di archivi identità e utenti di archivi identità individuali. I gruppi personalizzati forniscono maggiore controllo granulare sull'accesso all'interno di vRealize

Automation rispetto ai gruppi di business che corrispondono a una linea di business, un reparto o un'altra unità organizzativa.

I gruppi personalizzati consentono di assegnare diritti di accesso per le attività su una base più dettagliata rispetto alle assegnazioni di gruppo vRealize Automation standard. Ad esempio, si potrebbe pensare di creare un gruppo personalizzato per consentire agli amministratori del tenant di controllare chi dispone delle autorizzazioni specifiche all'interno del tenant.

È possibile assegnare ruoli a un gruppo personalizzato, ma questo non è necessario in tutti i casi. Ad esempio, è possibile creare il gruppo personalizzato chiamato Machine Specification Approvers, da utilizzare per tutte le pre-approvazioni delle macchine. È possibile anche creare gruppi personalizzati da associare a gruppi di business in modo che sia possibile gestire tutti i gruppi da un'unica punto. In questi casi, non è necessario assegnare ruoli.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

1 Selezionare **Amministrazione > Utenti e gruppi > Gruppi personalizzati**.

2 Fare clic su **Nuovo**.

3 Specificare il nome del gruppo nella casella di testo **Nome**.

I nomi dei gruppi personalizzati non possono contenere la combinazione di un punto e virgola (;) seguito da un segno uguale (=).

4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.

5 Selezionare uno o più ruoli dall'elenco Aggiungi ruoli a questo gruppo.

L'elenco Autorità concesse dai ruoli selezionati indica le autorità specifiche che si stanno autorizzando.

6 Fare clic su **Avanti**.

7 Aggiungere utenti e gruppi per creare il gruppo personalizzato.

a Immettere il nome di un utente o di un gruppo nella casella **Cerca** e premere Invio.

Non utilizzare i caratteri "@", "\" e "/" nel nome. È possibile ottimizzare la ricerca specificando il nome completo dell'utente o del gruppo nella forma utente@dominio.

b Selezionare l'utente o il gruppo da aggiungere al gruppo personalizzato.

8 Fare clic su **Fine**.

Risultati

Gli utenti che sono attualmente connessi a vRealize Automation devono disconnettersi e riaccedere a vRealize Automation per poter visualizzare le pagine per cui hanno ricevuto le autorizzazioni di accesso.

Aggiunta di utenti JIT con regole e gruppi personalizzati

È possibile aggiungere utenti di vRealize Automation in una distribuzione senza accesso ad Active Directory utilizzando il provisioning degli utenti JIT. Per richiamare il provisioning JIT per i nuovi utenti, è necessario creare regole per popolare il gruppo personalizzato pertinente.

All'accesso iniziale, agli utenti JIT viene assegnata l'iscrizione al gruppo in modo dinamico in base alle regole create nella pagina della procedura guidata Iscrizione avanzata al gruppo. Dopo l'accesso iniziale, è possibile assegnare l'appartenenza al gruppo nel modo consueto. Questa seconda pagina della procedura guidata contiene quattro caselle di selezione per la creazione di regole basate su una serie di criteri che definiscono gli utenti JIT.

Ad esempio, nella prima casella di selezione della regola è possibile selezionare Dominio come criterio e quindi Corrisponde a nella seconda casella. Nella terza casella della regola è possibile immettere un dominio. Queste selezioni creano una regola che definisce utenti basati sull'appartenenza JIT associati al dominio specificato. La terza casella di selezione è una casella di immissione a formato libero che consente di immettere qualsiasi informazione logicamente correlata alle selezioni delle prime due caselle di selezione.

Nota Quando si configurano gli utenti JIT, la mappatura del formato NameId specifica un attributo utilizzato per identificare in modo univoco un utente. Questo attributo utilizzato come NameId deve essere univoco per l'utente e l'attributo stesso deve essere specificato come parte dell'attestazione SAML. Se si modifica l'attributo NameId o il valore di NameId, si verificherà un errore durante il tentativo di accesso. Ad esempio, se si mappa NameId a SAMAccountName dell'utente utilizzando il formato NameId urn:oasis:names:tc:SAML:2.0:nameid-format:transient, è necessario specificare anche SAMAccountName separatamente. Il nome utente e il valore di SAMAccountName non devono mai essere modificati.

vRealize Automation supporta la corrispondenza con caratteri jolly per la configurazione degli utenti JIT. Per ulteriori informazioni sull'abilitazione e l'utilizzo della corrispondenza con caratteri jolly, vedere [Utilizzo della corrispondenza basata su caratteri jolly per gli utenti JIT](#).

Nota È possibile creare più regole per popolare gli utenti JIT in base a una serie di criteri. Se si creano più regole, è possibile utilizzare la casella di selezione della regola **Corrisponde a** presente sopra le caselle della regola principale, per indicare se vRealize Automation deve corrispondere a una qualsiasi o a tutte le regole quando vengono popolati gli utenti JIT.

Procedura

- 1 Selezionare **Amministrazione > Utenti e gruppi > Gruppi personalizzati** e individuare un gruppo esistente, ad esempio un gruppo appropriato per gli utenti JIT.

Vedere [Creazione di un gruppo personalizzato](#) per ulteriori informazioni.

Fare clic nella riga del gruppo ma non sul nome del gruppo.

- 2 Fare clic su **Iscrizione avanzata**.

Se lo si desidera, è possibile aggiungere singoli utenti nella pagina Aggiungi utenti a gruppo.

- 3 Fare clic su **Avanti** per visualizzare la pagina delle regole del gruppo.
- 4 Utilizzare le caselle di corrispondenza e di selezione della regola per creare una o più regole appropriate per la configurazione degli utenti.

Nelle tre caselle di selezione della regola principale, presenti sotto la casella di selezione della regola **Corrisponde a**, fare clic sulle frecce a discesa e immettere le informazioni per attivare i menu a discesa che consentono di creare la regola desiderata. È comunque sempre possibile utilizzare i caratteri * e \ come descritto in precedenza.

- 5 Fare clic su **Avanti**.
- 6 Se si desidera escludere utenti dal gruppo, cercare e aggiungere gli utenti nella pagina Escludi utenti dal gruppo.
- 7 Fare clic su **Avanti**.
- 8 Rivedere la configurazione del gruppo nella pagina di revisione e quindi fare clic su **Salva** per salvare e implementare le regole e la configurazione.

Risultati

Gli utenti JIT vengono aggiunti in base alle regole create.

Utilizzo della corrispondenza basata su caratteri jolly per gli utenti JIT

vRealize Automation supporta le regole di corrispondenza basate su caratteri jolly per la configurazione degli utenti JIT.

Abilitazione della corrispondenza basata su caratteri jolly

La corrispondenza basata su caratteri jolly è disabilitata per impostazione predefinita. Per abilitare la corrispondenza basata su caratteri jolly, è necessario eseguire il comando della REST API appropriato come indicato di seguito.

```
PUT:- https://{VRA_HOSTNAME}/SAAS/t/VSPHERE.LOCAL/jersey/manager/api/system/config/
isDynamicGroupWildcardEnabled
Content-Type: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Accept: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Authorization: HZN <token> (edited)
{
  "name": "isDynamicGroupWildcardEnabled",
  "values": {
    "values": [
      "true"
    ]
  }
}
```

Il token HZN da fornire all'API che abilita la configurazione con caratteri jolly deve essere riferito all'utente amministratore nel tenant vsphere.local.

Mappatura degli attributi nell'asserzione SAML agli attributi dell'utente vRealize Automation

Il nome dell'attributo nell'asserzione SAML deve coincidere completamente con il nome dell'attributo definito nella pagina Attributi utente di vRealize Automation. L'attributo SAML contenente il nome dell'utente deve essere denominato "firstName", quello contenente il cognome deve essere denominato "lastName" ecc. Se il provider di identità invia attributi dell'utente aggiuntivi che non sono definiti nella pagina Attributi utente, l'amministratore deve aggiungere tali attributi alla pagina. Ad esempio, se il provider di identità invia le informazioni sull'appartenenza al gruppo di utenti nell'attributo SAML denominato "groups" o "memberof", è necessario aggiungere gli attributi utente di vRealize Automation "groups" o "memberof". Assicurarsi di utilizzare correttamente le lettere maiuscole e minuscole nei nomi degli attributi.

Nota Per identificare positivamente una stringa come Group_Name nell'attributo a più valori che definisce l'appartenenza al gruppo di utenti, creare un carattere jolly come *Group_Name*.

Per le condizioni Corrisponde a e Non corrisponde a, è possibile utilizzare un * come carattere jolly per includere la corrispondenza dello schermo di caratteri nella regola. Ad esempio, immettendo <userinput>*Smi*</userinput>, vengono selezionati Smith, Smiley, Smirnoff e altre varianti simili, incluse quelle con "smi" al centro di un nome. Se si desidera trovare tutte le corrispondenze esatte a uno schema, aggiungere una barra rovesciata (\) prima di * quando si immette lo schermo. Ad esempio, <userinput>*Adam* </userinput> trova tutti i nomi che corrispondono esattamente allo schermo Adam*. È possibile utilizzare * in qualsiasi punto della frase, facendolo seguire e precedere da qualsiasi carattere, inclusi * & *.

Creazione di un gruppo di business

I gruppi di business vengono utilizzati per associare un set di servizi e risorse a un set di utenti. Questi gruppi spesso corrispondono a una linea di business, un reparto o altra unità organizzativa. È possibile creare un gruppo di business in modo da poter configurare prenotazioni e autorizzare utenti a eseguire il provisioning di elementi del catalogo dei servizi per i membri del gruppo di business.

Per aggiungere più utenti a un ruolo di un gruppo di business è possibile sia eseguire l'operazione più volte con singoli utenti e sia una sola volta con più utenti contemporaneamente aggiungendo un gruppo archivio identità o un gruppo personalizzato a un ruolo. Ad esempio, è possibile creare il gruppo personalizzato Team di supporto vendite e poi aggiungere questo gruppo al ruolo di supporto. Si possono anche utilizzare gruppi di utenti archivi identità esistenti. Gli utenti e i gruppi scelti devono essere validi nell'archivio identità.

Per supportare l'integrazione di vCloud Director, gli stessi membri del gruppo di business contenuti nel gruppo di business di vRealize Automation devono essere anche membri dell'organizzazione di vCloud Director.

Dopo che un amministratore tenant ha creato il gruppo di business, il manager gruppo di business ha l'autorizzazione a modificare l'indirizzo email del manager e i membri.

L'amministratore tenant può modificare tutte le opzioni.

La procedura si basa sul presupposto che IaaS sia installato e configurato.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.
- Per aggiungere macchine create da membri del gruppo di business a un'unità organizzativa Active Directory particolare, configurare il criterio di Active Directory. Vedere [Creazione di un criterio di Active Directory](#). È possibile applicare il criterio quando si crea il gruppo di business oppure aggiungerlo in un secondo momento.
- Se si desidera specificare un prefisso macchina predefinito per il gruppo da proporre ai nomi di macchina con provisioning, richiedere tale prefisso a un amministratore di struttura. Vedere [Configurazione dei prefissi macchina](#). I prefissi macchina non sono applicabili alle richieste XaaS.

Procedura

- 1 Selezionare **Amministrazione > Utenti e gruppi > Gruppi di business**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Configurare i dettagli relativi al gruppo di business.

Opzione	Descrizione
Nome	Immettere il nome per il gruppo di business.
Descrizione	Immettere la descrizione.
Invia email di avviso relative alla capacità a:	Immettere uno o più indirizzi email degli utenti che devono ricevere le notifiche degli avvisi relativi alla capacità. Gli indirizzi alias email non sono supportati. Ciascun indirizzo email deve essere associato a un utente specifico. Separare più voci con una virgola. Ad esempio JoeAdmin@mycompany.com,WeiMgr@mycompany.com.
Criterio di Active Directory	Selezionare il criterio di Active Directory predefinito per il gruppo di business.

- 4 Aggiungere proprietà personalizzate.
- 5 Fare clic su **Avanti** per passare alla pagina Membri.
- 6 Immettere un nome utente o il nome del gruppo di utenti personalizzato e premere Invio.

Al gruppo di business è possibile aggiungere uno o più individui o gruppi di utenti personalizzati. È possibile specificare gli utenti adesso oppure creare gruppi di business vuoti da popolare in un secondo momento.

Opzione	Descrizione
Ruolo manager gruppo	Può creare permessi e assegnare criteri di approvazione per il gruppo.
Ruolo di supporto	Può richiedere e gestire elementi del catalogo dei servizi per conto degli altri membri del gruppo di business.

Opzione	Descrizione
Ruolo accesso condiviso	Può utilizzare ed eseguire azioni sulle risorse che vengono distribuite da altri membri del gruppo di business.
Ruolo utente	Può richiedere elementi del catalogo dei servizi per cui è autorizzato.

7 Fare clic su **Avanti** per passare alla pagina Infrastruttura.

8 Configurare le opzioni dell'infrastruttura predefinita.

Opzione	Descrizione
Prefisso macchina predefinito	<p>Selezionare un prefisso macchina preconfigurato per il gruppo di business. Il prefisso è utilizzato dai blueprint delle macchine. Se il blueprint utilizza il prefisso predefinito ma questo non viene specificato, viene creato un prefisso macchina basato sul nome del gruppo di business. La procedura consigliata consiste nel fornire un prefisso predefinito. È sempre possibile configurare i blueprint con prefissi specifici o consentire agli utenti del catalogo dei servizi di sovrascrivere quello predefinito quando richiedono un blueprint.</p> <p>I blueprint di XaaS non utilizzano prefissi macchina predefiniti. Se si configura un prefisso in questo campo e si autorizza un blueprint di XaaS per questo gruppo di business, esso non influirà sul provisioning di una macchina XaaS.</p>
Contenitore Active Directory	<p>Immettere un contenitore Active Directory. Questa opzione si applica solo al provisioning WIM.</p> <p>Altri metodi di provisioning richiedono una configurazione aggiuntiva necessaria per unire le macchine di cui viene eseguito il provisioning a un contenitore Active Directory.</p>

9 Fare clic su **Fine**.

Risultati

Gli amministratori tenant possono allocare risorse al gruppo di business creando una prenotazione. I manager dei gruppi di business possono creare permessi per i membri del gruppo di business.

Operazioni successive

- Creare una prenotazione per il gruppo di business in base a dove esso esegue il provisioning delle macchine. Vedere [Scelta di uno scenario di prenotazione](#).
- Se gli elementi del catalogo sono pubblicati e i servizi esistono, è possibile creare un permesso per i membri del gruppo di business. Vedere [Autorizzazione degli utenti per servizi, elementi di catalogo e azioni](#).

Risoluzione dei problemi relativi alle prestazioni durante la visualizzazione dei membri di un gruppo

La visualizzazione dei dettagli di un gruppo da parte dei membri del gruppo di business o del gruppo personalizzato è particolarmente lenta.

Problema

Quando si visualizzano informazioni sugli utenti in ambienti con un gran numero di utenti, il caricamento dei nomi degli utenti nell'interfaccia è particolarmente lento.

Causa

La maggiore lentezza necessaria per caricare i nomi si verifica in ambienti in cui Active Directory contiene un gran numero di elementi.

Soluzione

- ◆ Per ridurre il carico di lavoro nel recupero dei dati, utilizzare ogni volta che è possibile gruppi personalizzati o gruppi di Active Directory invece di aggiungere centinaia di membri singoli per nome.

Risoluzione dei problemi relativi alle voci impreviste per il filtro

L'elenco dei gruppi di business utilizzato per effettuare selezioni di filtro include voci impreviste o duplicate.

Problema

Sono state apportate modifiche ai gruppi di business in **Amministrazione > Utenti e gruppi > Gruppi di business**. Nella pagina Distribuzioni, quando si tenta di filtrare le distribuzioni in base al gruppo di business, l'elenco dei gruppi di business disponibili da filtrare non riflette le modifiche o include risultati imprevisti, ad esempio gruppi di business duplicati.

Causa

Il sistema esegue il polling delle modifiche solo una volta ogni 30 minuti.

Soluzione

Attendere 30 minuti e aggiornare l'elenco di gruppi di business per la selezione del filtro aggiornando il browser.

Creazione di tenant aggiuntivi

Un amministratore di sistema può creare tenant di vRealize Automation aggiuntivi in modo che gli utenti possano accedere alle applicazioni e alle risorse appropriate di cui necessitano per completare le assegnazioni di lavoro.

Un tenant è un gruppo di utenti con privilegi specifici che lavorano nell'ambito di un'istanza software. Generalmente, durante l'installazione del sistema e la configurazione iniziale viene creato un tenant di vRealize Automation predefinito. Successivamente gli amministratori possono creare tenant aggiuntivi a cui gli utenti possono accedere per completare le proprie assegnazioni di lavoro. Gli amministratori possono creare tutti i tenant necessari per garantire l'operatività del sistema. Quando creano tenant, gli amministratori devono specificare la configurazione di base comprensiva di nome, URL di accesso, utenti locali e amministratori. Dopo aver configurato le

informazioni di base del tenant, l'amministratore tenant deve accedere e configurare una connessione Active Directory valida utilizzando la funzionalità Gestione directory disponibile nella scheda di amministrazione della console di vRealize Automation. Gli amministratori tenant possono anche applicare un branding personalizzato ai tenant.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore di sistema**.

Procedura

1 (Facoltativo) Definizione delle informazioni sui tenant

Le prime operazioni da compiere nella configurazione di un tenant sono assegnare un nome al nuovo tenant, aggiungerlo a vRealize Automation e creare l'URL di accesso specifico del tenant.

2 (Facoltativo) Configurazione di utenti locali

L'amministratore di sistema di vRealize Automation deve configurare utenti locali per ciascun tenant applicabile.

3 (Facoltativo) Nomina degli amministratori

È possibile nominare uno o più amministratori tenant e amministratori IaaS dagli archivi identità configurati per un tenant.

Definizione delle informazioni sui tenant

Le prime operazioni da compiere nella configurazione di un tenant sono assegnare un nome al nuovo tenant, aggiungerlo a vRealize Automation e creare l'URL di accesso specifico del tenant.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore di sistema**.

Procedura

1 Selezionare **Amministrazione > Tenant**.

2 Fare clic sull'icona **Nuovo** (+).

3 Immettere un nome nella casella di testo **Nome**.

4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.

5 Inserire un identificatore univoco per il tenant nella casella di testo **Nome URL**.

Questo token URL è utilizzato per apporre un identificatore specifico del tenant all'URL della console di vRealize Automation.

Inserire ad esempio **mytenant** per creare l'URL `https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant`.

Nota L'URL del tenant deve essere indicato con caratteri minuscoli solo in vRealize Automation 7.0 e 7.1.

6 (Facoltativo) Inserire un indirizzo email nella casella di testo **Email di contatto**.

7 Fare clic su **Invia e Avanti**.

Configurazione di utenti locali

L'amministratore di sistema di vRealize Automation deve configurare utenti locali per ciascun tenant applicabile.

Dopo che un amministratore ha creato le informazioni generali per un tenant, la scheda Utenti locali diventa attiva e l'amministratore può stabilire quali utenti potranno accedere al tenant. Quando la configurazione del tenant è completa, gli utenti dei tenant locali potranno accedere ai rispettivi tenant per completare le assegnazioni dei lavori.

Nota Dopo aver aggiunto un utente, non è possibile cambiarne la configurazione. Per cambiare qualsiasi aspetto della configurazione di un utente, è necessario eliminare l'utente e ricrearlo.

Procedura

- 1** Fare clic sul pulsante **Aggiungi** nella scheda Utenti locali.
- 2** Specificare nome e cognome degli utenti nei campi **Nome** e **Cognome** della finestra di dialogo Dettagli utente.
- 3** Immettere l'indirizzo email dell'utente nel campo **Email**.
- 4** Immettere ID e password dell'utente nei campi **Nome utente** e **Password**.
- 5** Fare clic sul pulsante **Aggiungi**.
- 6** Ripetere la procedura per tutti gli utenti locali del tenant.

Risultati

Gli utenti locali specificati per il tenant vengono creati.

Nomina degli amministratori

È possibile nominare uno o più amministratori tenant e amministratori IaaS dagli archivi identità configurati per un tenant.

Gli amministratori tenant sono responsabili della configurazione del branding specifico del tenant, nonché della gestione di archivi identità, archivi, utenti, gruppi, permessi e blueprint condivisi nell'ambito del contesto del proprio tenant. Gli amministratori IaaS sono responsabili della configurazione degli endpoint delle origini delle infrastrutture in IaaS, della nomina degli amministratori di struttura e del monitoraggio dei registri di IaaS.

Prerequisiti

- Prima di nominare amministratori IaaS è necessario installare IaaS. Per ulteriori informazioni sull'installazione di IaaS, vedere *Installazione di vRealize Automation*.

Procedura

- 1 Inserire il nome di un utente o di un gruppo nella casella di ricerca **Amministratori tenant** e premere Invio.

Per risultati più veloci, inserire il nome intero dell'utente o del gruppo, ad esempio myAdmins@mycompany.domain. Ripetere questo passaggio per designare amministratori tenant aggiuntivi.

- 2 Se è installato IaaS, inserire il nome di un utente o di un gruppo nella casella di ricerca **Amministratori IaaS** e premere Invio.

Per risultati più veloci, inserire il nome intero dell'utente o del gruppo, ad esempio IaaSAdmins@mycompany.domain. Ripetere questo passaggio per designare amministratori di infrastruttura aggiuntivi.

- 3 Fare clic su **Aggiungi**.

Eliminazione di un tenant

Un amministratore di sistema può eliminare qualsiasi tenant non desiderato da vRealize Automation.

Se si elimina un tenant, questo verrà rimosso immediatamente dall'interfaccia di vRealize Automation, tuttavia potrebbero trascorrere diverse ore prima che il tenant venga rimosso completamente dalla distribuzione. Se si elimina un tenant e si desidera crearne un altro con lo stesso URL, attendere diverse ore prima di creare il nuovo tenant, per far sì che l'eliminazione di quello precedente venga portata a termine.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore di sistema**.

Procedura

- 1 Selezionare **Amministrazione > Tenant**.

- 2 Selezionare il tenant che si desidera eliminare.

Non fare clic sul nome effettivo per selezionare il tenant, poiché verrebbe aperto per la modifica.

- 3 Fare clic su **Elimina**.

Risultati

Il tenant viene eliminato dalla distribuzione di vRealize Automation.

Configurazione delle impostazioni di sicurezza per il multi-tenancy

È possibile controllare la disponibilità di oggetti di sicurezza NSX tra tenant in un ambiente multi-tenant.

Quando si crea un oggetto di sicurezza NSX, la sua disponibilità predefinita può essere globale, il che significa che l'oggetto è disponibile in tutti i tenant per cui l'endpoint associato ha una prenotazione, oppure nascosta per tutti gli utenti ad eccezione dell'amministratore.

La disponibilità degli oggetti di sicurezza in un tenant dipende dal fatto che l'endpoint associato disponga o meno di una prenotazione o di un criterio di prenotazione nel tenant.

L'argomento correlato [Controllo dell'accesso al tenant per gli oggetti di sicurezza in vRealize Automation](#) illustra i mezzi tramite i quali controllare la disponibilità di nuovi oggetti di sicurezza tra tenant e il comportamento degli oggetti di sicurezza esistenti, relativi alla cross-tenancy, dopo l'aggiornamento a questa versione di vRealize Automation.

Configurazione del branding personalizzato

vRealize Automation consente di applicare un branding personalizzato alle pagine di accesso e delle applicazioni del tenant.

Un branding personalizzato può comprendere testo e colori di sfondo, logo dell'azienda, nome dell'azienda, informative sulla privacy, note sul copyright e altre informazioni importanti che si desidera visualizzare sulle pagine di accesso e delle applicazioni del tenant.

Branding personalizzato per la pagina di accesso del tenant

Utilizzare la pagina Branding schermata di accesso per applicare un branding personalizzato alle pagine di accesso ai tenant di vRealize Automation.

È possibile utilizzare il branding di vRealize Automation predefinito nelle pagine di accesso al tenant oppure configurare un branding personalizzato operando dalla pagina Branding schermata di accesso. Il branding personalizzato si applica allo stesso modo in tutte le applicazioni del tenant.

Da questa pagina è possibile configurare il branding di tutte le pagine di accesso al tenant.

La pagina Branding schermata di accesso visualizza il branding di accesso correntemente implementato nel riquadro di anteprima.

Nota Dopo aver salvato il nuovo branding della pagina di accesso al tenant, può verificarsi un ritardo di un massimo di cinque minuti prima che diventi visibile in tutte le pagine di accesso.

Prerequisiti

Per utilizzare un logo personalizzato o un'altra immagine per il branding, è necessario avere a disposizione i file appropriati.

Procedura

- 1 Accedere a vRealize Automation come amministratore di sistema o tenant.
- 2 Fare clic sulla scheda **Amministrazione**.
- 3 Selezionare **Branding > Branding schermata di accesso**.

- 4 Per aggiungere un'immagine logo, fare clic su **Carica** sotto il campo Logo, individuare la cartella in cui si trova il file immagine del logo e selezionarlo.
- 5 Per aggiungere un'ulteriore immagine, fare clic su **Carica** sotto il campo Immagine (facoltativo), individuare la cartella in cui si trova il file immagine aggiuntivo e selezionarlo.
- 6 Per personalizzare i colori di sfondo, immettere i codici esadecimali corrispondenti nei campi **Colore sfondo**, **Colore titolo**, **Colore sfondo pulsante di accesso** e **Colore primo piano pulsante di accesso**.

Se necessario, cercare su Internet un elenco dei codici esadecimali dei colori.

- 7 Fare clic su **Salva** per applicare le impostazioni.

Risultati

Gli utenti del tenant vedranno il branding personalizzato nelle loro pagine di accesso.

Branding personalizzato per le applicazioni del tenant

Utilizzare la pagina Branding applicazione per applicare un branding personalizzato alle applicazioni del tenant di vRealize Automation.

È possibile utilizzare il branding di vRealize Automation predefinito nelle applicazioni degli utenti oppure configurare un branding personalizzato operando dalla pagina Branding applicazione. Da questa pagina è possibile configurare il branding nelle sezioni dell'intestazione e del piè di pagina nelle schermate dell'applicazione. Il branding personalizzato si applica allo stesso modo in tutte le applicazioni utente.

La pagina Branding applicazione visualizza il branding di intestazione e piè di pagina correntemente implementato nella parte inferiore della pagina.

Prerequisiti

Per utilizzare un logo personalizzato per il proprio branding, è necessario avere a disposizione il file immagine del logo.

Procedura

- 1 Accedere a vRealize Automation come amministratore di sistema o tenant.
- 2 Fare clic sulla scheda **Amministrazione**.
- 3 Selezionare **Branding > Branding applicazione**
- 4 Fare clic sulla scheda **Intestazione** se non già attiva.
- 5 Per utilizzare il branding di vRealize Automation predefinito, fare clic sulla casella di controllo **Utilizza predefinito**.

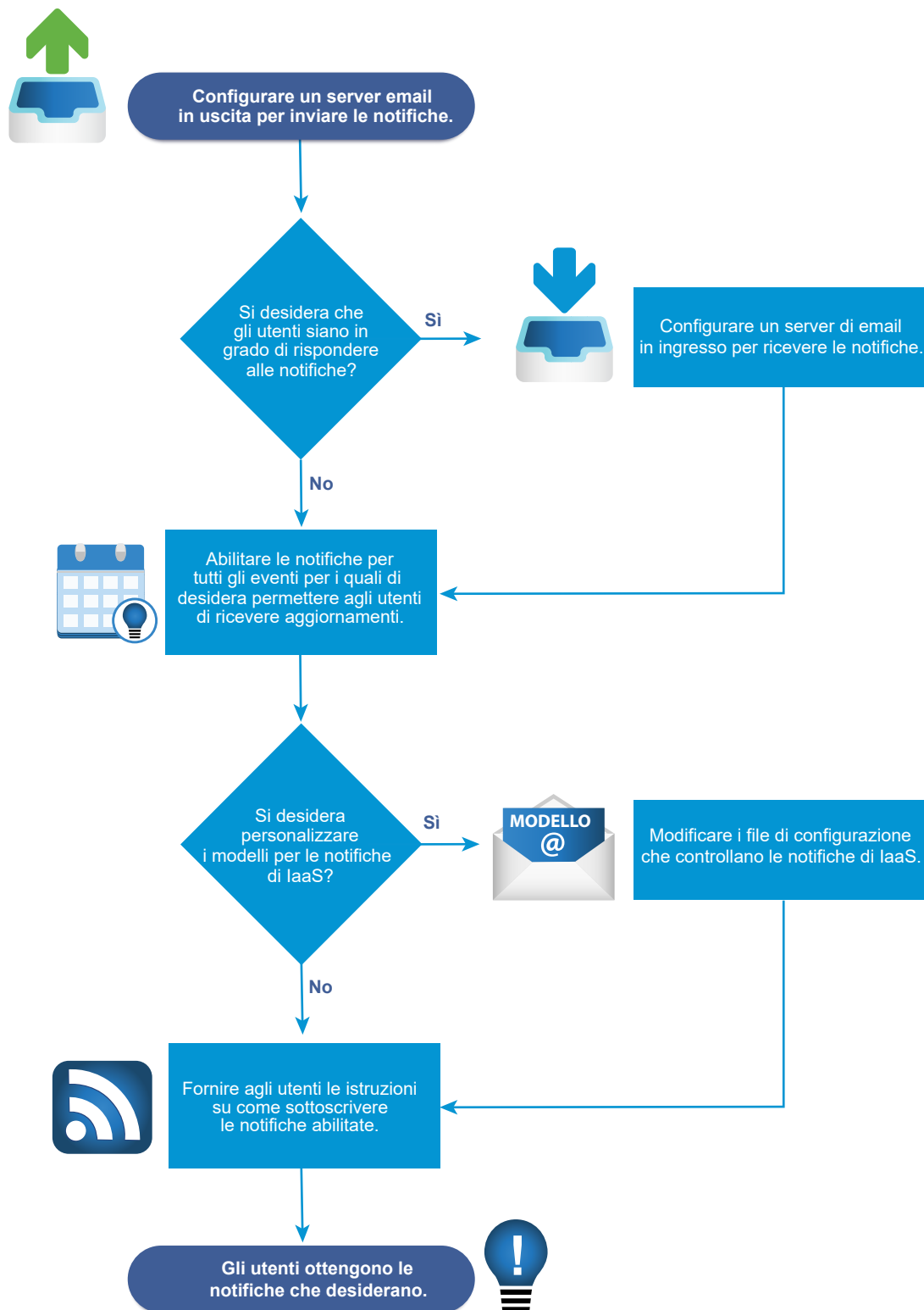
- 6 Per implementare il branding personalizzato, fare le opportune selezioni nei campi contenuti nelle schede **Intestazione** e **Piè di pagina**.
 - a Fare clic sul pulsante **Sfoglia** nel campo **Logo dell'intestazione**, individuare la cartella in cui si trova il file immagine del logo e selezionare il file.
 - b Immettere il nome dell'azienda nel campo **Nome azienda**.
Il nome specificato in questo campo viene visualizzato quando si passa il cursore del mouse sul logo.
 - c Immettere un nome appropriato nel campo **Nome prodotto**.
Il nome specificato in questo campo viene visualizzato nell'intestazione dell'applicazione accanto al logo.
 - d Specificare nel campo **Colore in formato esadecimale dello sfondo** il codice esadecimale del colore desiderato per lo sfondo del perimetro dell'applicazione.
Se necessario, cercare su Internet un elenco dei codici esadecimali dei colori.
 - e Specificare il codice esadecimale del colore del testo nel campo **Colore in formato esadecimale del testo**.
Se necessario, cercare su Internet un elenco dei codici esadecimali dei colori per il testo.
 - f Fare clic su **Avanti** per passare alla scheda Piè di pagina.
 - g Immettere il testo desiderato nel campo **Informazioni sul copyright**.
 - h Specificare il link all'informativa sulla privacy dell'azienda nel campo **Collegamento all'informativa sulla privacy**.
 - i Immettere nel campo **Collegamento ai contatti** le informazioni di contatto dell'azienda che si desidera mostrare.
- 7 Fare clic su **Aggiorna** per implementare la configurazione del branding.

Risultati

Gli utenti del tenant vedranno il branding personalizzato nelle loro pagine dell'applicazione.

Elenco di controllo per la configurazione delle notifiche

È possibile configurare vRealize Automation per inviare notifiche agli utenti quando si verificano eventi specifici. Gli utenti possono scegliere quali notifiche sottoscrivere, ma possono selezionare solo gli eventi volutamente abilitati come elementi scatenanti delle notifiche.



L'elenco di controllo per la configurazione delle notifiche è una panoramica ad alto livello della sequenza di passaggi necessari per configurare le notifiche e contiene i collegamenti ai punti di decisione e alle istruzioni dettagliate per ogni passaggio.

Tabella 2-10. Elenco di controllo per la configurazione delle notifiche

Attività	Ruolo richiesto	Dettagli
<input type="checkbox"/> Configurare un server email in uscita per inviare le notifiche.	<ul style="list-style-type: none"> ■ Gli amministratori di sistema possono configurare server globali predefiniti. ■ Gli amministratori tenant possono configurare server per i propri tenant. 	<p>Per configurare per la prima volta un server per il proprio tenant, vedere Aggiunta di un server email in uscita specifico di un tenant. Se occorre utilizzare un server diverso da quello globale predefinito, vedere Priorità inferiore del server di email in uscita predefinito di un sistema. Per configurare server predefiniti globali per tutti i tenant, vedere Creazione di un server email in uscita globale.</p>
<input type="checkbox"/> (Facoltativo) Configurare un server email in entrata che consenta agli utenti di completare delle attività rispondendo alle notifiche.	<ul style="list-style-type: none"> ■ Gli amministratori di sistema possono configurare server globali predefiniti. ■ Gli amministratori tenant possono configurare server per i propri tenant. 	<p>Per configurare per la prima volta un server per il proprio tenant, vedere Aggiunta di un server email in entrata specifico di un tenant. Se occorre utilizzare un server diverso da quello globale predefinito, vedere Priorità inferiore del server di email in entrata predefinito di un sistema. Per configurare un server predefinito globale per tutti i tenant, vedere Creazione di un server email in entrata globale.</p>
<input type="checkbox"/> (Facoltativo) Specificare quando inviare una notifica via email prima della data di scadenza di una macchina.	Amministratore di sistema	Vedere Personalizzazione della data per la notifica via email della scadenza di una macchina .
<input type="checkbox"/> Selezionare gli eventi di vRealize Automation che fanno scattare le notifiche agli utenti. Gli utenti possono sottoscrivere solo le notifiche relative agli eventi volutamente abilitati come elementi scatenanti delle notifiche.	Amministratore tenant	Vedere Configurazione delle notifiche .

Tabella 2-10. Elenco di controllo per la configurazione delle notifiche (continua)

Attività	Ruolo richiesto	Dettagli
<input type="checkbox"/> (Facoltativo) Configurare i modelli delle notifiche da inviare ai proprietari delle macchine e che riguardano gli eventi che coinvolgono le loro macchine, come ad esempio la scadenza del lease.	Chiunque abbia accesso alla directory \Templates sotto la directory d'installazione del server di vRealize Automation (generalmente %SystemDrive%\Programmi (x86)\VMware\VCAC\Server) può configurare i modelli di queste notifiche via email.	Vedere Configurazione dei modelli per le email automatiche di IaaS .
<input type="checkbox"/> Gli utenti vengono automaticamente registrati per le notifiche configurate. Se necessario, è possibile fornire agli utenti le istruzioni su come sottoscrivere le notifiche abilitate per loro. Gli utenti potranno scegliere di sottoscrivere solo le notifiche rilevanti per i propri ruoli.	Tutti gli utenti	Vedere Iscrizione alle notifiche .

Configurazione di server email globali per le notifiche

Quando configurano le notifiche per i propri tenant, gli amministratori tenant possono aggiungere server email. Un amministratore tenant può impostare server email in entrata e in uscita globali che appariranno in tutti i tenant come server predefiniti di sistema. Se gli amministratori tenant non sovrascrivono queste impostazioni prima di attivare le notifiche, vRealize Automation utilizzerà i server email configurati globalmente.

Creazione di un server email in entrata globale

Gli amministratori di sistema possono creare un server email in entrata per gestire le notifiche via email in arrivo, come le risposte alle approvazioni. È possibile creare un solo server in entrata, che apparirà a tutti i tenant come il server predefinito. Se gli amministratori tenant non sovrascrivono queste impostazioni prima di attivare le notifiche, vRealize Automation utilizzerà il server email configurato globalmente.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore di sistema**.

Procedura

- 1 Selezionare **Amministrazione > Server email**.
- 2 Fare clic sull'icona **Aggiungi** (+).

- 3 Selezionare **Email - In entrata**.
- 4 Fare clic su **OK**.
- 5 Immettere un nome nella casella di testo **Nome**.
- 6 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 7 (Facoltativo) Selezionare la casella di controllo **SSL** per utilizzare il protocollo SSL e garantire così la sicurezza.
- 8 Selezionare il protocollo del server.
- 9 Immettere il nome del server nella casella di testo **Nome server**.
- 10 Immettere il numero della porta server nella casella di testo **Porta server**.
- 11 Immettere il nome della cartella per le email nella casella di testo **Nome cartella**.
Questa opzione è obbligatoria solo se si sceglie il protocollo server IMAP.
- 12 Immettere un nome utente nella casella di testo **Nome utente**.
- 13 Immettere una password nella casella di testo **Password**.
- 14 Immettere l'indirizzo email a cui gli utenti di vRealize Automation possono rispondere nella casella di testo **Indirizzo email**.
- 15 (Facoltativo) Selezionare **Elimina dal server** per eliminare dal server tutte le email elaborate che sono state recuperate dal servizio di notifica.
- 16 Scegliere se vRealize Automation può accettare certificati autofirmati dal server email.
- 17 Fare clic su **Prova connessione**.
- 18 Fare clic su **Aggiungi**.

Creazione di un server email in uscita globale

Gli amministratori di sistema possono creare un server email in uscita per gestire le notifiche via email in uscita. È possibile creare un solo server in uscita, che apparirà a tutti i tenant come il server predefinito. Se gli amministratori tenant non sovrascrivono queste impostazioni prima di attivare le notifiche, vRealize Automation utilizzerà il server email configurato globalmente.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore di sistema**.

Procedura

- 1 Selezionare **Amministrazione > Server email**.
- 2 Fare clic sull'icona **Aggiungi** (+).
- 3 Selezionare **Email - In uscita**.
- 4 Fare clic su **OK**.

- 5 Immettere un nome nella casella di testo **Nome**.
- 6 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 7 Immettere il nome del server nella casella di testo **Nome server**.
- 8 Selezionare un metodo di crittografia.
 - Fare clic su **Usa SSL**.
 - Fare clic su **Usa TLS**.
 - Fare clic su **Nessuno** per inviare comunicazioni non crittografate.
- 9 Immettere il numero della porta server nella casella di testo **Porta server**.
- 10 (Facoltativo) Selezionare la casella di controllo **Obbligatorio** se il server richiede l'autenticazione.
 - a Immettere un nome utente nella casella di testo **Nome utente**.
 - b Immettere una password nella casella di testo **Password**.
- 11 Immettere casella di testo **Indirizzo mittente** l'indirizzo email mostrato nelle email di vRealize Automation come indirizzo mittente.

Questo indirizzo email corrisponde al nome utente e alla password forniti.
- 12 Scegliere se vRealize Automation può accettare certificati autofirmati dal server email.
- 13 Fare clic su **Prova connessione**.
- 14 Fare clic su **Aggiungi**.

Aggiunta di un server email in uscita specifico di un tenant

Gli amministratori tenant possono aggiungere un server email in uscita che consenta di inviare notifiche relative al completamento degli elementi di lavoro, come ad esempio le approvazioni.

Ogni tenant può avere un solo server email in uscita. Se l'amministratore di sistema ha già configurato un server email in uscita globale, vedere [Priorità inferiore del server di email in uscita predefinito di un sistema](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.
- Se il server email richiede autenticazione, l'utente specificato deve trovarsi in un archivio identità e nel gruppo di business.

Procedura

- 1 Selezionare **Amministrazione > Notifiche > Server email**.
- 2 Fare clic sull'icona **Aggiungi** (+).
- 3 Selezionare **Email - In uscita**.

- 4 Fare clic su **OK**.
- 5 Immettere un nome nella casella di testo **Nome**.
- 6 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 7 Immettere il nome del server nella casella di testo **Nome server**.
- 8 Selezionare un metodo di crittografia.
 - Fare clic su **Usa SSL**.
 - Fare clic su **Usa TLS**.
 - Fare clic su **Nessuno** per inviare comunicazioni non crittografate.
- 9 Immettere il numero della porta server nella casella di testo **Porta server**.
- 10 (Facoltativo) Selezionare la casella di controllo **Obbligatorio** se il server richiede l'autenticazione.
 - a Immettere un nome utente nella casella di testo **Nome utente**.
 - b Immettere una password nella casella di testo **Password**.
- 11 Immettere casella di testo **Indirizzo mittente** l'indirizzo email mostrato nelle email di vRealize Automation come indirizzo mittente.
Questo indirizzo email corrisponde al nome utente e alla password forniti.
- 12 Scegliere se vRealize Automation può accettare certificati autofirmati dal server email.
Questa opzione è disponibile solo se è stata abilitata la crittografia.
 - Fare clic su **Sì** per accettare certificati autofirmati.
 - Fare clic su **No** per rifiutare i certificati autofirmati.
- 13 Fare clic su **Prova connessione**.
- 14 Fare clic su **Aggiungi**.

Aggiunta di un server email in entrata specifico di un tenant

Gli amministratori tenant possono aggiungere un server email in entrata che consenta agli utenti di rispondere alle notifiche di completamento degli elementi di lavoro, come ad esempio le approvazioni.

Ogni tenant può avere un solo server email in entrata. Se l'amministratore di sistema ha già configurato un server email in entrata globale, vedere [Priorità inferiore del server di email in entrata predefinito di un sistema](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.
- Verificare che l'utente specificato sia presente in un archivio identità e nel gruppo di business.

Procedura

- 1 Selezionare **Amministrazione > Notifiche > Server email**.
- 2 Fare clic sull'icona **Aggiungi** (+).
- 3 Selezionare **Email - In entrata** e fare clic su **OK**.
- 4 Configurare le seguenti opzioni per il server email in entrata.

Opzione	Azione
Nome	Immettere un nome per il server email in entrata.
Descrizione	Immettere una descrizione per il server email in entrata.
Sicurezza	Selezionare la casella di controllo Usa SSL .
Protocollo	Selezionare il protocollo del server.
Nome server	Specificare il nome del server.
Porta server	Specificare il numero di porta del server.

- 5 Immettere il nome della cartella per le email nella casella di testo **Nome cartella**.
Questa opzione è obbligatoria solo se si sceglie il protocollo server IMAP.
- 6 Immettere un nome utente nella casella di testo **Nome utente**.
- 7 Immettere una password nella casella di testo **Password**.
- 8 Immettere l'indirizzo email a cui gli utenti di vRealize Automation possono rispondere nella casella di testo **Indirizzo email**.
- 9 (Facoltativo) Selezionare **Elimina dal server** per eliminare dal server tutte le email elaborate che sono state recuperate dal servizio di notifica.
- 10 Scegliere se vRealize Automation può accettare certificati autofirmati dal server email.
Questa opzione è disponibile solo se è stata abilitata la crittografia.
 - Fare clic su **Sì** per accettare certificati autofirmati.
 - Fare clic su **No** per rifiutare i certificati autofirmati.
- 11 Fare clic su **Prova connessione**.
- 12 Fare clic su **Aggiungi**.

Priorità inferiore del server di email in uscita predefinito di un sistema

Se l'amministratore di sistema ha configurato un server email di uscita predefinito per il sistema, l'amministratore tenant può sovrascrivere questa impostazione globale.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Notifiche > Server email**.
- 2 Selezionare il server di email di uscita.
- 3 Fare clic su **Sovrascrivi Globale**.
- 4 Immettere un nome nella casella di testo **Nome**.
- 5 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 6 Immettere il nome del server nella casella di testo **Nome server**.
- 7 Selezionare un metodo di crittografia.
 - Fare clic su **Usa SSL**.
 - Fare clic su **Usa TLS**.
 - Fare clic su **Nessuno** per inviare comunicazioni non crittografate.
- 8 Immettere il numero della porta server nella casella di testo **Porta server**.
- 9 (Facoltativo) Selezionare la casella di controllo **Obbligatorio** se il server richiede l'autenticazione.
 - a Immettere un nome utente nella casella di testo **Nome utente**.
 - b Immettere una password nella casella di testo **Password**.
- 10 Immettere casella di testo **Indirizzo mittente** l'indirizzo email mostrato nelle email di vRealize Automation come indirizzo mittente.
Questo indirizzo email corrisponde al nome utente e alla password forniti.
- 11 Scegliere se vRealize Automation può accettare certificati autofirmati dal server email.
Questa opzione è disponibile solo se è stata abilitata la crittografia.
 - Fare clic su **Sì** per accettare certificati autofirmati.
 - Fare clic su **No** per rifiutare i certificati autofirmati.
- 12 Fare clic su **Prova connessione**.
- 13 Fare clic su **Aggiungi**.

Priorità inferiore del server di email in entrata predefinito di un sistema

Se l'amministratore di sistema ha configurato un server email in entrata predefinito per il sistema, gli amministratori tenant possono sovrascrivere questa impostazione globale.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Notifiche > Server email**.

- 2 Selezionare il server di email in entrata nella tabella Server email.
- 3 Fare clic su **Sovrascrivi Globale**.
- 4 Inserire le seguenti opzioni per il server email in entrata.

Opzione	Azione
Nome	Specificare il nome del server email in entrata.
Descrizione	Immettere una descrizione per il server email in entrata.
Sicurezza	Selezionare la casella di controllo SSL per utilizzare il protocollo SSL e garantire così la sicurezza.
Protocollo	Selezionare il protocollo del server.
Nome server	Specificare il nome del server.
Porta server	Specificare il numero di porta del server.

- 5 Immettere il nome della cartella per le email nella casella di testo **Nome cartella**.
Questa opzione è obbligatoria solo se si sceglie il protocollo server IMAP.
- 6 Immettere un nome utente nella casella di testo **Nome utente**.
- 7 Immettere una password nella casella di testo **Password**.
- 8 Immettere l'indirizzo email a cui gli utenti di vRealize Automation possono rispondere nella casella di testo **Indirizzo email**.
- 9 (Facoltativo) Selezionare **Elimina dal server** per eliminare dal server tutte le email elaborate che sono state recuperate dal servizio di notifica.
- 10 Scegliere se vRealize Automation può accettare certificati autofirmati dal server email.
Questa opzione è disponibile solo se è stata abilitata la crittografia.
 - Fare clic su **Sì** per accettare certificati autofirmati.
 - Fare clic su **No** per rifiutare i certificati autofirmati.
- 11 Fare clic su **Prova connessione**.
- 12 Fare clic su **Aggiungi**.

Ripristino dei server email predefiniti del sistema

Gli amministratori tenant che sovrascrivono i server predefiniti di sistema possono riportare nuovamente le impostazioni alle impostazioni globali.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Notifiche > Server email**.

- 2 Selezionare il server email da ripristinare.
- 3 Fare clic su **Ripristina Globale**.
- 4 Fare clic su **Sì**.

Configurazione delle notifiche

Ogni utente sceglie se ricevere notifiche, ma sono gli amministratori tenant a determinare quali sono gli eventi che generano notifiche.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.
- Verificare che un amministratore tenant o un amministratore di sistema abbia configurato un server email in uscita. Vedere [Aggiunta di un server email in uscita specifico di un tenant](#).

Procedura

- 1 Selezionare **Amministrazione > Notifiche > Scenari**.
- 2 Selezionare una o più notifiche.
- 3 Fare clic su **Attiva**.

Risultati

Da questo momento le notifiche saranno ricevute dagli utenti che si iscriveranno alle notifiche nelle impostazioni delle proprie preferenze.

Personalizzazione della data per la notifica via email della scadenza di una macchina

È possibile specificare quando inviare una notifica via email prima della data di scadenza di una macchina.

L'impostazione che definisce quanti giorni prima della data di scadenza di una macchina vRealize Automation invierà una notifica via email può essere modificata. L'email informa gli utenti della data di scadenza di una macchina. Il valore predefinito dell'impostazione è 7 giorni prima della scadenza della macchina.

Procedura

- 1 Accedere al server vRealize Automation utilizzando credenziali con accesso amministrativo.
- 2 Aprire il file `/etc/vcac/setenv-user`.
- 3 Aggiungere la riga indicata di seguito per specificare il numero di giorni precedenti alla data di scadenza di una macchina. In questo esempio il numero 3 corrisponde a 3 giorni prima della data di scadenza.

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 Riavviare i servizi vCAC sull'appliance virtuale mediante l'esecuzione del comando indicato di seguito:

```
service vcac-server restart
```

Operazioni successive

Se si opera in un ambiente a disponibilità elevata, ripetere questa procedura per tutte le appliance virtuali presenti nell'ambiente HA (High Availability).

Configurazione dei modelli per le email automatiche di IaaS

È possibile configurare le email di notifica da inviare ai proprietari delle macchine su vari eventi di vRealize Automation che coinvolgono le loro macchine.

Tra gli eventi che attivano l'invio delle notifiche vi sono, ad esempio, la scadenza o l'avvicinarsi della scadenza di periodi di archiviazione e lease delle macchine virtuali.

Per ulteriori informazioni sulla configurazione e sull'abilitazione o disabilitazione delle notifiche via email di vRealize Automation, consultare i seguenti articoli del blog e della Knowledge Base:

- [Personalizzazione dell'email in vRealize automation](#)
- [Personalizzazione dei modelli di email in vRealize Automation \(2088805\)](#)
- [Esempi di personalizzazione dei modelli di email in vRealize Automation \(2102019\)](#)

Iscrizione alle notifiche

Se gli amministratori hanno configurato notifiche, si viene iscritti automaticamente. Gli eventi notificati possono includere il corretto completamento di una richiesta di catalogo o di un'approvazione richiesta.

Se l'iscrizione deve essere effettuata manualmente, è possibile abilitare le notifiche.

Prerequisiti

Accedere a vRealize Automation.

Procedura

- 1 Fare clic su **Preferenze**.
- 2 Selezionare la casella di controllo **Attivato** per il protocollo Email nella tabella Notifiche.
- 3 Fare clic su **Applica**.
- 4 Fare clic su **Chiudi**.

Creazione di un file RDP personalizzato per il supporto di connessioni RDP per le macchine di cui è stato eseguito il provisioning

Un amministratore di sistema crea un file di protocollo di desktop remoto personalizzato che verrà utilizzato dagli architetti IaaS nei blueprint per configurare le impostazioni RDP. Dopo aver creato il file RDP, si fornisce agli architetti il nome e il percorso completo del file in modo che possano includerlo nei blueprint. Un amministratore del catalogo autorizza quindi gli utenti ad eseguire l'azione RDP.

Nota se si utilizza Internet Explorer con la configurazione di sicurezza avanzata abilitata, non è possibile scaricare i file `.rdp`.

Prerequisiti

Accedere al servizio di gestione IaaS come amministratore.

Procedura

- 1 Impostare la directory corrente su `<vRA_installation_dir>\Rdp`.
- 2 Copiare il file `Default.rdp` e rinominarlo `Console.rdp` nella stessa directory.
- 3 Aprire il file `Console.rdp` in un editor.
- 4 Aggiungere al file le impostazioni RDP.
Ad esempio, **connect to console:i:1**.
- 5 Se si lavora in un ambiente distribuito, accedere come utente con privilegi di amministratore alla macchina host IaaS su cui è installato il componente sito Web del Model Manager.
- 6 Copiare il file `Console.rdp` nella directory `vRA_installation_dir\Server\Website\Rdp`.
- 7 Aggiungere la proprietà personalizzata `VirtualMachine.Rdp.File` a un blueprint.

Gli architetti IaaS possono aggiungere le proprietà RDP personalizzate ai blueprint di macchine Windows e gli amministratori del catalogo possono quindi autorizzare gli utenti ad eseguire l'azione Connetti con RDP. Vedere [Aggiunta del supporto delle connessioni RDP ai blueprint di macchine Windows](#).

Scenario: aggiunta di posizioni di data center per distribuzioni tra più regioni

Si supponga che un amministratore di sistema desideri definire delle posizioni per i data center di Boston e Londra, in modo da consentire agli amministratori di struttura di applicare la posizione appropriata alle risorse di elaborazione in ciascun data center. Quando gli architetti creano i blueprint, possono attivare la funzionalità delle posizioni. Durante la compilazione dei moduli di richiesta per gli elementi del catalogo, gli utenti potranno quindi scegliere di eseguire il provisioning delle macchine a Boston o Londra.

Se si dispone di un data center a Londra e di uno a Boston, è importante evitare che gli utenti di Boston eseguano il provisioning di macchine sull'infrastruttura di Londra e viceversa. Affinché gli utenti di Boston e Londra possano eseguire il provisioning solo nella propria infrastruttura, è necessario consentire loro di selezionare la posizione appropriata per il provisioning al momento della richiesta delle macchine.



Non è possibile filtrare le posizioni dei data center nel file xml in base al tenant o al gruppo di business. Quando si opera in un ambiente multi-tenant, non è possibile utilizzare definizioni di proprietà per filtrare in base al tenant o al gruppo di business. Per informazioni sull'uso delle definizioni di proprietà, vedere il post del blog [How to use dynamic property definitions](#).

Procedura

- 1 Accedere all'host del server Web IaaS con credenziali di amministratore.

Si tratta della macchina su cui è stato installato il componente del sito Web di IaaS.

- 2 Modificare il file `WebSite\XmlData\DataCenterLocations.xml` nella directory di installazione del server in Windows (in genere `%SystemDrive%\Programmi x86\VMware\vCAC\Server`).
- 3 Modificare la sezione `CustomDataType` del file per creare le voci `Data Name` per ciascuna posizione.

```

<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
  
```

- 4 Salvare e chiudere il file.
- 5 Riavviare il servizio di gestione.
- 6 Se sono presenti più host del server Web IaaS, ripetere questa procedura su ciascuna istanza ridondante.

Risultati

L'amministratore di struttura può quindi applicare la posizione appropriata alle risorse di elaborazione di ciascun data center. Vedere [Scenario: applicazione di una posizione a una risorsa di elaborazione per distribuzioni tra più regioni](#).

Operazioni successive

È possibile aggiungere la proprietà `Vrm.DataCenter.Location` a un blueprint oppure abilitare l'opzione **Visualizza posizione su richiesta** nel blueprint per fare in modo che l'utente specifichi la posizione di un data center quando richiede il provisioning di una macchina.

Configurazione di vRealize Orchestrator

vRealize Orchestrator è un motore di automazione e gestione che apporta funzionalità a vRealize Automation, aggiungendo il supporto per XaaS e altre estendibilità. È possibile configurare e utilizzare il server vRealize Orchestrator preconfigurato nell'appliance vRealize Automation oppure distribuire vRealize Orchestrator come istanza di server esterna e associare tale istanza esterna a vRealize Automation.

vRealize Orchestrator consente ad amministratori e architetti di sviluppare complesse attività di automazione utilizzando lo strumento di progettazione dei workflow, i quali saranno successivamente accessibili ed eseguibili da vRealize Automation.

vRealize Orchestrator può accedere e controllare tecnologie e applicazioni esterne utilizzando plug-in di vRealize Orchestrator.

La configurazione di vRealize Automation per l'uso di vRealize Orchestrator consente di pubblicare i workflow di vRealize Orchestrator nel catalogo dei servizi di vRealize Orchestrator come parte della gestione dei blueprint XaaS.

Se si desidera eseguire i workflow per estendere la gestione delle macchine IaaS, è necessario configurare vRealize Orchestrator come endpoint.

Privilegi di configurazione

Gli amministratori di sistema e tenant possono configurare vRealize Automation per l'uso di un server vRealize Orchestrator esterno o di quello incorporato.

Inoltre, gli amministratori di sistema possono definire le cartelle dei workflow che saranno disponibili a ciascun tenant.

Gli amministratori tenant possono configurare i plug-in di vRealize Orchestrator come endpoint.

Ruolo	Privilegi di configurazione correlati a vRealize Orchestrator
Amministratori di sistema	<ul style="list-style-type: none"> ■ Configurare il server vRealize Orchestrator per tutti i tenant. ■ Definire cartelle di workflow di vRealize Orchestrator predefinite per ogni tenant.
Amministratori tenant	<ul style="list-style-type: none"> ■ Configurare il server vRealize Orchestrator per il proprio tenant. ■ Aggiungere plug-in di vRealize Orchestrator come endpoint.

Configurazione del server vRealize Orchestrator incorporato

L'appliance vRealize Automation include un'istanza preconfigurata di vRealize Orchestrator.

Prerequisiti

Distribuire l'appliance vRealize Automation. Per i dettagli, vedere *Distribuire l'appliance vRealize Automation* in *Installazione di vRealize Automation*.

Procedura

- 1 Accedere alla console di vRealize Automation come **amministratore di sistema** o **amministratore tenant**.
- 2 Selezionare **Amministrazione > Configurazione vRO > Configurazione server**.
- 3 Fare clic su **Usare il server Orchestrator predefinito**.

Risultati

Le connessioni al server vRealize Orchestrator incorporato sono configurate. La cartella dei workflow **VCAC** e le azioni dell'utilità correlata vengono importate automaticamente. La cartella dei workflow **VCAC > ASD** contiene i workflow per configurare gli endpoint e creare le mappature delle risorse.

Accesso a vRealize Orchestrator Control Center

Per modificare la configurazione dell'istanza di vRealize Orchestrator predefinita incorporata in vRealize Automation, è necessario accedere a vRealize Orchestrator Control Center.

I servizi di configurazione dell'istanza di vRealize Orchestrator incorporata vengono avviati automaticamente.

Nota È possibile verificare che la configurazione venga avviata automaticamente eseguendo il comando `chkconfig vco-configurator` dalla console della riga di comando di vRealize Orchestrator Appliance. Se il servizio segnala off, eseguire il comando `chkconfig vco-configurator on` e riavviare l'appliance.

Procedura

- 1 Collegarsi all'URL di vRealize Automation in un browser Web.
- 2 Fare clic su **vRealize Orchestrator Control Center**.

Si verrà reindirizzati a `https://vra-vd-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter`.

- 3 Immettere le credenziali root dell'ambiente vRealize Automation.

Accesso al client di vRealize Orchestrator

Per eseguire attività amministrative generali o per modificare e creare workflow nell'istanza predefinita di vRealize Orchestrator, è necessario accedere al client di vRealize Orchestrator.

L'interfaccia del client di vRealize Orchestrator è pensata per gli sviluppatori con diritti amministrativi che desiderano sviluppare workflow, azioni e altri elementi personalizzati.

Procedura

1 Collegarsi all'URL di vRealize Automation in un browser Web.

2 Per accedere al client vRealize Orchestrator basato su HTML5.

a Fare clic su **vRealize Orchestrator Client**.

b Immettere nome utente e password del client vRealize Orchestrator, quindi fare clic su **Accedi**.

Le credenziali corrispondono al nome utente e alla password dell'amministratore tenant predefinito.

3 Per accedere al client vRealize Orchestrator legacy.

a Fare clic su **Client vRealize Orchestrator legacy**.

Il file del client è stato scaricato.

b Fare clic sul download e seguire le istruzioni visualizzate.

c Nella finestra **Avviso sicurezza**, selezionare un'opzione per gestire l'avviso relativo al certificato.

Il client di vRealize Orchestrator comunica con il server di vRealize Orchestrator utilizzando un certificato SSL. Un'autorità di certificazione attendibile non firma il certificato durante l'installazione. L'avviso di sicurezza viene visualizzato ogni volta che ci si connette al server di vRealize Orchestrator.

Opzione	Descrizione
Continua	Continua utilizzando il certificato SSL corrente. Il messaggio di avviso viene visualizzato nuovamente quando ci si riconnette allo stesso server vRealize Orchestrator o quando si tenta di sincronizzare un workflow con un server vRealize Orchestrator remoto.
Annulla	Chiude la finestra e interrompe il processo di accesso.

d Fare clic su **Esegui**.

e Nella pagina di accesso a vRealize Orchestrator, immettere l'indirizzo IP o il nome di dominio dell'appliance vRealize Automation nella casella di testo **Nome host** e **443** come numero di porta predefinito.

Ad esempio immettere *vrealize_automation_appliance_ip:443*.

f Immettere nome utente e password del client vRealize Orchestrator, quindi fare clic su **Accedi**.

Le credenziali corrispondono al nome utente e alla password dell'amministratore tenant predefinito.

Operazioni successive

Utilizzare il client vRealize Orchestrator per sviluppare ed eseguire i workflow ed esportare i contenuti in altri ambienti vRealize Orchestrator utilizzando pacchetti. Vedere *Utilizzo del client di VMware vRealize Orchestrator e Sviluppare con VMware vRealize Orchestrator*.

Configurazione di un server vRealize Orchestrator esterno

È possibile configurare vRealize Automation per utilizzare un server vRealize Orchestrator esterno.

Gli amministratori di sistema possono configurare globalmente il server vRealize Orchestrator predefinito per tutti i tenant. Gli amministratori tenant possono configurare il server vRealize Orchestrator solo per i propri tenant.

Per potersi connettere a istanze del server vRealize Orchestrator esterno, gli account degli utenti devono disporre delle autorizzazioni di visualizzazione ed esecuzione in vRealize Orchestrator.

- Autenticazione Single Sign-On. Le informazioni degli utenti vengono trasmesse a vRealize Orchestrator insieme alla richiesta di XaaS e all'utente vengono concesse le autorizzazioni di visualizzazione ed esecuzione per il workflow richiesto.
- Autenticazione di base. L'account utente fornito deve essere membro di un gruppo di vRealize Orchestrator che disponga delle autorizzazioni di visualizzazione ed esecuzione o membro del gruppo vcoadmins.

Prerequisiti

- Installare e configurare un'appliance vRealize Orchestrator esterna. Vedere *Installazione e configurazione di vRealize Orchestrator* nella [documentazione del prodotto vRealize Orchestrator](#).
- Accedere alla console di vRealize Automation come **amministratore di sistema** o **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Configurazione server**.
- 2 Fare clic su **Usare un server Orchestrator esterno**.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Specificare l'indirizzo IP o il nome DNS della macchina su cui è in esecuzione il server vRealize Orchestrator nella casella di testo **Host**.

Nota Se il server vRealize Orchestrator esterno è configurato per l'utilizzo in modalità cluster, immettere l'indirizzo IP o il nome host del server virtuale del bilanciamento del carico che distribuisce le richieste dei client ai server vRealize Orchestrator nel cluster.

- 5 Specificare il numero di porta da utilizzare per la comunicazione con il server vRealize Orchestrator esterno nella casella di testo **Porta**.

La porta predefinita per vRealize Orchestrator è 8281.

- 6 Selezionare il tipo di autenticazione.

Opzione	Descrizione
Single Sign-On	La connessione al server vRealize Orchestrator avviene utilizzando vCenter Single Sign-On. Questa opzione è applicabile solo se vRealize Orchestrator e vRealize Automation sono stati configurati per utilizzare un'istanza vCenter Single Sign-On comune.
Di base	La connessione al server vRealize Orchestrator avviene utilizzando il nome utente e la password specificati nelle caselle di testo Nome utente e Password . L'account specificato deve essere un membro del gruppo vcoadmins di vRealize Orchestrator o un membro di un gruppo con autorizzazioni di visualizzazione ed esecuzione.

- 7 Fare clic su **Prova connessione**.

- 8 Fare clic su **OK**.

- 9 Importare il pacchetto `xaas.package`.

- Accedere all'appliance vRealize Automation come utente **root**.
- Individuare il pacchetto `xaas.package` nella cartella `/usr/lib/vcac/content/o11n/`.
- Importare il pacchetto `xaas.package` nel client esterno.

Risultati

È stata configurata la connessione al server vRealize Orchestrator esterno e sono state importate la cartella dei workflow **VCAC** e le azioni dell'utilità correlata. La cartella dei workflow **VCAC > ASD** contiene i workflow per configurare gli endpoint e creare le mappature delle risorse.

Operazioni successive

[Accesso al client di vRealize Orchestrator](#).

Configurazione delle risorse

È possibile configurare risorse quali endpoint, prenotazioni e profili di rete per supportare la definizione di blueprint di vRealize Automation e il provisioning di macchine.

Elenco di controllo per la configurazione di risorse di IaaS

Gli amministratori IaaS e gli amministratori di struttura configurano le risorse IaaS per integrare l'infrastruttura esistente con vRealize Automation e allocare le risorse dell'infrastruttura ai gruppi di business di vRealize Automation.

È possibile utilizzare l'Elenco di controllo per la configurazione di risorse di IaaS per avere un quadro generale della sequenza di passaggi necessari per configurare risorse di IaaS.

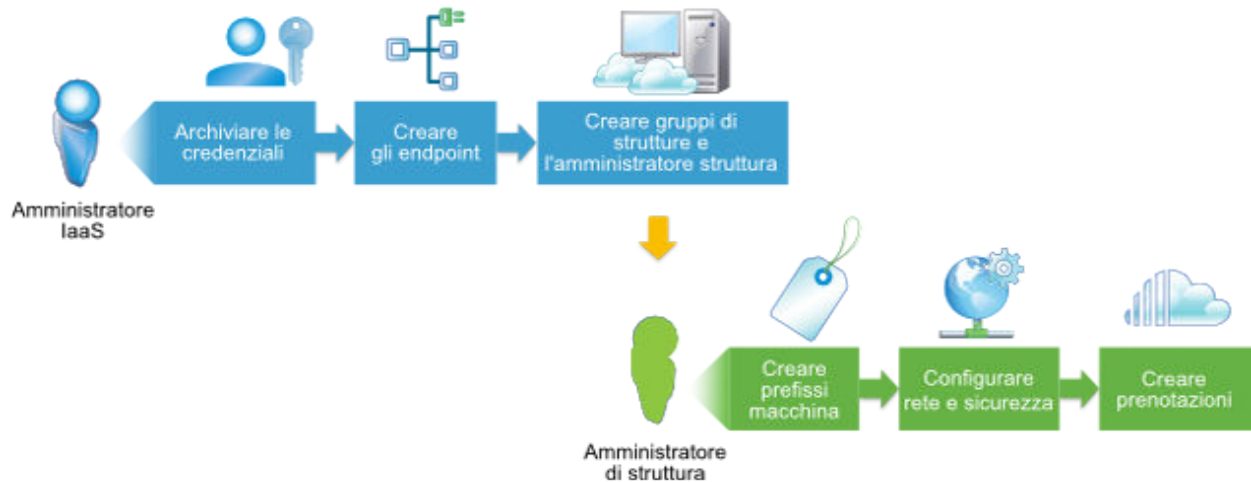


Tabella 2-11. Elenco di controllo per la configurazione di risorse di IaaS

Attività	Ruolo di vRealize Automation	Dettagli
<input type="checkbox"/> Creare endpoint per l'infrastruttura al fine di includere le risorse nell'ambito della gestione di vRealize Automation.	Amministratore di IaaS	Scelta dello scenario per un endpoint.
<input type="checkbox"/> Creare un gruppo di strutture per organizzare le risorse dell'infrastruttura in gruppi e assegnare uno o più amministratori per gestire queste risorse in qualità di amministratori di struttura di vRealize Automation.	Amministratore di IaaS	Creazione di un gruppo di strutture.
<input type="checkbox"/> Configurare i prefissi macchina utilizzati per creare i nomi delle macchine con provisioning eseguito tramite vRealize Automation.	Amministratore di struttura	Configurazione dei prefissi macchina.
<input type="checkbox"/> (Facoltativo) Creare profili di rete per configurare le impostazioni di rete per le macchine con provisioning eseguito.	Amministratore di struttura	Creazione di un profilo di rete in vRealize Automation.
<input type="checkbox"/> Allocare risorse dell'infrastruttura per i gruppi di business creando prenotazioni e, facoltativamente, profili di prenotazione e di prenotazione storage.	<ul style="list-style-type: none"> Amministratore e IaaS se configurato anche come amministratore di struttura Amministratore di struttura 	Configurazione di prenotazione e criteri di prenotazione.

Configurazione degli endpoint

È possibile creare e configurare gli endpoint che consentono a vRealize Automation di comunicare con l'infrastruttura.

Le definizioni degli endpoint vengono suddivise in categorie in base al tipo:

- Cloud

La categoria Cloud include i tipi di endpoint vCloud Air, vCloud Director, Amazon EC2 e OpenStack.

- IPAM

Questa categoria è visibile solo se è stato registrato un tipo di endpoint IPAM di terze parti, ad esempio Infoblox IPAM, in un workflow di vRealize Orchestrator.

- Gestione

Questa categoria include solo l'endpoint vRealize Operations Manager.

- Rete e sicurezza

Questa categoria include i tipi di endpoint Proxy e NSX.

Un endpoint Proxy può essere associato a un endpoint Amazon, vCloud Air o vCloud Director.

Un endpoint NSX può essere associato a un endpoint vSphere.

- Orchestration

Questa categoria include solo l'endpoint vRealize Orchestrator.

- Storage

Questa categoria include l'endpoint NetApp ONTAP.

- Virtuale

La categoria Virtuale include i tipi di endpoint vSphere, Hyper-V (SCVMM) e KVM (RHEV).

È possibile configurare tipi di endpoint aggiuntivi in vRealize Orchestrator e utilizzarli con i tipi di endpoint supportati in vRealize Automation. È inoltre possibile importare ed esportare gli endpoint a livello di programmazione.

Per informazioni sull'utilizzo degli endpoint dopo l'aggiornamento o la migrazione, vedere [Considerazioni sull'utilizzo di endpoint aggiornati o migrati](#).

Scelta dello scenario per un endpoint

Scegliere uno scenario di endpoint in base al tipo di endpoint di destinazione.

Per informazioni sulle impostazioni dell'endpoint disponibili, vedere [Riferimenti delle impostazioni degli endpoint](#).

Tabella 2-12. Scelta dello scenario per un endpoint

Endpoint	Ulteriori informazioni
vSphere	Vedere Creazione di un endpoint vSphere in vRealize Automation e associazione a NSX.
NSX	Vedere Creazione di un endpoint NSX for vSphere e associazione a un endpoint vSphere in vRealize Automation o Creazione di un endpoint NSX-T e associazione a un endpoint vSphere in vRealize Automation .
vCloud Air (sottoscrizione oppure OnDemand)	Vedere Creazione di un endpoint vCloud Air .
vCloud Director	Vedere Creazione di un endpoint vCloud Director .
vRealize Orchestrator	Vedere Creazione di un endpoint vRealize Orchestrator .
vRealize Operations	Vedere Creazione di un endpoint vRealize Operations Manager .
Provider IPAM di terze parti	Vedere Creazione di un endpoint di un provider IPAM di terze parti .
Microsoft Azure	Vedere Creazione di un endpoint Microsoft Azure .
Puppet	Vedere Creazione di un endpoint Puppet .
Amazon	Vedere Creazione di un endpoint Amazon e Aggiunta di un tipo di istanza Amazon .
OpenStack	Vedere Creazione di un endpoint OpenStack .
Proxy	Creazione di un endpoint Proxy e associazione a un endpoint Cloud
Hyper-V (SCVMM)	Vedere Creazione di un endpoint Hyper-V (SCVMM) .
KVM (RHEV)	Vedere Riferimenti delle impostazioni degli endpoint .
NetApp ONTAP	Vedere Storage con ottimizzazione dello spazio per il provisioning virtuale e Riferimenti delle impostazioni degli endpoint .
Hyper-V (autonomo), XenServer o master del pool Xen	Vedere Creazione di un endpoint Hyper-V, XenServer o di pool Xen .
Importazione di endpoint	Vedere Importazione o esportazione di endpoint a livello di programmazione .

Riferimenti delle impostazioni degli endpoint

È possibile utilizzare le impostazioni degli endpoint per definire la posizione e le credenziali di accesso per la raccolta dati e la distribuzione del catalogo dei servizi.

Scheda Generale

La maggior parte degli endpoint vRealize Automation include le opzioni seguenti. Le impostazioni che si riferiscono a un tipo specifico di endpoint sono segnalate.

Tabella 2-13. Impostazioni della scheda **Generale**

Impostazione	Descrizione
Nome	Immettere il nome dell'endpoint.
Descrizione	Immettere una descrizione per l'endpoint.
Indirizzo	<p>Immettere l'indirizzo dell'endpoint utilizzando il formato specifico degli endpoint.</p> <ul style="list-style-type: none"> ■ Per un endpoint KVM (RHEV) o NetApp ONTAP, l'indirizzo deve avere uno dei seguenti formati: <ul style="list-style-type: none"> ■ <code>https://FQDN</code> ■ <code>https://IP_address</code> Ad esempio: <code>https://mycompany-kvmrhev1.mycompany.local</code> o <code>netapp-1.mycompany.local</code>. ■ Per un endpoint OpenStack, il formato dell'indirizzo deve essere <code>https:// FQDN/powervc/openstack/ service</code>. Ad esempio: <code>https://openstack.mycompany.com/powervc/openstack/admin</code>. ■ Per un endpoint OpenStack, l'indirizzo deve avere uno dei seguenti formati: <ul style="list-style-type: none"> ■ <code>https://FQDN:500</code> ■ <code>https://IP_address:500</code> ■ Per un endpoint vSphere, il formato dell'indirizzo deve essere <code>https://host/sdk</code>. ■ Per un endpoint NSX, il formato dell'indirizzo deve essere <code>https://host</code>. ■ Per un endpoint vRealize Orchestrator, l'indirizzo deve essere del protocollo <code>https</code> e includere il nome completo o l'indirizzo IP del server vRealize Orchestrator e il numero di porta di vRealize Orchestrator, ad esempio <code>https://vrealize-automation-appliance-hostname:443/vco</code>. ■ Per un endpoint vRealize Operations, il formato dell'indirizzo deve essere <code>https://host/suite-api</code>.
Credenziali integrate	<p>Se si utilizzano le proprie credenziali integrate di vSphere, non è necessario immettere nome utente e password.</p> <p>Questa impostazione si applica solo agli endpoint vSphere.</p>
Nome utente	Immettere il nome utente di livello amministrativo archiviato per l'endpoint nel formato specifico dell'endpoint, come suggerito nell'interfaccia utente.
Password	Immettere la password di livello amministrativo archiviata per l'endpoint.
Progetto OpenStack	<p>Immettere un nome tenant OpenStack.</p> <p>Questa impostazione si applica solo agli endpoint OpenStack.</p>
Organizzazione	<p>In qualità di amministratore di un'organizzazione, è possibile immettere il nome di un'organizzazione di vCloud Director.</p> <p>Questa impostazione si applica solo a vCloud Director.</p>
ID chiave di accesso	<p>Immettere l'ID della chiave AWS Amazon.</p> <p>Questa impostazione si applica solo agli endpoint Amazon.</p>

Tabella 2-13. Impostazioni della scheda **Generale** (continua)

Impostazione	Descrizione
Chiave di accesso segreta	Immettere la chiave di accesso segreta AWS Amazon. Questa impostazione si applica solo agli endpoint Amazon.
Porta	Immettere il valore della porta per connettersi all'indirizzo dell'endpoint Proxy. Questa impostazione si applica solo agli endpoint Proxy.
Priorità	Immettere un valore di priorità come numero intero maggiore o uguale a 1. Più il valore è basso, più alta è la priorità. Il valore della priorità è associato alla proprietà personalizzata VMware.VCenterOrchestrator.Priority incorporata. Questa impostazione si applica solo agli endpoint vRealize Orchestrator.

Scheda Proprietà

Tutti i tipi di endpoint utilizzano una scheda delle proprietà per acquisire impostazioni e proprietà o gruppi di proprietà personalizzate. Per esempi di proprietà personalizzate per tipi di endpoint specifici, vedere *Guida di riferimento alle proprietà personalizzate*.

Scheda Associazioni

È possibile creare un'associazione a un endpoint NSX oppure a un endpoint Proxy, in base all'endpoint da cui si esegue l'associazione. È possibile associare un endpoint vSphere a un endpoint NSX per assegnare impostazioni di NSX all'endpoint vSphere. È inoltre possibile associare un endpoint vCloud Air, vCloud Director o Amazon a un endpoint Proxy per assegnare le impostazioni del proxy all'endpoint vCloud Air, vCloud Director o Amazon.

Prova connessione

È possibile utilizzare l'azione di prova della connessione per convalidare le credenziali, l'indirizzo endpoint dell'host e il certificato per un endpoint vSphere, NSX o vRealize Operations Manager. Vedere [Considerazioni sull'utilizzo della prova della connessione](#).

Creazione di un endpoint vSphere in vRealize Automation e associazione a NSX

È possibile creare endpoint vSphere in vRealize Automation che comunicano con vCenter per individuare le risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine. È inoltre possibile associare le impostazioni di NSX all'endpoint vSphere eseguendo l'associazione a un endpoint NSX for vSphere, a uno o più endpoint NSX-T oppure a entrambi i tipi di endpoint NSX.

L'associazione di un endpoint vSphere agli endpoint NSX for vSphere e NSX-T consente di configurare NSX for vSphere e NSX-T per cluster diversi in un singolo vCenter:

- Un amministratore IaaS può associare un endpoint vSphere a un endpoint NSX for vSphere e a un endpoint NSX-T.
- Un amministratore di struttura può creare una prenotazione NSX for vSphere o NSX-T in base alla risorsa di elaborazione.
- Un architetto di blueprint può creare blueprint che siano specifici di NSX for vSphere o NSX-T. Entrambi i tipi di blueprint possono essere distribuiti nello stesso ambiente vCenter.

È possibile creare un'associazione tra gli endpoint vSphere e NSX. Le associazioni includono:

- Un endpoint vSphere associato a un singolo endpoint NSX for vSphere.
- Un endpoint vSphere associato a più endpoint NSX-T.
- Un endpoint NSX-T associato a più endpoint vSphere.
- Un endpoint NSX for vSphere associato a un singolo endpoint vSphere.
- Un endpoint vSphere associato a un endpoint NSX for vSphere e a un endpoint NSX-T.

Quando un endpoint vSphere è associato sia a un endpoint NSX for vSphere sia a un endpoint NSX-T, il cluster viene gestito da NSX for vSphere o da NSX-T. La gestione di NSX è determinata da vRealize Automation quando gli endpoint vengono raccolti in base ai dati e la relazione viene stabilita. È possibile visualizzare il tipo di piattaforma NSX che gestisce un cluster specifico ispezionando la colonna **Tipo NSX** nella pagina **Risorse di elaborazione**.

Per informazioni sulla creazione di endpoint NSX associati a un endpoint vSphere, vedere [Creazione di un endpoint NSX for vSphere e associazione a un endpoint vSphere in vRealize Automation](#) o [Creazione di un endpoint NSX-T e associazione a un endpoint vSphere in vRealize Automation](#).

Per ulteriori informazioni sulla convalida della connessione dell'endpoint e l'attendibilità del certificato, vedere [Considerazioni sull'utilizzo della prova della connessione](#).

Se si aggiorna o si migra un endpoint vSphere che utilizzava un gestore NSX, viene creato un nuovo endpoint NSX contenente un'associazione tra l'endpoint vSphere di origine e un nuovo endpoint NSX.

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Per gestire l'endpoint vSphere, è necessario installare un agente proxy vSphere. Il nome dell'agente e il nome dell'endpoint devono coincidere. Per informazioni sull'installazione dell'agente, vedere *Installazione di vRealize Automation*.
- Se si intende utilizzare un endpoint vSphere per distribuire macchine virtuali da modelli OVF, verificare che le proprie credenziali includano il privilegio `VApp.Import` di vSphere nell'istanza di vCenter Server associata all'endpoint.

Il privilegio `VApp.Import` consente di distribuire una macchina vSphere utilizzando le impostazioni importate da un OVF. Informazioni dettagliate sul privilegio vSphere sono disponibili nella [documentazione di vSphere SDK](#).

Se il file OVF è ospitato su un sito Web, vedere [Creazione di un endpoint proxy per il sito Web host di OVF](#).

- Configurare impostazioni di rete e di sicurezza di NSX aggiuntive per l'endpoint vSphere, creare un endpoint NSX for vSphere o NSX-T. È possibile stabilire l'associazione all'endpoint NSX quando si crea o si modifica l'endpoint vSphere.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.

- 2 Selezionare **Nuovo > Virtuale > vSphere**.

- 3 Immettere un nome nella casella di testo **Nome**.

Il nome deve corrispondere al nome dell'endpoint fornito all'agente proxy di vSphere durante l'installazione. Se il nome non coincide, la raccolta dati non riesce.

- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.

- 5 Specificare l'URL dell'istanza di vCenter Server nella casella di testo **Indirizzo**.

L'URL deve essere di tipo **https://hostname/sdk** o **https://IP_address/sdk**.

Ad esempio **https://vsphereA/sdk**.

- 6 Immettere il nome utente e la password di livello amministratore di vSphere oppure utilizzare le credenziali di vSphere integrate.

Fornire credenziali autorizzate alla modifica di attributi personalizzati.

Il formato del nome utente è *dominio\nomeutente*.

Per utilizzare l'account del servizio dell'agente proxy di vSphere per connettersi al vCenter Server, selezionare **Usa credenziali integrate**.

Se si utilizzano le proprie credenziali integrate di vSphere, non è necessario immettere nome utente e password.

- 7 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.

- 8 (Facoltativo) Per configurare impostazioni di rete e sicurezza NSX per l'endpoint, fare clic su **Associazioni** ed effettuare l'associazione a un endpoint NSX for vSphere o NSX-T esistente.

È necessario disporre di almeno un endpoint NSX per creare un'associazione.

- 9 (Facoltativo) Per convalidare le credenziali, l'indirizzo dell'endpoint host e l'attendibilità del certificato, fare clic su **Prova connessione**. L'azione consente inoltre di verificare che il servizio e l'agente di gestione siano in esecuzione, in modo da consentire la raccolta dati nell'endpoint. L'azione **OK** consente di provare queste stesse condizioni.

L'azione **Prova connessione** restituisce informazioni relative a qualsiasi condizione seguente:

- Errore del certificato

Se non viene rilevato alcun certificato, oppure se questo non è attendibile o è scaduto, viene chiesto di accettare un'identificazione personale del certificato. Se non si accetta l'identificazione personale, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

- Errore dell'agente

L'agente di vSphere associato non viene rilevato. Per la buona riuscita della prova, è necessario che l'agente sia in esecuzione.

- Errore dell'host

L'indirizzo dell'endpoint specificato non è raggiungibile oppure il servizio di gestione associato non è in esecuzione. Per la buona riuscita della prova, è necessario che il servizio di gestione sia in esecuzione.

- Errore delle credenziali

La combinazione di nome utente e password specificata non è valida per l'endpoint nell'indirizzo specificato.

- Timeout

Non è stato possibile completare l'azione di prova nel periodo di tempo di due minuti consentito.

Se l'azione **Prova connessione** non riesce, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

Se si è verificato un problema di attendibilità del certificato, ad esempio se il certificato è scaduto, verrà chiesto di accettare un'identificazione personale del certificato.

10 Per salvare l'endpoint, fare clic su **OK**.

L'azione **OK** verifica le stesse condizioni dell'azione **Prova connessione**. Se viene trovata una qualsiasi delle condizioni precedenti, viene restituito un messaggio. Se è possibile salvarlo, l'errore viene mantenuto sullo schermo per consentirne l'analisi.

Risultati

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Nota Non rinominare i data center di vSphere dopo la raccolta iniziale dei dati, altrimenti il provisioning potrebbe non riuscire.

Per ulteriori informazioni, vedere [Visualizzazione delle risorse di elaborazione ed esecuzione della raccolta dati](#).

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint NSX for vSphere e associazione a un endpoint vSphere in vRealize Automation

È possibile creare un endpoint NSX for vSphere e associarlo a un endpoint vSphere esistente in vRealize Automation.

È possibile associare un endpoint NSX for vSphere a un endpoint vSphere.

È possibile creare un'associazione tra gli endpoint vSphere e NSX. Le associazioni includono:

- Un endpoint vSphere associato a un singolo endpoint NSX for vSphere.
- Un endpoint vSphere associato a più endpoint NSX-T.
- Un endpoint NSX-T associato a più endpoint vSphere.
- Un endpoint NSX for vSphere associato a un singolo endpoint vSphere.
- Un endpoint vSphere associato a un endpoint NSX for vSphere e a un endpoint NSX-T.

Quando un endpoint vSphere è associato sia a un endpoint NSX for vSphere sia a un endpoint NSX-T, il cluster viene gestito da NSX for vSphere o da NSX-T. La gestione di NSX è determinata da vRealize Automation quando gli endpoint vengono raccolti in base ai dati e la relazione viene stabilita. È possibile visualizzare il tipo di piattaforma NSX che gestisce un cluster specifico ispezionando la colonna **Tipo NSX** nella pagina **Risorse di elaborazione**.

Per ulteriori informazioni sulla convalida della connessione dell'endpoint e l'attendibilità del certificato, vedere [Considerazioni sull'utilizzo della prova della connessione](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- È necessario installare un agente proxy di vSphere per gestire l'endpoint di vSphere ed è necessario utilizzare esattamente lo stesso nome per l'endpoint e l'agente. Per informazioni sull'installazione dell'agente, vedere *Installazione di vRealize Automation*.
- Configurare le impostazioni della rete NSX for vSphere. Vedere [Configurazione delle impostazioni dei componenti rete e sicurezza in vRealize Automation](#).
- [Creazione di un endpoint vSphere in vRealize Automation e associazione a NSX](#).

Nella preparazione per l'utilizzo delle funzionalità di rete, sicurezza e bilanciamento del carico di NSX in vRealize Automation, quando si utilizzano credenziali di NSX Manager è necessario utilizzare l'account amministratore di NSX Manager.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Rete e sicurezza > NSX**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Specificare l'URL dell'istanza di NSX for vSphere nella casella di testo **Indirizzo**.

L'URL deve essere di tipo **https://hostname** o **https://IP_address**.

Ad esempio, **https://abx.nsx-manager.local/**.

- 6 Immettere il nome utente e la password di livello amministrativo di NSX archiviati per l'endpoint NSX for vSphere.

- 7 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.

- 8 Per associare le impostazioni di rete e sicurezza NSX for vSphere a un endpoint vSphere esistente, fare clic su **Associazioni** e selezionare un endpoint vSphere esistente.

Prima di poter creare l'associazione, è necessario creare l'endpoint vSphere.

Un endpoint vSphere può essere associato a un solo tipo di piattaforma di rete e sicurezza - NSX for vSphere o NSX-T.

Un endpoint NSX for vSphere può essere associato solo a un endpoint vSphere. Questo vincolo di associazione indica che non si può eseguire il provisioning di una rete su richiesta universale e collegarlo alle macchine vSphere con provisioning su vCenter diversi.

Al termine dell'associazione, la colonna Descrizione nella pagina indica il tipo di associazione di NSX for vSphere.

- 9 (Facoltativo) Per convalidare le credenziali, l'indirizzo dell'endpoint host e l'attendibilità del certificato, fare clic su **Prova connessione**. L'azione consente inoltre di verificare che il servizio e l'agente di gestione siano in esecuzione, in modo da consentire la raccolta dati nell'endpoint. L'azione **OK** consente di provare queste stesse condizioni.

L'azione **Prova connessione** restituisce informazioni relative a qualsiasi condizione seguente:

- Errore del certificato

Se non viene rilevato alcun certificato, oppure se questo non è attendibile o è scaduto, viene chiesto di accettare un'identificazione personale del certificato. Se non si accetta l'identificazione personale, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

- Errore dell'agente

L'agente di vSphere associato non viene rilevato. Per la buona riuscita della prova, è necessario che l'agente sia in esecuzione.

- Errore dell'host

L'indirizzo dell'endpoint specificato non è raggiungibile oppure il servizio di gestione associato non è in esecuzione. Per la buona riuscita della prova, è necessario che il servizio di gestione sia in esecuzione.

- Errore delle credenziali

La combinazione di nome utente e password specificata non è valida per l'endpoint nell'indirizzo specificato.

- Timeout

Non è stato possibile completare l'azione di prova nel periodo di tempo di due minuti consentito.

Se l'azione **Prova connessione** non riesce, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

Se si è verificato un problema di attendibilità del certificato, ad esempio se il certificato è scaduto, verrà chiesto di accettare un'identificazione personale del certificato.

10 Per salvare l'endpoint, fare clic su **OK**.

L'azione **OK** verifica le stesse condizioni dell'azione **Prova connessione**. Se viene trovata una qualsiasi delle condizioni precedenti, viene restituito un messaggio. Se è possibile salvarlo, l'errore viene mantenuto sullo schermo per consentirne l'analisi.

Risultati

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Per informazioni sull'esecuzione della raccolta dati per endpoint esistenti dopo la raccolta dati iniziale, vedere [Visualizzazione delle risorse di elaborazione ed esecuzione della raccolta dati](#).

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint NSX-T e associazione a un endpoint vSphere in vRealize Automation
È possibile creare un endpoint NSX-T e associarlo a un endpoint vSphere esistente in vRealize Automation.

vRealize Automation utilizza l'autenticazione di base per la connessione con l'endpoint NSX-T.

Per semplificare la tolleranza agli errori e l'alta disponibilità nelle distribuzioni, ogni endpoint del data center di NSX-T rappresenta un cluster di tre NSX Manager.

- vRealize Automation può puntare a uno degli NSX Manager. Con questa opzione, un NSX Manager riceve le chiamate API da vRealize Automation.
- vRealize Automation può puntare all'IP virtuale del cluster. Con questa opzione, un NSX Manager assume il controllo del VIP. Tale Manager riceve le chiamate API da vRealize Automation. In caso di errore, un altro nodo del cluster assume il controllo del VIP e riceve le chiamate API da vRealize Automation.

Per ulteriori informazioni sulla configurazione del VIP, vedere *Configurazione di un indirizzo IP virtuale (VIP) per un cluster nella Guida all'installazione di NSX-T Data Center* nella [documentazione di VMware NSX-T Data Center](#).

- vRealize Automation può puntare a un VIP di bilanciamento del carico per bilanciare il carico delle chiamate ai tre NSX Manager. Utilizzando questa opzione, tutti e tre gli NSX Manager ricevono chiamate API da vRealize Automation.

È possibile configurare il VIP in un bilanciamento del carico di terze parti o in un bilanciamento del carico di NSX-T.

Per gli ambienti su larga scala, è consigliabile utilizzare questa opzione per suddividere le chiamate API di vRealize Automation fra i tre NSX Manager.

Utilizzare queste informazioni quando si specifica l'endpoint NSX-T nel passaggio 5.

È possibile associare un endpoint NSX-T a più endpoint vSphere.

È possibile creare un'associazione tra gli endpoint vSphere e NSX. Le associazioni includono:

- Un endpoint vSphere associato a un singolo endpoint NSX for vSphere.
- Un endpoint vSphere associato a più endpoint NSX-T.
- Un endpoint NSX-T associato a più endpoint vSphere.
- Un endpoint NSX for vSphere associato a un singolo endpoint vSphere.
- Un endpoint vSphere associato a un endpoint NSX for vSphere e a un endpoint NSX-T.

Quando un endpoint vSphere è associato sia a un endpoint NSX for vSphere sia a un endpoint NSX-T, il cluster viene gestito da NSX for vSphere o da NSX-T. La gestione di NSX è determinata da vRealize Automation quando gli endpoint vengono raccolti in base ai dati e la relazione viene stabilita. È possibile visualizzare il tipo di piattaforma NSX che gestisce un cluster specifico ispezionando la colonna **Tipo NSX** nella pagina **Risorse di elaborazione**.

Quando si distribuisce un blueprint che contiene un endpoint NSX-T, la distribuzione assegna un tag ai componenti NSX-T nella distribuzione. Il nome del tag e il nome della distribuzione corrispondono.

Per ulteriori informazioni sulla convalida della connessione dell'endpoint e l'attendibilità del certificato, vedere [Considerazioni sull'utilizzo della prova della connessione](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- È necessario installare un agente proxy di vSphere per gestire l'endpoint di vSphere ed è necessario utilizzare esattamente lo stesso nome per l'endpoint e l'agente. Per informazioni sull'installazione dell'agente, vedere *Installazione di vRealize Automation*.
- Configurare le impostazioni della rete NSX-T. Vedere [Configurazione delle impostazioni dei componenti rete e sicurezza in vRealize Automation](#).
- [Creazione di un endpoint vSphere in vRealize Automation e associazione a NSX](#).

Nella preparazione per l'utilizzo delle funzionalità di rete, sicurezza e bilanciamento del carico di NSX in vRealize Automation, quando si utilizzano credenziali di NSX Manager è necessario utilizzare l'account amministratore di NSX Manager.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Rete e sicurezza > NSX-T**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.

- 5 Immettere l'URL per l'istanza di NSX-T Endpoint Manager o VIP (vedere sopra) nella casella di testo **Indirizzo**.

L'URL deve essere di tipo **https://hostname** o **https://IP_address**.

Ad esempio, **https://abx-nsxt3-manager.local**.

- 6 Immettere il nome utente e la password di livello amministrativo di NSX archiviati per l'endpoint NSX-T.
- 7 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.
- 8 Per associare le impostazioni di rete e sicurezza NSX-T a un endpoint vSphere esistente, fare clic su **Associazioni** e selezionare un endpoint vSphere esistente.

Prima di poter creare l'associazione, è necessario creare l'endpoint vSphere.

Un endpoint vSphere può essere associato a un solo tipo di piattaforma di rete e sicurezza - NSX for vSphere o NSX-T.

È possibile associare un endpoint NSX-T a più endpoint vSphere. Un'istanza di NSX-T può gestire più cluster ESX in vCenter diversi.

Al termine dell'associazione, la colonna Descrizione nella pagina indica il tipo di associazione di NSX-T.

- 9 (Facoltativo) Per convalidare le credenziali, l'indirizzo dell'endpoint host e l'attendibilità del certificato, fare clic su **Prova connessione**. L'azione consente inoltre di verificare che il servizio e l'agente di gestione siano in esecuzione, in modo da consentire la raccolta dati nell'endpoint. L'azione **OK** consente di provare queste stesse condizioni.

L'azione **Prova connessione** restituisce informazioni relative a qualsiasi condizione seguente:

- Errore del certificato

Se non viene rilevato alcun certificato, oppure se questo non è attendibile o è scaduto, viene chiesto di accettare un'identificazione personale del certificato. Se non si accetta l'identificazione personale, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

- Errore dell'agente

L'agente di vSphere associato non viene rilevato. Per la buona riuscita della prova, è necessario che l'agente sia in esecuzione.

- Errore dell'host

L'indirizzo dell'endpoint specificato non è raggiungibile oppure il servizio di gestione associato non è in esecuzione. Per la buona riuscita della prova, è necessario che il servizio di gestione sia in esecuzione.

- Errore delle credenziali

La combinazione di nome utente e password specificata non è valida per l'endpoint nell'indirizzo specificato.

- Timeout

Non è stato possibile completare l'azione di prova nel periodo di tempo di due minuti consentito.

Se l'azione **Prova connessione** non riesce, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

Se si è verificato un problema di attendibilità del certificato, ad esempio se il certificato è scaduto, verrà chiesto di accettare un'identificazione personale del certificato.

10 Per salvare l'endpoint, fare clic su **OK**.

L'azione **OK** verifica le stesse condizioni dell'azione **Prova connessione**. Se viene trovata una qualsiasi delle condizioni precedenti, viene restituito un messaggio. Se è possibile salvarlo, l'errore viene mantenuto sullo schermo per consentirne l'analisi.

Risultati

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Per informazioni sull'esecuzione della raccolta dati per endpoint esistenti dopo la raccolta dati iniziale, vedere [Visualizzazione delle risorse di elaborazione ed esecuzione della raccolta dati](#).

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint vCloud Air

È possibile creare un endpoint vCloud Air per un servizio di sottoscrizione o di OnDemand. Facoltativamente è possibile associare le impostazioni del proxy all'endpoint vCloud Director effettuando l'associazione a un endpoint Proxy.

Per informazioni sulla console di gestione di vCloud Air, vedere la documentazione di vCloud Air.

Nota Le prenotazioni definite per gli endpoint vCloud Air e gli endpoint vCloud Director non supportano l'uso di profili di rete per il provisioning delle macchine.

Per gli endpoint vCloud Air, il nome dell'organizzazione e il nome vDC devono essere identici per un'istanza di sottoscrizione di vCloud Air.

Per informazioni sull'associazione delle impostazioni del proxy all'endpoint, vedere [Creazione di un endpoint Proxy e associazione a un endpoint Cloud](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Verificare di avere l'autorizzazione **Virtual Infrastructure Administrator** per il servizio di sottoscrizione di vCloud Air o l'account di OnDemand.

- Se si desidera configurare una protezione aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy, creare un endpoint Proxy. È possibile effettuare un'associazione all'endpoint Proxy quando si crea l'endpoint vCloud Director. Vedere [Creazione di un endpoint Proxy e associazione a un endpoint Cloud](#).

Procedura

1 Selezionare **Infrastruttura > Endpoint > Endpoint**.

2 Selezionare **Nuovo > Cloud > vCloud Air**.

3 Immettere un nome e, facoltativamente, una descrizione.

4 Accettare l'indirizzo dell'endpoint di vCloud Air predefinito nella casella di testo **Indirizzo** o immetterne uno nuovo.

L'indirizzo dell'endpoint di vCloud Air predefinito è `https://vca.vmware.com`, come specificato nella proprietà globale `Default URL for vCloud Air endpoint`.

5 Immettere il nome utente e la password di livello amministrativo.

Le credenziali devono essere quelle del servizio di sottoscrizione di vCloud Air o dell'amministratore dell'account di OnDemand.

Il formato del nome utente è `dominio\nomeutente`.

Fornire le credenziali di un amministratore di organizzazione con diritti di connessione utilizzando VMware Remote Console.

6 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.

7 (Facoltativo) Per configurare una sicurezza aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy, fare clic su **Associazioni** ed effettuare l'associazione a un endpoint Proxy esistente.

È necessario disporre di almeno un endpoint Proxy per creare un'associazione.

8 Fare clic su **OK**.

Operazioni successive

[Creazione di un gruppo di strutture](#).

Creazione di un endpoint vCloud Director

È possibile creare un endpoint vCloud Director per gestire tutti i virtual data center (vDC) di vCloud Director nell'ambiente, oppure creare endpoint separati per gestire ciascuna organizzazione vCloud Director. Facoltativamente è possibile associare le impostazioni del proxy all'endpoint vCloud Director effettuando l'associazione a un endpoint Proxy.

Per informazioni sui vDC di organizzazione, vedere la documentazione di vCloud Director.

Evitare di creare un singolo endpoint ed endpoint di organizzazione individuali per la stessa istanza di vCloud Director.

vRealize Automation utilizza un agente proxy per gestire le risorse di vSphere.

Nota Le prenotazioni definite per gli endpoint vCloud Air e gli endpoint vCloud Director non supportano l'uso di profili di rete per il provisioning delle macchine.

Le informazioni sul lease per le macchine vCloud Director devono essere specificate in vRealize Automation e non in vCloud Director. Se si specificano informazioni sul lease in vCloud Director, non vengono riconosciute o utilizzate in vRealize Automation. Immettere le informazioni sul lease per le macchine vCloud Director nel blueprint di vRealize Automation, non in vCloud Director.

Per informazioni sull'associazione delle impostazioni del proxy all'endpoint, vedere [Creazione di un endpoint Proxy e associazione a un endpoint Cloud](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Se si desidera configurare una protezione aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy, creare un endpoint Proxy. È possibile effettuare un'associazione all'endpoint Proxy quando si crea l'endpoint vCloud Director. Vedere [Creazione di un endpoint Proxy e associazione a un endpoint Cloud](#).

Procedura

1 Selezionare **Infrastruttura > Endpoint > Endpoint**.

2 Selezionare **Nuovo > Cloud > vCloud Director**.

3 Immettere un nome e, facoltativamente, una descrizione.

4 Immettere l'URL del server vCloud Director nella casella di testo **Indirizzo**.

L'URL deve essere di tipo *FQDN* o *IP_address*.

Ad esempio <https://mycompany.com>.

5 Immettere il nome utente e la password di livello amministrativo.

- Per connettersi al server vCloud Director e specificare l'organizzazione per cui l'utente ha un ruolo di amministratore, utilizzare le credenziali dell'amministratore dell'organizzazione. Con queste credenziali, l'endpoint potrà accedere solo ai vDC di organizzazione associati. È possibile aggiungere endpoint per ogni altra organizzazione nell'istanza di vCloud Director da integrare con vRealize Automation.
- Per consentire l'accesso a tutte le vDC di organizzazione nell'istanza di vCloud Director, utilizzare le credenziali di amministratore di sistema di un vCloud Director e lasciare vuota la casella di testo **Organizzazione**.

- 6 Un amministratore dell'organizzazione può specificare un nome per l'organizzazione di vCloud Director nella casella di testo **Organizzazione**.

Opzione	Descrizione
Rileva tutti i vCD dell'organizzazione	Se vCloud Director è stato implementato in un cloud privato, è possibile lasciare vuota la casella di testo Organizzazione per consentire all'applicazione di trovare tutti i vDC di organizzazione disponibili.
Separa endpoint per ogni vCD dell'organizzazione	Immettere un nome per l'organizzazione di vCloud Director nella casella di testo Organizzazione .

Il nome **Organizzazione** corrisponde al nome della propria organizzazione di vCloud Director, che potrebbe essere mostrato anche come nome del virtual data center (vDC). Se si utilizza un Virtual Private Cloud, questo nome è un identificatore univoco nel formato M123456789-12345. In un dedicated cloud, è il nome del vDC di destinazione.

Se ci si connette direttamente a vCloud Director a livello di sistema, ad esempio lasciando vuoto il campo Organizzazione, è necessario specificare credenziali di amministratore di sistema. Se si accede a un'organizzazione nell'endpoint, è necessario disporre delle credenziali di amministratore per tale organizzazione.

Fornire credenziali con diritti di connessione utilizzando VMware Remote Console.

- Per gestire tutte le organizzazioni con un singolo endpoint, fornire le credenziali di un amministratore di sistema.
- Per gestire ciascun vDC (Virtual Data Center) con un endpoint separato, creare credenziali di amministratore di organizzazione per ogni vDC.

Evitare di creare un singolo endpoint a livello di sistema ed endpoint di organizzazione individuali per la stessa istanza di vCloud Director.

- 7 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.
- 8 (Facoltativo) Per configurare una sicurezza aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy, fare clic su **Associazioni** ed effettuare l'associazione a un endpoint Proxy esistente.

È necessario disporre di almeno un endpoint Proxy per creare un'associazione.

- 9 Fare clic su **OK**.

Operazioni successive

Creazione di un gruppo di strutture.

Creazione di un endpoint Amazon

È possibile creare un endpoint da connettere a un'istanza di Amazon. Facoltativamente, è possibile associare le impostazioni del proxy all'endpoint Amazon stabilendo l'associazione a un endpoint Proxy.

vRealize Automation offre diversi tipi di istanze di Amazon utilizzabili quando si creano blueprint, ma se si desidera importare altri tipi di istanze, vedere [Aggiunta di un tipo di istanza Amazon](#).

Per informazioni sull'associazione delle impostazioni del proxy all'endpoint, vedere [Creazione di un endpoint Proxy e associazione a un endpoint Cloud](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Se si desidera configurare una protezione aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy, creare un endpoint Proxy. È possibile stabilire l'associazione all'endpoint Proxy quando si crea l'endpoint Amazon. Vedere [Creazione di un endpoint Proxy e associazione a un endpoint Cloud](#).

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Cloud > Amazon EC2**.
- 3 Immettere un nome e, facoltativamente, una descrizione.
Questo nome indica in genere l'account Amazon corrispondente a questo endpoint.
- 4 Immettere l'ID della chiave di accesso di livello amministrativo per l'endpoint Amazon.
A un dato ID di chiave di accesso di Amazon è possibile associare un solo endpoint.
Per ottenere la chiave di accesso necessaria per creare l'endpoint Amazon, è necessario richiedere una chiave a un utente che dispone di credenziali di amministratore con accesso completo di AWS oppure essere configurato ulteriormente con il criterio di amministratore con accesso completo di AWS. Per ulteriori dettagli, vedere la documentazione di Amazon.
- 5 Immettere la chiave di accesso segreta per l'endpoint Amazon.
- 6 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.
- 7 (Facoltativo) Per configurare una sicurezza aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy, fare clic su **Associazioni** ed effettuare l'associazione a un endpoint Proxy esistente.
È necessario disporre di almeno un endpoint Proxy per creare un'associazione.
- 8 Fare clic su **OK**.

Risultati

Dopo la creazione dell'endpoint, vRealize Automation inizia a raccogliere i dati dalle regioni di Amazon Web Services.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Aggiunta di un tipo di istanza Amazon

vRealize Automation include diversi tipi di istanza da utilizzare con i blueprint Amazon. Un amministratore può aggiungere e rimuovere i tipi di istanza.

I tipi di istanza della macchina gestiti dagli amministratori IaaS sono disponibili per gli architetti dei blueprint durante la creazione o la modifica di un blueprint Amazon. Le immagini e i tipi di istanza delle macchine Amazon vengono rese disponibili tramite il prodotto Amazon Web Services.

Prerequisiti

Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Fare clic su **Infrastruttura > Amministrazione > Tipi di istanze**.
- 2 Fare clic su **Nuovo**.
- 3 Aggiungere un nuovo tipo di istanza, specificando i parametri seguenti.

Le informazioni sui tipi di istanza di Amazon disponibili e sui valori delle impostazioni che è possibile specificare per questi parametri sono contenute nella documentazione di Amazon Web Services in *Tipi di istanze di Amazon EC2 - Amazon Web Services (AWS)* all'indirizzo <https://aws.amazon.com/it/ec2/> e in *Tipi di istanze* all'indirizzo <http://aws.amazon.com/it/documentation/>.

- Nome
- Nome API
- Nome tipo
- Nome prestazioni I/O
- CPU
- Memoria (GB)
- Storage (GB)
- Unità di elaborazione

- 4 Fare clic sull'icona **Salva** (✓).

Risultati

Quando gli architetti di IaaS creano i blueprint di Amazon Web Services, possono utilizzare i tipi di istanze personalizzati.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint Proxy e associazione a un endpoint Cloud

È possibile creare un endpoint Proxy e associare le relative impostazioni a un endpoint vCloud Air, vCloud Director o Amazon.

Se si aggiorna o si migra un endpoint vCloud Air, vCloud Director o Amazon che utilizzava un gestore proxy, viene creato un nuovo endpoint vCloud Air, vCloud Director o Amazon contenente un'associazione tra l'endpoint vCloud Air, vCloud Director o Amazon e un nuovo endpoint Proxy.

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Creare uno dei seguenti tipi di endpoint:
 - [Creazione di un endpoint vCloud Air](#)
 - [Creazione di un endpoint Amazon](#)
 - [Creazione di un endpoint vCloud Director](#)

Per creare un'associazione dall'endpoint Proxy, è necessario disporre di almeno un endpoint vCloud Air, vCloud Director o Amazon.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Rete e sicurezza > Proxy**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Nella casella di testo **Indirizzo** immettere l'URL dell'agente proxy installato.
- 6 Specificare il numero di porta da utilizzare per la connessione al server proxy nella casella di testo **Porta**.
- 7 Immettere il nome utente e la password di livello amministrativo.
- 8 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.
- 9 Per associare le impostazioni del proxy a un endpoint vCloud Air, vCloud Director o Amazon, fare clic su **Associazioni** e selezionare uno o più endpoint.

 È necessario disporre di almeno un endpoint vCloud Air, vCloud Director o Amazon per creare un'associazione.

 È possibile associare l'endpoint Proxy a più endpoint.
- 10 Fare clic su **OK**.

Risultati

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint proxy per il sito Web host di OVF

È possibile creare un endpoint proxy da utilizzare quando si importa un OVF in un componente macchina vSphere in un blueprint o come set di valori per un profilo componente immagine quando l'OVF è ospitato su un sito Web.

Per informazioni sulla configurazione per la distribuzione di OVF, vedere [Creazione di un endpoint vSphere in vRealize Automation e associazione a NSX](#) e [Configurazione di un blueprint per il provisioning da un OVF](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Rete e sicurezza > Proxy**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Immettere l'URL del sito Web che ospita il file OVF nella casella di testo **Indirizzo**.
- 6 Specificare il numero di porta da utilizzare per la connessione al server proxy del sito Web nella casella di testo **Porta**.
- 7 Immettere il nome utente e la password di livello amministrativo.
- 8 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.
- 9 Fare clic su **OK**.

Risultati

A questo punto è possibile utilizzare l'endpoint per definire il sito Web in cui si desidera ottenere l'OVF. Per informazioni dettagliate, vedere [Definizione delle impostazioni del blueprint per un componente vSphere utilizzando un OVF](#) e [Definizione di un set di valori dell'immagine per un profilo componente mediante un OVF](#).

Creazione di un endpoint vRealize Orchestrator

È possibile creare un endpoint vRealize Orchestrator per effettuare la connessione a un server vRealize Orchestrator.

È possibile configurare più endpoint per connettersi a diversi server vRealize Orchestrator, ma è necessario configurare una priorità per ciascun endpoint.

Quando si eseguono workflow di vRealize Orchestrator, vRealize Automation prova prima con gli endpoint di vRealize Orchestrator con priorità più alta. Se l'endpoint provato non è raggiungibile, procede con l'endpoint con priorità maggiore successivo, finché non si ottiene un server vRealize Orchestrator disponibile per l'esecuzione del workflow.

Prerequisiti

- Accedere a vRealize Automation come **amministratore laaS**.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Orchestrazione > vRealize Orchestrator**.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Immettere un URL con il nome completo o l'indirizzo IP del server di vRealize Orchestrator e il numero di porta di vRealize Orchestrator.

Il protocollo di trasporto deve essere HTTPS. Se non viene specificata alcuna porta, viene utilizzata la porta predefinita 443.

Per utilizzare l'istanza di vRealize Orchestrator predefinita incorporata nell'appliance vRealize Automation, immettere **https://vrealize-automation-appliance-hostname:443/vco**.

- 5 Immettere le credenziali di vRealize Orchestrator nelle caselle di testo **Nome utente** e **Password** per connettersi all'endpoint vRealize Orchestrator.

Le credenziali utilizzate devono disporre delle autorizzazioni di esecuzione per tutti i workflow di vRealize Orchestrator da richiamare da laaS.

Per utilizzare l'istanza di vRealize Orchestrator predefinita incorporata nell'appliance vRealize Automation, il nome utente è **administrator@vsphere.local** e la password è quella dell'amministratore specificata durante la configurazione di SSO.

- 6 Immettere un valore intero maggiore o uguale a 1 nella casella di testo **Priorità**.

Più basso è il valore, più alta è la priorità.

- 7 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.

- 8 Fare clic su **OK**.

Configurazione degli endpoint vRealize Orchestrator per il networking

Se si utilizzano workflow di vRealize Automation per chiamare i workflow di vRealize Orchestrator, è necessario configurare come endpoint l'istanza di vRealize Orchestrator o il server.

Per informazioni sull'aggiunta di un endpoint vRealize Orchestrator, vedere [Creazione di un endpoint vRealize Orchestrator](#).

È possibile associare un endpoint vRealize Orchestrator a un blueprint di macchine per assicurarsi che tutti i workflow di vRealize Orchestrator per le macchine fornite in provisioning da quel blueprint vengano eseguite utilizzando quell'endpoint.

Per impostazione predefinita, vRealize Automation include un'istanza di vRealize Orchestrator incorporata. È consigliabile utilizzare l'istanza incorporata come endpoint di vRealize Orchestrator per eseguire workflow di vRealize Automation in un ambiente di produzione o di test o quando si crea un ambiente di prototipazione.

È inoltre consigliabile utilizzare questo endpoint vRealize Orchestrator per eseguire workflow di vRealize Automation in un ambiente di produzione.

Il plug-in vRealize Orchestrator viene installato automaticamente con vRealize Orchestrator 7.1 e versioni successive. Non è necessario installare alcun plug-in vRealize Orchestrator separato.

Creazione di un endpoint vRealize Operations Manager

È possibile creare un endpoint vRealize Operations Manager per connettersi all'API suite di un host vRealize Operations Manager.

Per informazioni sulla convalida della connessione a vRealize Operations Manager e sull'attendibilità dei certificati, vedere [Considerazioni sull'utilizzo della prova della connessione](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Gestione > vRealize Operations Manager**.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Specificare l'URL del server di vRealize Operations Manager nella casella di testo **Indirizzo**.
L'URL deve essere nel formato: **https://nomehost/suite-api**.
- 5 Immettere le proprie credenziali di nome utente e password di vRealize Operations Manager.
- 6 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.
- 7 (Facoltativo) Per convalidare le credenziali, l'indirizzo dell'endpoint host e l'attendibilità del certificato, fare clic su **Prova connessione**. L'azione consente inoltre di verificare che il servizio e l'agente di gestione siano in esecuzione, in modo da consentire la raccolta dati nell'endpoint. L'azione **OK** consente di provare queste stesse condizioni.

L'azione **Prova connessione** restituisce informazioni relative a qualsiasi condizione seguente:

- Errore del certificato

Se non viene rilevato alcun certificato, oppure se questo non è attendibile o è scaduto, viene chiesto di accettare un'identificazione personale del certificato. Se non si accetta l'identificazione personale, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

- Errore dell'agente

L'agente di vSphere associato non viene rilevato. Per la buona riuscita della prova, è necessario che l'agente sia in esecuzione.

- Errore dell'host

L'indirizzo dell'endpoint specificato non è raggiungibile oppure il servizio di gestione associato non è in esecuzione. Per la buona riuscita della prova, è necessario che il servizio di gestione sia in esecuzione.

- Errore delle credenziali

La combinazione di nome utente e password specificata non è valida per l'endpoint nell'indirizzo specificato.

- Timeout

Non è stato possibile completare l'azione di prova nel periodo di tempo di due minuti consentito.

Se l'azione **Prova connessione** non riesce, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

Se si è verificato un problema di attendibilità del certificato, ad esempio se il certificato è scaduto, verrà chiesto di accettare un'identificazione personale del certificato.

8 Fare clic su **OK**.

Creazione di un endpoint di un provider IPAM di terze parti

Se è stato registrato e configurato un tipo di endpoint IPAM di terze parti in vRealize Orchestrator, è possibile creare un endpoint per quel provider di soluzioni IPAM in vRealize Automation.

Se è stato importato un pacchetto vRealize Orchestrator per fornire una soluzione IPAM esterna ed è stato registrato il tipo di endpoint IPAM in vRealize Orchestrator, è possibile selezionare il tipo di endpoint IPAM quando si crea un endpoint di vRealize Automation.

Nota Questo esempio si basa sull'uso del plug-in IPAM Infoblox, disponibile per il download in VMware Solution Exchange. È anche possibile utilizzare questa procedura se si è creato il proprio pacchetto del provider IPAM utilizzando l'SDK della soluzione IPAM fornita da VMware. La procedura per l'importazione e la configurazione del pacchetto di una soluzione IPAM di terze parti è identica a quella descritta nei prerequisiti.

Il primo endpoint IPAM per vRealize Automation viene creato quando si registra il tipo di endpoint per il plug-in del provider di soluzioni IPAM in vRealize Orchestrator.

Prerequisiti

- [Download e importazione di un pacchetto di un provider IPAM di terze parti in vRealize Orchestrator.](#)
- [Eseguire il workflow per registrare il tipo di endpoint IPAM di terze parti in vRealize Orchestrator.](#)
- Accedere a vRealize Automation come **amministratore laaS**.

Per questo esempio, creare un endpoint IPAM Infoblox utilizzando un tipo di endpoint registrato in vRealize Orchestrator per il plug-in o il pacchetto del provider IPAM di terze parti.

Procedura

1 Selezionare **Infrastruttura > Endpoint > Endpoint**.

2 Selezionare **Nuovo > IPAM > Tipo di endpoint IPAM**.

Selezionare un tipo di endpoint del provider IPAM esterno registrato come ad esempio Infoblox. Gli endpoint del provider IPAM esterno sono disponibili solo se è stato importato un pacchetto vRealize Orchestrator di terze parti e sono stati eseguiti i workflow del pacchetto per registrare il tipo di endpoint.

Per l'IPAM Infoblox, vengono elencati solo i tipi di endpoint IPAM principali. È possibile specificare tipi di endpoint IPAM secondari utilizzando le proprietà personalizzate.

Per questo esempio, selezionare un tipo di endpoint IPAM esterno registrato, ad esempio **Infoblox NIOS**.

3 Immettere un nome e, facoltativamente, una descrizione.

4 Inserire la posizione dell'endpoint IPAM registrato nella casella di testo **Indirizzo** utilizzando il formato dell'URL specifico del provider, ad esempio `https://host_name/name`.

Ad esempio, è possibile creare diversi endpoint IPAM, come `https://nsx62-scale-infoblox` e `https://nsx62-scale-infoblox2`, quando si registra il tipo di endpoint IPAM in vRealize Orchestrator. Inserire un tipo di endpoint registrato principale. Per specificare anche uno o più endpoint IPAM secondari, è possibile utilizzare proprietà personalizzate per emulare attributi estendibili che sono specifici del provider di soluzioni IPAM.

5 Per accedere all'account del provider di soluzioni IPAM, immettere il nome utente e la password richiesti.

Per creare, configurare e modificare l'endpoint quando si lavora in vRealize Automation, sono necessarie le credenziali dell'account del provider di soluzioni IPAM. vRealize Automation utilizza le credenziali dell'endpoint IPAM per comunicare con il tipo di endpoint specificato, ad esempio Infoblox, al fine di allocare gli indirizzi IP ed eseguire altre operazioni. Questo comportamento è simile al modo in cui vRealize Automation utilizza le credenziali dell'endpoint vSphere.

- 6** (Facoltativo) Fare clic su **Proprietà** e aggiungere proprietà dell'endpoint significative per il provider di soluzioni IPAM specifico.

Ciascun provider di soluzioni IPAM, ad esempio Infoblox e Bluecat, utilizza attributi estendibili univoci che l'utente può emulare usando le proprietà personalizzate vRealize Automation. Ad esempio, Infoblox utilizza attributi estendibili per distinguere gli endpoint principali e secondari.

- 7** Fare clic su **OK**.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint Microsoft Azure

È possibile creare un endpoint Microsoft Azure per facilitare una connessione con credenziali tra vRealize Automation e una distribuzione di Azure.

Un endpoint stabilisce una connessione a una risorsa, in questo caso un'istanza di Azure, che è possibile usare per creare blueprint di macchine virtuali. È necessario disporre di un endpoint Azure da utilizzare come base dei blueprint per eseguire il provisioning delle macchine virtuali Azure. Se si utilizzano più sottoscrizioni per Azure, è necessario creare un endpoint per ciascun ID sottoscrizione.

In alternativa, è possibile creare una connessione Azure direttamente da vRealize Orchestrator usando il comando **Aggiungi una connessione Azure** disponibile nell'albero del workflow **Libreria > Azure > Configurazione** di vRealize Orchestrator. Per la maggior parte degli scenari, la creazione di una connessione tramite la configurazione dell'endpoint, come descritto qui, è l'opzione preferita.

Gli endpoint Azure sono supportati da vRealize Orchestrator e dalla funzionalità XaaS. È possibile creare, eliminare o modificare endpoint Azure. Se si modifica un endpoint esistente e sono stati eseguiti aggiornamenti sul portale Azure tramite la connessione aggiornata per diverse ore, possono verificarsi problemi. È necessario riavviare il servizio vRealize Orchestrator utilizzando il comando `service vco-service restart`. Se il servizio non viene riavviato potrebbero verificarsi degli errori.

Prerequisiti

- Configurare un'istanza di Microsoft Azure e ottenere una sottoscrizione valida per Microsoft Azure dalla quale sia possibile utilizzare l'ID di sottoscrizione. Per ulteriori informazioni, sulla configurazione di Azure e su come ottenere un ID di sottoscrizione, vedere [Configurazione di endpoint di Microsoft Azure](#).
- Verificare che la distribuzione di vRealize Automation disponga di almeno un tenant e un gruppo di business.
- Creare un'applicazione Active Directory come indicato in <https://azure.microsoft.com/it-it/documentation/articles/resource-group-create-service-principal-portal>

- Prendere nota delle seguenti informazioni relative ad Azure, che saranno necessarie nel corso della configurazione dell'endpoint e del blueprint.
 - ID sottoscrizione
 - ID tenant
 - nome account storage
 - nome gruppo di risorse
 - posizione
 - nome rete virtuale
 - ID applicazione client
 - chiave privata applicazione client
 - URN immagine macchina virtuale
- L'implementazione di Azure di vRealize Automation supporta un sottoinsieme delle aree geografiche supportate da Microsoft Azure. Vedere [Aree geografiche supportate da Azure](#).
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Nella scheda Plug-in, fare clic sul menu a discesa **Plug-in** e selezionare **Azure**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.
- 7 Compilare le caselle di testo nella scheda Dettagli come opportuno per l'endpoint.

Parametro	Descrizione
Impostazioni di connessione	
Nome connessione	Nome univoco per la nuova connessione dell'endpoint. Questo nome viene visualizzato nell'interfaccia di vRealize Orchestrator per semplificare l'identificazione di una connessione particolare.
ID sottoscrizione Azure	L'identificatore per la sottoscrizione di Azure. L'ID definisce gli account di storage, le macchine virtuali e altre risorse Azure alle quali l'utente ha accesso.
Ambiente di Azure	La località geografica per la risorsa Azure distribuita. vRealize Automation supporta tutte le regioni di Azure correnti in base all'ID di sottoscrizione.
Impostazioni di Gestione risorse	

Parametro	Descrizione
URI servizio Azure	L'URI attraverso il quale si ottiene l'accesso alla propria istanza di Azure. Il valore predefinito <code>https://management.azure.com/</code> è appropriato per molte implementazioni tipiche. Questa casella viene popolata quando si seleziona un ambiente.
ID tenant	L'ID tenant di Azure che si desidera utilizzare per l'endpoint.
ID client	L'identificatore del client di Azure che si desidera utilizzare per l'endpoint. L'identificatore viene assegnato quando si crea un'applicazione Active Directory.
Segreto client	La chiave utilizzata con un ID client di Azure. La chiave viene assegnata quando si crea un'applicazione Active Directory.
URI storage Azure	L'URI che consente di accedere alla propria istanza dello storage di Azure. Questa casella viene popolata quando si seleziona un ambiente.
Impostazioni proxy	
Host proxy	Se l'azienda utilizza un server Web proxy, immettere il nome host del server.
Porta proxy	Se l'azienda utilizza un server Web proxy, immettere il numero della porta del server.

8 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate.

9 Fare clic su **Fine**.

Operazioni successive

Creare gruppi di risorse, account di storage e gruppi di sicurezza di rete in Azure. È inoltre consigliabile creare servizi di bilanciamento del carico, se appropriato per l'implementazione.

Azione	Opzioni
Creare un gruppo di risorse Azure	<ul style="list-style-type: none"> ■ Creare il gruppo di risorse utilizzando il portale Azure. Vedere la documentazione Azure per le istruzioni specifiche. ■ Utilizzare il workflow vRealize Orchestrator appropriato nel gruppo di risorse Library/Azure/Resource/Create. ■ In vRealize Automation, creare e pubblicare un blueprint XaaS che contenga il workflow di vRealize Orchestrator. È possibile richiedere il gruppo di risorse dopo averlo allegato al servizio e ai permessi. <hr/> <p>Nota Il tipo di risorsa Gruppo di risorse non è supportato né gestito da vRealize Automation.</p>
Creare un account di storage Azure	<ul style="list-style-type: none"> ■ Usare Azure per creare un account di storage. Vedere la documentazione Azure per le istruzioni specifiche. ■ Utilizzare il workflow vRealize Orchestrator appropriato nell'account di storage Library/Azure/Storage/Create. ■ In vRealize Automation, creare e pubblicare un blueprint XaaS che contenga il workflow di vRealize Orchestrator. È possibile richiedere l'account di storage dopo averlo allegato al servizio e ai permessi.
Creare un gruppo di sicurezza di rete Azure	<ul style="list-style-type: none"> ■ Utilizzare Azure per creare un gruppo di sicurezza. Vedere la documentazione Azure per le istruzioni specifiche. ■ Utilizzare il workflow vRealize Orchestrator appropriato nel gruppo di sicurezza di rete Library/Azure/Network/Create. ■ In vRealize Automation, creare e pubblicare un blueprint XaaS che contenga il workflow di vRealize Orchestrator. È possibile richiedere il gruppo di sicurezza dopo averlo allegato al servizio e ai permessi.

Configurazione di endpoint di Microsoft Azure

Per creare un endpoint di Microsoft Azure in vRealize Automation, è necessario raccogliere alcune informazioni ed eseguire alcune configurazioni.

Procedura

- 1 Individuare e registrare la sottoscrizione a Microsoft Azure e gli ID dei tenant.
 - ID sottoscrizione: fare clic sull'icona Sottoscrizioni sulla barra degli strumenti a sinistra nel portale di Azure per visualizzare l'ID della sottoscrizione.
 - ID tenant: fare clic sull'icona ? e selezionare Visualizza diagnostica nel portale di Azure. Cercare il tenant e registrare l'ID una volta individuato.

- 2** È possibile creare un nuovo account di storage e un gruppo di risorse per iniziare. In alternativa, è possibile crearli nei blueprint in un secondo momento.
- Account di storage: per configurare un account, utilizzare la procedura seguente.
 - 1 Nel portale di Azure, individuare l'icona Account di archiviazione nella barra laterale. Assicurarsi che sia selezionata la sottoscrizione corretta e fare clic su **Aggiungi**. È inoltre possibile cercare l'account di storage nel campo di ricerca di Azure.
 - 2 Immettere le informazioni richieste per l'account di storage. Sarà necessario l'ID della sottoscrizione.
 - 3 Scegliere se utilizzare un gruppo di risorse esistente o crearne uno nuovo. Prendere nota del nome del gruppo di risorse, poiché sarà necessario in un secondo momento.

Nota Salvare la posizione dell'account di storage perché sarà necessaria in un secondo momento.

- 3** Creare una rete virtuale. In alternativa, se si dispone di una rete esistente idonea, è possibile selezionarla.

Se si sta creando una rete, è necessario selezionare Usa un gruppo di risorse esistente e specificare il gruppo creato nel passaggio precedente. Selezionare inoltre la stessa posizione specificata in precedenza. Microsoft Azure non distribuirà macchine virtuali o altri oggetti se la posizione non coincide in tutti i componenti applicabili che l'oggetto utilizzerà.

- a Individuare l'icona Rete virtuale nel pannello sinistro e fare clic su tale icona oppure cercare una rete virtuale. Assicurarsi di selezionare la sottoscrizione corretta e fare clic su **Aggiungi**.
 - b Immettere un nome univoco per la nuova rete virtuale e registrarlo per riferimento successivo.
 - c Immettere l'indirizzo IP appropriato per la rete virtuale nel campo **Spazio indirizzi**.
 - d Assicurarsi che sia selezionata la sottoscrizione corretta e fare clic su **Aggiungi**.
 - e Immettere le informazioni di configurazione di base rimanenti.
 - f È possibile modificare le altre opzioni in base alle necessità, ma per la maggior parte delle configurazioni è consigliabile lasciare le impostazioni predefinite.
 - g Fare clic su **Crea**.
- 4** Configurare un'applicazione Active Directory di Azure in modo che vRealize Automation possa eseguire l'autenticazione.
- a Individuare l'icona di Active Directory nel menu a sinistra di Azure e fare clic su tale icona.
 - b Fare clic su **Registrazioni app** e selezionare **Aggiungi**.
 - c Digitare un nome per l'applicazione conforme alla convalida dei nomi di Azure.
 - d Lasciare App Web/API come tipo di applicazione.

- e L'URL di accesso può essere qualsiasi URL appropriato per l'utilizzo.
 - f Fare clic su **Crea**.
- 5** Creare una chiave segreta per eseguire l'autenticazione dell'applicazione in vRealize Automation.
- a Fare clic sul nome dell'applicazione in Azure.
Prendere nota dell'ID dell'applicazione per un uso successivo.
 - b Fare clic su **Tutte le impostazioni** nel riquadro successivo e selezionare Chiavi nell'elenco delle impostazioni.
 - c Immettere una descrizione per la nuova chiave e scegliere una durata.
 - d Fare clic su **Salva** e assicurarsi di copiare il valore della chiave in una posizione sicura, poiché non sarà possibile recuperarlo in un secondo momento.
 - e Nel menu a sinistra, selezionare **Autorizzazioni API** per l'applicazione e fare clic su **Aggiungi un'autorizzazione** per creare una nuova autorizzazione.
 - f Selezionare Gestione servizio Azure nella pagina Selezionare un'API.
 - g Fare clic su **Autorizzazioni delegate**.
 - h In Seleziona autorizzazioni, selezionare user_impersonation, quindi fare clic su **Aggiungi autorizzazioni**.
- 6** Autorizzare l'applicazione Active Directory per la connessione alla sottoscrizione di Azure in modo da poter distribuire e gestire le macchine virtuali.
- a Nel menu a sinistra, fare clic sull'icona Sottoscrizioni e selezionare la nuova sottoscrizione.
Potrebbe essere necessario fare clic sul testo del nome per far scorrere il pannello.
 - b Selezionare l'opzione Controllo di accesso (IAM) per visualizzare le autorizzazioni per la sottoscrizione.
 - c Fare clic su **Aggiungi** sotto l'intestazione Aggiungi assegnazione ruolo.
 - d Scegliere Collaboratore dal menu a discesa Ruolo.
 - e Lasciare la selezione predefinita nel menu a discesa Assegna accesso a.
 - f Digitare il nome dell'applicazione nella casella Seleziona.
 - g Fare clic su **Salva**.
 - h Aggiungere ulteriori ruoli in modo che la nuova applicazione disponga dei ruoli Proprietario, Collaboratore e Lettore.
 - i Fare clic su **Salva**.

Operazioni successive

È necessario installare gli strumenti dell'interfaccia della riga di comando di Microsoft Azure. Questi strumenti sono disponibili gratuitamente per i sistemi operativi Windows e Mac. Per ulteriori informazioni sul download e l'installazione di questi strumenti, vedere la documentazione di Microsoft.

Una volta installata l'interfaccia della riga di comando, è necessario eseguire l'autenticazione nella nuova sottoscrizione.

- 1 Aprire una finestra del terminale e digitare le credenziali di accesso di Microsoft Azure. Si riceveranno un URL e un codice breve che consentiranno di eseguire l'autenticazione.

- 2 In un browser, immettere il codice ricevuto dall'applicazione sul dispositivo.

- 3 Immettere il codice di autenticazione e fare clic su **Continua**.

- 4 Selezionare l'account e le credenziali di accesso di Azure.

Se si dispone di più sottoscrizioni, assicurarsi che sia selezionata quella corretta utilizzando il comando `azure account set <subscription-name>`.

- 5 Prima di procedere, è necessario registrare il provider Microsoft.Compute nella nuova sottoscrizione di Azure utilizzando il comando `azure provider register microsoft.compute`.

Se si verifica il timeout del comando e viene generato un errore la prima volta che il comando viene eseguito, eseguirlo di nuovo.

Una volta completata la configurazione, è possibile utilizzare il comando `azure vm image list` per recuperare i nomi delle immagini delle macchine virtuali disponibili. È possibile scegliere l'immagine desiderata e registrare l'URN fornito per utilizzarlo successivamente nei blueprint.

Creazione di un endpoint Puppet

È possibile creare un endpoint Puppet per consentire l'aggiunta di componenti di gestione della configurazione Puppet alle macchine virtuali vSphere. Questi componenti consentono di utilizzare un master Puppet per applicare la gestione della configurazione alle macchine virtuali.

Un endpoint stabilisce una connessione a una risorsa esterna, in questo caso un'istanza del master Puppet. L'endpoint consente di collocare i componenti di gestione della configurazione Puppet nei blueprint delle macchine virtuali vSphere. Le macchine virtuali con provisioning basate su questi blueprint contengono un agente Puppet che semplifica il controllo mediante il master Puppet associato.

Per ulteriori informazioni sul plug-in Puppet e una demo della relativa configurazione, vedere <https://www.youtube.com/watch?v=P-VglzE9o-o>.

Prerequisiti

- Installare e configurare la soluzione Puppet Enterprise appropriata al proprio ambiente.

- Scaricare e installare il plug-in Puppet 3.0 sulla distribuzione di vRealize Orchestrator in uso. È possibile scaricare il plug-in da <https://marketplace.vmware.com/vsx/solutions/puppet-plugin-for-vrealize-automation?ref=search>. Vedere https://docs.puppet.com/pe/latest/vro_intro.html per informazioni sull'installazione e l'utilizzo del plug-in.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Nella scheda Plug-in fare clic sul menu a discesa **Plug-in** e selezionare **Plug-in Puppet**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.
- 7 Compilare le caselle di testo nella scheda **Dettagli** come opportuno per l'endpoint.

Parametro	Descrizione
Nome visualizzato di questo master Puppet	Il nome del master Puppet associato alla connessione endpoint. Questo nome viene visualizzato nell'interfaccia di vRealize Orchestrator per semplificare l'identificazione di una connessione particolare.
Nome host o indirizzo IP	Il nome di dominio completo o l'indirizzo IP del master Puppet utilizzato da questo endpoint.
Porta SSH	La porta definita per l'uso con la comunicazione sicura di questo master Puppet.
Nome utente e RBAC SSH	Il nome utente del controllo dell'accesso basato su ruoli richiesto per connettersi con il master Puppet.
Password SSH e RBAC	Il nome utente del controllo dell'accesso basato su ruoli richiesto per la configurazione sicura con il master Puppet.
Usare Sudo per i comandi della shell su questo master?	Selezionare questa opzione se si desidera consentire agli amministratori l'uso dei comandi Sudo sui server Linux per le opzioni di sicurezza delle macchine virtuali basate su questo endpoint.

- 8 Fare clic su **OK**.

Risultati

È ora possibile aggiungere i componenti di gestione della configurazione Puppet ai blueprint vSphere in modo da poter distribuire le macchine virtuali vSphere che contengono agenti Puppet.

Creazione di un endpoint Ansible

È possibile creare un endpoint Ansible per consentire l'aggiunta di componenti di gestione della configurazione Ansible alle macchine virtuali vSphere. Questi componenti consentono di utilizzare una Ansible Tower per applicare la gestione della configurazione alle macchine virtuali.

Prerequisiti

- Installare e configurare una Ansible Tower appropriata per il proprio ambiente.
- Scaricare e installare il plug-in di Ansible nella distribuzione di vRealize Orchestrator. Il plug-in è disponibile presso <https://marketplace.vmware.com/vsx/solutions/sovlabs-ansible-tower-plugin-in-for-vra-cm-framework-1?ref=search>.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo**.
- 3 Nella scheda Plug-in, fare clic sul menu a discesa **Plug-in** e selezionare Plug-in Ansible.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione nella scheda Endpoint.
- 6 Fare clic su **Avanti**.
- 7 Compilare le caselle di testo nella pagina della scheda Dettagli nel modo appropriato per l'endpoint.

Pagina della scheda Dettagli	Descrizione
Configurazione dell'endpoint Ansible Tower	<p>Aggiungere informazioni relative alla configurazione dell'endpoint.</p> <ul style="list-style-type: none"> ■ Configurazione dell'endpoint Ansible Tower: immettere il nome e l'indirizzo IP o il nome host nelle caselle di testo corrispondenti. ■ Configurazione delle credenziali Ansible Tower: immettere le credenziali di accesso per il dispositivo Ansible Tower associato a questo endpoint. ■ Importazione del certificato SSL: selezionare se si desidera che il certificato di Ansible Tower venga accettato automaticamente da vRealize Orchestrator.
Accesso all'host Ansible Tower	Se applicabile, immettere le credenziali SSH per la macchina Ansible Tower in modo che una macchina distribuita possa connettersi a tale macchina e configurare uno script di inventario dinamico personalizzato.
Organizzazione e configurazione dell'inventario	Configurare il nome dell'organizzazione e l'inventario. Aggiungere i valori di configurazione dinamica dell'inventario.
Filtri e gruppi	Configurare i filtri delle proprietà delle coppie di valori delle chiavi e i gruppi dinamici Ansible.

Pagina della scheda Dettagli	Descrizione
Ignorare le richieste all'avvio (facoltativo)	Configurare le opzioni del processo Ansible, nonché le opzioni della macchina, del modello e dell'inventario.
Conversione delle proprietà di vRA	Se applicabile, immettere la stringa di sostituzione desiderata che Ansible deve usare durante l'elaborazione delle proprietà personalizzate dopo il provisioning.

8 Fare clic su **Fine**.

Creazione di un endpoint Hyper-V (SCVMM)

È possibile creare endpoint per consentire a vRealize Automation di comunicare con l'ambiente SCVMM, nonché trovare risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Per gestire l'endpoint Hyper-V (SCVMM) è necessario installare e configurare un agente DEM. Per ulteriori dettagli, vedere le informazioni sui requisiti di SCVMM in *Installazione di vRealize Automation*.

Per informazioni correlate, vedere [Preparazione dell'ambiente di SCVMM](#).

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Virtuale > Hyper-V (SCVMM)**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Immettere l'URL dell'endpoint nella casella di testo **Indirizzo**.
L'URL deve essere di tipo *FQDN* o *IP_address*.
Ad esempio `mycompany-scvmm1.mycompany.local`.
- 6 Immettere il nome utente e la password di livello amministrativo archiviati per questo endpoint.
Se le credenziali non sono state già memorizzate, è possibile farlo a questo punto.
- 7 (Facoltativo) Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.
- 8 Fare clic su **OK**.

Risultati

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint OpenStack

È possibile creare un endpoint per consentire a vRealize Automation di comunicare con l'istanza di OpenStack.

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Verificare che i DEM vRealize Automation siano installati in una macchina che soddisfa i requisiti OpenStack o PowerVC. Vedere *Installazione di vRealize Automation*.
- Verificare che la versione in uso di OpenStack sia attualmente supportata. Vedere *Matrice di supporto di vRealize Automation*.

Dopo aver eseguito l'aggiornamento o la migrazione da un'installazione precedente di vRealize Automation, se la raccolta dati non riesce per gli endpoint OpenStack è possibile aggiungere la proprietà personalizzata `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` a ogni endpoint Keystone V3 OpenStack per specificare un nome di dominio valido e abilitare la raccolta dati.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Cloud > OpenStack**.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Immettere l'URL dell'endpoint nella casella di testo **Indirizzo**.

Opzione	Descrizione
PowerVC	L'URL deve avere il formato http://myPowerVC.com:5000 o http://FQDN:5000 .
OpenStack	L'URL deve essere nel formato FQDN:5000 o IP_address:5000 . non includere il suffisso /v2.0 nell'indirizzo dell'endpoint.

- 5 Immettere il nome utente e la password di amministratore.

Le credenziali fornite devono corrispondere al ruolo di amministratore nel tenant OpenStack associato all'endpoint.

- 6 Specificare il nome di un tenant OpenStack nella casella di testo **Progetto OpenStack**.

Se si impostano più endpoint con tenant OpenStack differenti, creare criteri di prenotazione per ciascun tenant. Ciò garantisce il provisioning delle macchine alle risorse tenant appropriate.

- 7 Fare clic su **Proprietà** e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate per l'endpoint.

Se è utilizzato Keystone V3, aggiungere la proprietà personalizzata

`VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` per designare un dominio specifico.

- 8 Fare clic su **OK**.

Risultati

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Creazione di un endpoint Hyper-V, XenServer o di pool Xen

È possibile creare endpoint per consentire a vRealize Automation di comunicare con l'ambiente principale di Hyper-V, XenServer o pool Xen, nonché trovare risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Un amministratore di sistema deve installare un agente proxy con credenziali memorizzate che corrispondono all'endpoint. Vedere *Installazione di vRealize Automation*.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Agenti**.
- 2 Nella casella di testo **Risorsa di elaborazione** specificare il nome DNS completo del server Hyper-V, di XenServer o del pool principale Xen.

Nota Per un endpoint del pool Xen, è necessario immettere il nome del pool principale. Per evitare voci duplicate nella tabella delle risorse di elaborazione di vRealize Automation, specificare un indirizzo che corrisponda a quello principale del pool Xen configurato. Ad esempio, se l'indirizzo principale del pool Xen utilizza il nome dell'host, immettere quest'ultimo e non il nome di dominio completo (FQDN). Se l'indirizzo principale del pool Xen utilizza FQDN, immettere lo stesso nome completo.

- 3 Selezionare l'agente proxy che l'amministratore di sistema ha installato per questo endpoint dal menu a discesa **Nome agente proxy**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Fare clic su **OK**.

Risultati

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Operazioni successive

Aggiungere le risorse di elaborazione dall'endpoint a un gruppo di strutture. Vedere [Creazione di un gruppo di strutture](#).

Considerazioni sull'utilizzo della prova della connessione

È possibile utilizzare l'azione di prova della connessione per convalidare le credenziali, l'indirizzo endpoint dell'host e il certificato per un endpoint vSphere, NSX for vSphere, NSX-T o vRealize Operations Manager.

L'azione consente inoltre di verificare che il servizio e l'agente di gestione siano in esecuzione, in modo da consentire la raccolta dati nell'endpoint.

L'azione **Prova connessione** restituisce informazioni relative a qualsiasi condizione seguente:

- Errore del certificato

Se non viene rilevato alcun certificato, oppure se questo non è attendibile o è scaduto, viene chiesto di accettare un'identificazione personale del certificato. Se non si accetta l'identificazione personale, è ancora possibile salvare l'endpoint ma il provisioning della macchina potrebbe non riuscire.

- Errore dell'agente

L'agente di vSphere associato non viene rilevato. Per la buona riuscita della prova, è necessario che l'agente sia in esecuzione.

- Errore dell'host

L'indirizzo dell'endpoint specificato non è raggiungibile oppure il servizio di gestione associato non è in esecuzione. Per la buona riuscita della prova, è necessario che il servizio di gestione sia in esecuzione.

- Errore delle credenziali

La combinazione di nome utente e password specificata non è valida per l'endpoint nell'indirizzo specificato.

- Timeout

Non è stato possibile completare l'azione di prova nel periodo di tempo di due minuti consentito.

Se si ricevono errori durante l'esecuzione di **Prova connessione** su endpoint aggiornati o migrati, vedere [Considerazioni sull'utilizzo di endpoint aggiornati o migrati](#) per la procedura da eseguire per implementare l'attendibilità del certificato.

Importazione o esportazione di endpoint a livello di programmazione

Per impostare ed esportare endpoint tramite programma in vRealize Automation 7.3 o versione successiva, è necessario utilizzare le nuove API REST endpoint-configuration-service di vRealize Automation oppure utilizzare vRealize CloudClient.

La documentazione di vRealize CloudClient contiene tutte le formattazioni della riga di comando applicabili, esempi e informazioni di utilizzo.

È possibile scaricare l'applicazione vRealize CloudClient e la documentazione dalla pagina del prodotto vRealize CloudClient di <https://developercenter.vmware.com/tool/cloudclient>.

Visualizzazione delle risorse di elaborazione ed esecuzione della raccolta dati

È possibile visualizzare la risorsa macchina e di elaborazione associata a un endpoint specifico. È possibile inoltre avviare manualmente la raccolta dati.

Prerequisiti

Verificare che esista almeno un endpoint.

Procedura

1 Selezionare **Infrastruttura > Endpoint > Endpoint**.

Gli utenti che non dispongono di privilegi di amministratore IaaS, possono selezionare **Infrastruttura > Risorse di elaborazione > Risorse di elaborazione** per visualizzare le risorse ed eseguire la raccolta dati dalla risorsa di elaborazione.

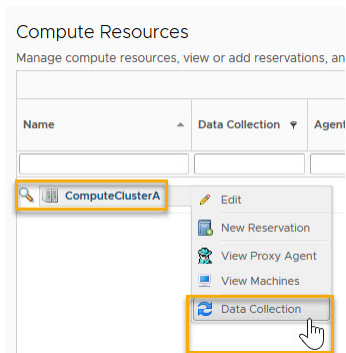
2 Selezionare **Infrastruttura > Endpoint > Endpoint**.

3 Selezionare una riga dell'endpoint esistente e fare clic su **Azioni**.

Selezionare una delle seguenti azioni disponibili.

- Fare clic su **Visualizza risorse di elaborazione** per aprire la pagina **Infrastruttura > Risorsa di elaborazione**. In questa pagina è possibile visualizzare e modificare le impostazioni della risorsa di elaborazione. È inoltre possibile eseguire la raccolta dati per una risorsa di elaborazione selezionata dalla pagina **Risorse di elaborazione**.
- Fare clic su **Visualizza macchine** per aprire la pagina **Infrastruttura > Macchine gestite**.
- Fare clic su **Raccolta dati** per aprire la pagina Raccolta dati e avviare la raccolta dati per l'endpoint. È possibile aggiornare la pagina per visualizzare lo stato corrente della richiesta.

È possibile eseguire la raccolta dati da una risorsa di elaborazione associata dell'endpoint. Ad esempio, per raccogliere dati in un endpoint di NSX-T esistente, utilizzare **Infrastruttura > Risorse di elaborazione > Risorse di elaborazione** per visualizzare le risorse, quindi fare clic su **Raccolta dati** per aprire la pagina **Raccolta dati** per la risorsa di elaborazione. Trovare l'endpoint desiderato nell'elenco e fare clic su **Richiedi ora**.



Considerazioni sull'utilizzo di endpoint aggiornati o migrati

Dopo aver eseguito un aggiornamento o una migrazione da una versione precedente di vRealize Automation 7.3, è importante comprendere le considerazioni seguenti e agire di conseguenza.

Queste informazioni si applicano agli endpoint che sono stati aggiornati o migrati a questa versione di vRealize Automation.

- Quando si effettua l'aggiornamento o la migrazione da una release precedente a vRealize Automation 7.3, ogni endpoint vCloud Air, vCloud Director e Amazon che include impostazioni del proxy viene associato a un nuovo endpoint Proxy che include le impostazioni del proxy corrispondenti.

Dopo l'aggiornamento o la migrazione, il nuovo nome dell'endpoint Proxy sarà Proxy_YYYYYY, dove YYYYYY è un hash dell'URL, della porta e delle credenziali del proxy. Se si utilizzano le stesse impostazioni del proxy (ad esempio l'URL, la porta e le credenziali) per un endpoint diverso (ad esempio un endpoint vCloud Air o Amazon), dopo l'aggiornamento o la migrazione saranno presenti un solo endpoint Proxy e un'associazione tra l'endpoint vCloud Air o Amazon e il nuovo endpoint Proxy. Un endpoint Proxy può essere associato a più endpoint Amazon, vCloud Air o vCloud Director.

- Quando si effettua l'aggiornamento o la migrazione degli endpoint vSphere che includono impostazioni del manager NSX, ogni endpoint vSphere viene associato a un nuovo endpoint NSX che include le impostazioni del manager NSX corrispondenti.

Dopo l'aggiornamento o la migrazione, il nome dell'endpoint NSX sarà NSX_XXXXX, dove XXXXX è il nome dell'endpoint vSphere padre nella release precedente a vRealize Automation 7.3.

- Al termine dell'aggiornamento o della migrazione di vRealize Automation, un amministratore dell'infrastruttura può modificare i nuovi nomi degli endpoint NSX e Proxy.
- L'impostazione di sicurezza predefinita per gli endpoint aggiornati o migrati prevede che i certificati non attendibili non vengano accettati.
- Dopo l'aggiornamento o la migrazione da un'installazione precedente di vRealize Automation, se venivano utilizzati certificati non attendibili, è necessario eseguire la procedura che segue per tutti gli endpoint vSphere e NSX per consentire la convalida dei certificati. In caso contrario, le operazioni sugli endpoint non riusciranno e verranno restituiti errori di certificato. Per ulteriori informazioni, vedere gli articoli della Knowledge Base di VMware *Endpoint*

communication is broken after upgrade to vRA 7.3 (2150230) all'indirizzo <http://kb.vmware.com/kb/2150230> e *How to download and install vCenter Server root certificates to avoid Web Browser certificate warnings (2108294)* all'indirizzo <http://kb.vmware.com/kb/2108294>.

- a Dopo l'aggiornamento o la migrazione, accedere alla macchina dell'agente vRealize AutomationvSphere e riavviare gli agenti vSphere utilizzando la scheda **Servizi**.

La migrazione potrebbe non riavviare tutti gli agenti, pertanto è necessario riavviarli manualmente se richiesto.
- b Attendere il completamento di almeno un report di ping. Questa operazione richiede uno o due minuti.
- c Dopo che gli agenti vSphere avranno avviato la raccolta dati, accedere a vRealize Automation come amministratore laaS.
- d Fare clic su **Infrastruttura > Endpoint > Endpoint**.
- e Modificare un endpoint vSphere e fare clic su **Prova connessione**.
- f Se viene visualizzato un prompt sul certificato, fare clic su **OK** per accettare il certificato.

In caso contrario, è possibile che al momento il certificato sia correttamente archiviato presso un'autorità root attendibile del servizio di hosting della macchina Windows per l'endpoint, ad esempio come macchina agente proxy o come macchina DEM.
- g Per accettare il certificato e salvare l'endpoint, fare clic su **OK**.
- h Ripetere questa procedura per ogni endpoint vSphere.
- i Ripetere questa procedura per ogni endpoint NSX.
- j Passare a **Infrastruttura > Risorse di elaborazione**, fare clic con il pulsante destro del mouse sulla **risorsa di elaborazione vCenter** ed eseguire **Raccolta dati**.

Se l'azione **Prova connessione** riesce ma alcune operazioni di provisioning o di raccolta dati hanno esito negativo, è possibile installare lo stesso certificato in tutte le macchine agente che servono l'endpoint e su tutte le macchine DEM. In alternativa, è possibile disinstallare il certificato dalle macchine esistenti e ripetere la procedura precedente per l'endpoint in cui si verifica l'errore.

- Le API REST di vRealize Automation utilizzate per creare, modificare ed eliminare gli endpoint a livello di programmazione in vRealize Automation 7.2 e versioni precedenti non sono più supportate in vRealize Automation 7.3 e versioni successive. Per creare, modificare ed eliminare gli endpoint a livello di programmazione in vRealize Automation 7.3 o versioni successive, è necessario utilizzare le nuove API REST del servizio di configurazione degli endpoint vRealize Automation oppure vRealize CloudClient.

- Dopo aver eseguito l'aggiornamento o la migrazione da un'installazione precedente di vRealize Automation, se la raccolta dati non riesce per gli endpoint OpenStack è possibile aggiungere la proprietà personalizzata `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` a ogni endpoint Keystone V3 OpenStack per specificare un nome di dominio valido e abilitare la raccolta dati.
- Quando si effettua l'aggiornamento di un endpoint IPAM di terze parti, ad esempio Infoblox IPAM, viene aggiornato il pacchetto di vRealize Orchestrator contenente il workflow `RegisterIPAMEndpoint`. Potrebbe essere necessario eseguire nuovamente il workflow in vRealize Orchestrator al termine dell'aggiornamento di vRealize Automation.
- Per modificare le credenziali per più endpoint, è possibile modificare gli endpoint singolarmente o utilizzare vRealize CloudClient per eseguire un aggiornamento di massa.
- Alcuni tipi di endpoint, ad esempio vCloud Air e vCloud Director, non possono essere aggiornati o migrati direttamente da vRealize Automation 6.2.x a vRealize Automation 7.3 o versioni successive.
- Una volta effettuato correttamente l'aggiornamento o la migrazione a vRealize Automation 7.3, se nella pagina **Infrastruttura > Endpoint** non viene visualizzato alcun endpoint o vengono visualizzati solo alcuni tipi di endpoint ed endpoint, vedere l'[articolo 2150252 della Knowledge Base](#) per applicare una soluzione suggerita.

Considerazioni sull'eliminazione degli endpoint

In determinate condizioni è possibile eliminare alcuni tipi di endpoint.

- È possibile eliminare gli endpoint non inclusi nella raccolta dati.
- È possibile eliminare un endpoint OpenStack, Amazon e VRO se è stato incluso nella raccolta dati ma non presenta prenotazioni. Altri tipi di endpoint non possono essere eliminati se sono stati inclusi nella raccolta dati.
- È possibile eliminare un endpoint IPAM di terze parti se non presenta alcuna associazione a un profilo di rete.
- Quando si elimina un endpoint vSphere, il prompt di conferma elenca le seguenti dipendenze:
 - È stata effettuata la raccolta dei dati nell'endpoint.
 - Esiste un riferimento all'endpoint in una prenotazione mappata a una risorsa di elaborazione. Non è possibile eliminare un endpoint se si fa riferimento a esso in una prenotazione. Le prenotazioni richiedono una risorsa di elaborazione.
 - L'endpoint contiene un modello a cui viene fatto riferimento in un blueprint esistente. Il blueprint non viene eliminato quando si elimina l'endpoint.
 - L'endpoint viene utilizzato dalle macchine virtuali in uso.

- È possibile eliminare gli endpoint tramite programma utilizzando le nuove API REST endpoint-configuration-service di vRealize Automation CREATE, EDIT e DELETE introdotte in vRealize Automation 7.3 o utilizzando vRealize CloudClient. Non è possibile eliminare gli endpoint utilizzando API REST endpoint-configuration-service precedenti a vRealize Automation 7.3.

Risoluzione dei messaggi di errore che attestano l'impossibilità di trovare l'endpoint vSphere collegato

Quando la raccolta dati non viene eseguita correttamente per un endpoint vSphere, il motivo potrebbe essere la mancata corrispondenza tra il nome del proxy e il nome dell'endpoint.

Problema

È impossibile completare la raccolta dati per un endpoint vSphere. I messaggi del registro restituiscono un errore simile al seguente:

```
Rilevata eccezione: impossibile trovare l'endpoint 'vCenter' allegato.
```

Causa

Il nome dell'endpoint configurato in vRealize Automation deve corrispondere al nome dell'endpoint fornito all'agente proxy di vSphere durante l'installazione. La raccolta dati per un endpoint vSphere non riesce se il nome del proxy e il nome dell'endpoint non coincidono. Finché non viene configurato un endpoint con un nome corrispondente, i messaggi del registro restituiscono un errore simile al seguente:

```
Rilevata eccezione: impossibile trovare l'endpoint allegato 'nome endpoint previsto'.
```

Soluzione

- 1 Selezionare **Infrastruttura > Monitoraggio > Registro**.
- 2 Cercare un messaggio di errore che indichi che non è possibile trovare l'endpoint collegato.

Ad esempio,

```
Rilevata eccezione: impossibile trovare l'endpoint allegato 'nome endpoint previsto'.
```

- 3 Modificare l'endpoint vSphere affinché nel messaggio del registro compaia il nome dell'endpoint previsto.
 - a Selezionare **Infrastruttura > Endpoint > Endpoint**.
 - b Fare clic sul nome dell'endpoint da modificare.
 - c Immettere il nome dell'endpoint previsto nella casella di testo **Nome**.
 - d Fare clic su **OK**.

Soluzione

L'agente proxy può comunicare con l'endpoint e la raccolta dati viene completata correttamente.

Creazione di un gruppo di strutture

È possibile organizzare le risorse dell'infrastruttura in gruppi di strutture e assegnare uno o più amministratori di struttura per gestire le risorse contenute nel gruppo di strutture.

I gruppi di strutture sono necessari per gli endpoint virtuali e cloud. È possibile assegnare il ruolo di amministratore di struttura a più utenti aggiungendoli uno alla volta o scegliendo un gruppo archivio identità o un gruppo personalizzato come amministratore di struttura.

Prerequisiti

- Accedere a vRealize Automation come **amministratore IaaS**.
- Creare almeno un endpoint. Vedere [Scelta dello scenario per un endpoint](#).

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Gruppi di strutture**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Immettere un nome utente o un indirizzo email dell'utente nella casella di testo **Amministratori di struttura**, fare clic sull'icona Cerca e selezionare l'indirizzo email dell'utente fornito.

Ripetere questo passaggio per aggiungere più utenti.
- 6 Selezionare una o più **Risorse di elaborazione** da includere nel gruppo di strutture.

Nel corso della raccolta dati vengono rilevate solo le risorse esistenti nei cluster selezionati per il proprio gruppo di strutture. Ad esempio, vengono rilevati solo i modelli esistenti nei cluster selezionati e disponibili per la clonazione nelle prenotazioni create per i gruppi di business.
- 7 Fare clic su **OK**.

Risultati

Gli amministratori di struttura a questo punto possono configurare i prefissi macchina. Vedere [Configurazione dei prefissi macchina](#).

Gli utenti che sono attualmente connessi a vRealize Automation devono disconnettersi e riaccedere a vRealize Automation per poter visualizzare le pagine per cui hanno ricevuto le autorizzazioni di accesso.

Configurazione dei prefissi macchina

È possibile utilizzare i prefissi macchina impiegati per creare i nomi delle macchine con provisioning effettuato tramite vRealize Automation. Quando si definisce un componente macchina nella tela di progettazione del blueprint è richiesto un prefisso macchina.

Un prefisso è il nome di base che deve essere seguito dal contatore di uno specifico numero di cifre. Quando sono state utilizzate tutte le cifre, vRealize Automation riparte dal primo numero.

I prefissi macchina devono rispettare le seguenti limitazioni:

- Contenere solo lettere ASCII dalla a alla z, sia maiuscole che minuscole, numeri da 0 a 9 e il carattere trattino (-).
- Iniziare con un carattere diverso dal trattino.
- Non utilizzare altri simboli, caratteri di punteggiatura o spazio vuoti.
- Contenere non più di 15 caratteri, inclusi i numeri, per rispettare il limite di Windows dei 15 caratteri per i nomi host.

Eventuali nomi host più lunghi vengono troncati al momento del provisioning della macchina e aggiornati alla successiva esecuzione della raccolta dati. Quando viene eseguito un provisioning WIM, però, se un nome supera la limitazione dei 15 caratteri non viene troncato e il provisioning non riesce.

- vRealize Automation non supporta macchine virtuali multiple con lo stesso nome in una singola istanza. Se le caratteristiche della convenzione di denominazione scelta sono tali da causare la presenza di due nomi macchina uguali, vRealize Automation non eseguirà il provisioning di una macchina con un nome già esistente. Se possibile, vRealize Automation salta il nome già in uso e genera un nuovo nome di macchina utilizzando il prefisso macchina specificato. Se non è possibile generare un nome univoco, il provisioning non riesce.

Prerequisiti

Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Fare clic su **Infrastruttura > Amministrazione > Prefissi macchina**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere il prefisso macchina nella casella di testo **Nome**.
- 4 Specificare se il prefisso macchina deve essere visualizzato in tutti i tenant o solo nel tenant corrente nella colonna **Visibilità**.
- 5 Immettere il numero di cifre del prefisso macchina nella casella di testo **Numero di cifre**.
- 6 Immettere il numero iniziale del contatore nella casella di testo **Numero successivo**.
- 7 Fare clic sull'icona **Salva** (✓).

Risultati

Gli amministratori tenant possono creare gruppi di business per consentire agli utenti di accedere a vRealize Automation per richiedere macchine.

Creazione di un profilo di rete in vRealize Automation

Un profilo di rete contiene informazioni IP come gateway, subnet e intervallo di indirizzi. vRealize Automation utilizza DHCP vSphere o un provider IPAM specificato per assegnare indirizzi IP alle macchine di cui esegue il provisioning in base alle impostazioni del profilo di rete.

È possibile creare un profilo di rete per definire un tipo di rete disponibile. È possibile creare modelli e profili di rete esterna per profili Network Address Translation (NAT) su richiesta e profili di rete instradata o privata. I profili possono creare switch logici NSX e impostazioni di routing appropriate per un percorso di rete.

I profili di rete vengono usati per configurare le impostazioni di rete durante il provisioning delle macchine. I profili di rete specificano anche la configurazione dei dispositivi NSX Edge che vengono creati durante il provisioning delle macchine.

Tipi di rete disponibili

Quando si definisce un profilo di rete, sono disponibili i seguenti tipi di rete:

- Rete esistente
- Rete instradata su richiesta
- Rete NAT su richiesta
- Rete privata su richiesta (solo NSX for vSphere)

Tabella 2-14. Tipi di reti disponibili per un profilo di rete di vRealize Automation

Tipo di rete	Descrizione
Esterna	<p>Rete esistente configurata sul server vSphere. Le reti di questo tipo rappresentano la parte esterna dei tipi di rete NAT e instradate. Un profilo di rete esterna può definire un intervallo di indirizzi IP statici disponibile sulla rete esterna.</p> <p>È possibile utilizzare gli intervalli di indirizzi IP ricavati dall'endpoint IPAM di VMware specificato o da un endpoint del provider di servizi IPAM di terze parti registrato e configurato in vRealize Orchestrator, ad esempio Infoblox IPAM. Durante l'allocazione, viene creato un intervallo di indirizzi IP da un blocco IP.</p> <p>Un profilo di rete esterna con un intervallo di IP statici è un prerequisito per le reti NAT e instradate. Vedere Creazione di un profilo di rete esterna per una rete esistente.</p>
NAT	<p>Rete su richiesta creata durante il provisioning. Si tratta di reti NAT che utilizzano un set di indirizzi IP per le comunicazioni esterne e un altro set per le comunicazioni interne.</p> <p>Con le reti NAT One-to-One, a ogni macchina virtuale viene assegnato un indirizzo IP esterno prelevato dal profilo di rete esterna e un indirizzo IP interno prelevato dal profilo di rete NAT. Con le reti NAT One-to-Many, tutte le macchine condividono un singolo indirizzo IP prelevato dal profilo di rete esterna per la comunicazione esterna.</p> <p>È possibile utilizzare gli intervalli di indirizzi IP ricavati dall'endpoint IPAM di VMware specificato o da un endpoint del provider di servizi IPAM di terze parti registrato e configurato in vRealize Orchestrator, ad esempio Infoblox IPAM. Durante l'allocazione, viene creato un intervallo di indirizzi IP da un blocco IP.</p> <p>Un profilo di rete NAT definisce una rete locale e una esterna che utilizzano una tabella di traduzione per comunicare tra loro.</p> <p>Vedere Creazione di un profilo di rete NAT per una rete su richiesta.</p>

Tabella 2-14. Tipi di reti disponibili per un profilo di rete di vRealize Automation (continua)

Tipo di rete	Descrizione
Instradato	<p>Rete su richiesta creata durante il provisioning. Le reti instradate contengono uno spazio degli indirizzi IP instradabili suddiviso tra subnet collegate tra loro tramite un DLR (Distributed Logical Router).</p> <p>A ogni nuova rete instradata viene assegnata la subnet disponibile successiva e le vengono associate altre reti instradate che utilizzano lo stesso profilo di rete. Le macchine virtuali di cui viene eseguito il provisioning con reti instradate aventi lo stesso profilo di rete instradata possono comunicare tra loro e con la rete esterna.</p> <p>È possibile utilizzare gli intervalli di indirizzi IP ricavati dall'endpoint IPAM di VMware specificato o da un endpoint del provider di servizi IPAM di terze parti registrato e configurato in vRealize Orchestrator, ad esempio Infoblox IPAM. Durante l'allocazione, viene creato un intervallo di indirizzi IP da un blocco IP.</p> <p>Un profilo di rete instradata definisce uno spazio instradabile e le subnet disponibili.</p> <p>Vedere Creazione di un profilo di rete instradata per una rete su richiesta.</p>
Privato (Solo NSX for vSphere)	<p>Rete su richiesta creata durante il provisioning. Questa opzione è disponibile solo per NSX for vSphere. Questa opzione non è disponibile per NSX-T.</p> <p>Le reti private includono le seguenti considerazioni:</p> <ul style="list-style-type: none"> ■ Le reti private non dispongono di connettività in entrata o in uscita. Non viene eseguito il provisioning di un edge per le reti private. ■ È possibile creare un profilo di rete privata con o senza indirizzi IP statici o intervalli. DHCP e IPAM di terze parti non sono supportati per le reti private. <p>Vedere Creazione di un profilo di rete privata per una rete su richiesta in vRealize Automation.</p>

Per informazioni relative a NSX sulla rete, vedere la [documentazione di VMware NSX Data Center for vSphere](#) e la [documentazione di VMware NSX-T Data Center](#).

Per informazioni correlate alla configurazione di rete e sicurezza per NSX-T in vRealize Automation, vedere il blog VMware [Networking e sicurezza dell'applicazione con vRealize Automation e NSX-T](#).

Utilizzo di IPAM fornito o di terze parti

I profili di rete supportano anche provider IPAM (IP Address Management) di terze parti come Infoblox. Quando si configura un profilo di rete per IPAM, le macchine con provisioning possono ottenere dalla soluzione IPAM configurata i dati dei loro indirizzi IP e le informazioni correlate, quali DNS e gateway. È possibile utilizzare un pacchetto IPAM esterno per un provider di terze parti, come Infoblox, per definire un endpoint IPAM da utilizzare con un profilo di rete.

Nota Se si utilizza un provider IPAM di terze parti e si desidera specificare in quale rete distribuire la macchina, usare un profilo di rete separato per ciascuna rete VLAN per evitare il problema noto descritto nell'[articolo 2148656 della Knowledge Base](#).

Se invece di un provider IPAM di terze parti si utilizza l'endpoint IPAM fornito con vRealize Automation, è possibile specificare gli intervalli di indirizzi IP utilizzabili dai profili di rete. Tutti gli indirizzi IP appartenenti agli intervalli specificati e allocati per le macchine verranno recuperati per poter essere riassegnati quando le macchine verranno eliminate. È possibile creare un profilo di

rete per definire un intervallo di indirizzi IP statici che possono essere assegnati alle macchine. Quando viene eseguito il provisioning di macchine virtuali clonando o utilizzando il provisioning kickstart/autoYaST, il proprietario della macchina richiesta può assegnare indirizzi IP statici appartenenti a un intervallo predeterminato.

Definizione di un profilo di rete in una prenotazione o in un blueprint

Quando si creano prenotazioni e blueprint, è possibile specificare un profilo di rete. In una prenotazione, è possibile assegnare un profilo di rete a un percorso di rete e specificare uno o più di questi percorsi per un componente macchina in un blueprint. È possibile assegnare profili di rete a percorsi di rete specifici su una prenotazione. Per alcuni tipi di componenti delle macchine, come ad esempio vSphere, è possibile assegnare un profilo di rete quando si creano o modificano blueprint.

È possibile utilizzare un profilo di rete esistente e un profilo di rete su richiesta durante la definizione delle schede di rete e dei bilanciamenti del carico per una macchina vSphere.

Se viene specificato un profilo di rete in una prenotazione e un blueprint, i valori del blueprint hanno la precedenza.

Applicazione di modifiche dopo la distribuzione del blueprint

Anche se non è possibile modificare il profilo di rete di una macchina virtuale distribuita, è possibile modificare la rete a cui la macchina virtuale è connessa. Se la rete è associata a un profilo di rete diverso, vRealize Automation assegna alla macchina virtuale un indirizzo IP di tale profilo di rete. La macchina virtuale continua a utilizzare l'indirizzo IP precedente finché non si aggiorna l'indirizzo IP nel sistema operativo guest. Se si utilizza l'azione Riconfigura nella macchina virtuale distribuita, è necessario aggiornare l'indirizzo IP nel sistema operativo guest.

Utilizzo dei profili di rete per controllare gli intervalli di indirizzi IP

È possibile utilizzare i profili di rete per assegnare gli indirizzi IP statici di un intervallo predefinito a macchine virtuali fornite in provisioning tramite clonazione, tramite Linux Kickstart o autoYaST, oppure a macchine cloud che sono state fornite in provisioning in OpenStack tramite Kickstart.

Per impostazione predefinita, vRealize Automation utilizza il protocollo DHCP (Dynamic Host Configuration Protocol) per assegnare indirizzi IP alle macchine di cui è stato eseguito il provisioning.

È possibile creare profili di rete per definire un intervallo di indirizzi IP statici che possono essere assegnati alle macchine. È possibile assegnare profili di rete a percorsi di rete specifici su una prenotazione. Per le macchine il cui provisioning avviene mediante clonazione, Kickstart o autoYaST e che sono allegate a un percorso di rete con un profilo di rete associato, il provisioning viene effettuato con un indirizzo IP statico assegnato. Per il provisioning con un'assegnazione di indirizzo IP statico, è necessario utilizzare una specifica di personalizzazione.

È possibile assegnare un profilo di rete a un componente macchina di vSphere in un blueprint aggiungendo un componente di rete esistente NAT su richiesta o di rete instradata su richiesta alla tela di progettazione, nonché selezionando un profilo di rete a cui collegare il componente macchina di vSphere. È possibile assegnare anche profili di rete ai blueprint utilizzando la proprietà personalizzata `VirtualMachine.NetworkN.ProfileName`, dove *N* è l'identificatore di rete.

Facoltativamente, è possibile utilizzare l'IPAM vRealize Automation fornito o un endpoint di provider di servizi IPAM di terze parti registrato e configurato nel profilo di rete per ottenere e configurare gli indirizzi IP. Per informazioni sui requisiti per IPAM esterni, vedere [Elenco di controllo per fornire il supporto del provider IPAM di terze parti](#).

Quando si seleziona un endpoint di provider di servizi IPAM di terze parti in un profilo di rete, vRealize Automation recupera gli intervalli IP dall'endpoint del provider IPAM esterno registrato, ad esempio Infoblox. Alloca quindi i valori IP a partire da tale endpoint. La subnet mask dell'intervallo specificato viene utilizzata per allocare subnet dal blocco IP.

Se viene specificato un profilo di rete in una prenotazione e un blueprint, i valori del blueprint hanno la precedenza.

Informazioni sul formato di file CSV per l'importazione degli indirizzi IP del profilo di rete

È possibile importare gli intervalli di rete degli indirizzi IP in un profilo di rete di vRealize Automation utilizzando un file CSV formattato correttamente.

Le voci dei file CSV devono rispettare il seguente formato.

Campo CSV	Descrizione
ip_address	Un indirizzo IP in formato IPv4.
machine_name	Nome di una macchina gestita in vRealize Automation. Se il campo è vuoto, il valore predefinito è senza nome. Se il campo è vuoto, il valore del campo status non può essere Allocated.
status	Allocato o Non allocato, viene fatta distinzione tra lettere maiuscole e minuscole. Se il campo è vuoto, il valore predefinito è Non allocato. Se lo stato è Allocated, il campo machine_name non può essere vuoto.
NIC_offset	Un numero intero non negativo. Lo scarto NIC indica la NIC della macchina virtuale a cui è assegnato l'indirizzo IP. Se una macchina virtuale alloca più indirizzi IP per NIC diverse, è presente una voce di indirizzo IP per ogni NIC che contiene lo scarto NIC corrispondente. Se si imposta il valore 0, non viene specificato alcuno scarto.

La voce di esempio seguente mostra l'indirizzo IP 100.10.100.1 di una macchina, il nome mymachine01, lo stato allocato e nessun scarto NIC.

```
100.10.100.1,mymachine01,Unallocated,0
```

Scenario: Importazione degli indirizzi IP in un profilo di rete da un file CSV

È possibile aggiungere indirizzi IP in un intervallo di profili di rete mediante l'importazione di un file CSV formattato correttamente. È anche possibile modificare gli indirizzi nell'intervallo di profili di rete modificando l'intervallo in vRealize Automation oppure importando un file CSV modificato o diverso.

È possibile aggiungere o modificare gli indirizzi IP in un intervallo di profili di rete mediante l'importazione da un file CSV o l'immissione manuale dei valori. In alternativa, è possibile consentire a un provider IPAM di terze parti di fornire indirizzi IP.

- Importare un intervallo iniziale di indirizzi IP in un profilo di rete di vRealize Automation.
- Applicare i valori importati per creare il primo intervallo di rete denominato nel profilo di rete.
- Eliminare uno o più indirizzi IP dall'intervallo di rete di vRealize Automation.
- Importare un file CSV modificato o diverso per esaminare in che modo vengono modificati i valori dell'intervallo di rete.

Non è possibile utilizzare l'opzione **Importa da CSV** per i profili di rete che utilizzano un endpoint IPAM di terze parti, perché gli indirizzi IP vengono gestiti dal provider IPAM di terze parti e non da vRealize Automation.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Creare un file CSV contenente gli indirizzi IP per l'importazione in un intervallo di reti. Vedere [Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti](#) e [Informazioni sul formato di file CSV per l'importazione degli indirizzi IP del profilo di rete](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare un tipo di profilo di rete dal menu a discesa.
Per questo esempio, selezionare *Esterno*.
- 3 Immettere **Il mio profilo di rete con CSV** nella casella di testo **Nome**.
- 4 Immettere **Test degli indirizzi IP dell'intervallo di rete con CSV** nella casella di testo **Descrizione**.
L'opzione di importazione del file CSV si applica alle impostazioni nelle pagine delle schede **Intervalli di rete** e **Indirizzi IP**.
- 5 (Facoltativo) Selezionare un endpoint IPAM configurato se ne è disponibile uno. Altrimenti, è possibile saltare questo passaggio.
- 6 Immettere un valore appropriato per l'indirizzo IP nelle caselle di testo **Subnet mask** e **Gateway**.
- 7 Fare clic sulla scheda **DNS**.
- 8 Immettere le informazioni applicabili come il suffisso DNS e fare clic sulla scheda **Intervalli di rete**.

Quando si fa clic sulla scheda **Intervalli di rete**, sarà disponibile l'opzione **Importa da CSV**.

- 9 Per immettere manualmente un nuovo nome di intervallo di rete e un nuovo intervallo di indirizzi IP, fare clic su **Nuovo** o per importare le informazioni relative agli IP da un file CSV formattato correttamente, fare clic su **Importa da CSV**.

■ Fare clic su **Nuovo**.

- a Assegnare un nome all'intervallo di rete.
- b Immettere una descrizione dell'intervallo di rete.
- c Immettere l'indirizzo IP iniziale dell'intervallo.
- d Immettere l'indirizzo IP finale dell'intervallo.

■ Fare clic su **Importa da CSV**.

- a Individuare e selezionare il file CSV o trascinarlo nella finestra di dialogo **Importa da CSV**.

Una riga del file CSV ha il seguente formato: *ip_address, machine_name, status, NIC offset*. Ad esempio:

```
100.10.100.1,mymachine01,Allocated,0
```

Campo CSV	Descrizione
ip_address	Un indirizzo IP in formato IPv4.
machine_name	Nome di una macchina gestita in vRealize Automation. Se il campo è vuoto, il valore predefinito è senza nome. Se il campo è vuoto, il valore del campo status non può essere Allocated.
status	Allocato o Non allocato, viene fatta distinzione tra lettere maiuscole e minuscole. Se il campo è vuoto, il valore predefinito è Non allocato. Se lo stato è Allocated, il campo machine_name non può essere vuoto.
NIC_offset	Un numero intero non negativo. Lo scarto NIC indica la NIC della macchina virtuale a cui è assegnato l'indirizzo IP. Se una macchina virtuale alloca più indirizzi IP per NIC diverse, è presente una voce di indirizzo IP per ogni NIC che contiene lo scarto NIC corrispondente. Se si imposta il valore 0, non viene specificato alcuno scarto.

- b Fare clic su **Applica**.

- 10 Fare clic su **OK**.

Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP vengono visualizzati quando si fa clic su **Applica** o dopo che si salva e quindi si modifica il profilo di rete.

- 11 Per visualizzare i dati degli indirizzi IP per lo spazio di indirizzi dell'intervallo specificato, fare clic sulla scheda **Indirizzi IP**.

Se le informazioni degli indirizzi IP sono state importate da un file CSV, il nome dell'intervallo viene generato come *importato da CSV*.

12 (Facoltativo) Per filtrare le voci degli indirizzi IP, selezionare un indirizzo IP dal menu a discesa **Intervallo di rete**.

È possibile visualizzare informazioni relative agli intervalli di rete definiti, agli intervalli di rete importati da un file CSV oppure a un intervallo di rete denominato.

Operazioni successive

Se si importano di nuovo gli indirizzi IP da un file CSV, gli indirizzi IP precedenti vengono sostituiti con le informazioni contenute nel file CSV importato.

Creazione di un profilo di rete esterna per una rete esistente

È possibile creare profili di rete esterne per specificare le impostazioni di rete da utilizzare per configurare reti esistenti per il provisioning di macchine, inclusa la configurazione di dispositivi NSX Edge da utilizzare durante il provisioning.

È possibile utilizzare l'endpoint del provider IPAM fornito con vRealize Automation oppure un endpoint di un provider IPAM di terze parti, ad esempio Infoblox, che è stato precedentemente registrato in vRealize Orchestrator.

Creazione di un profilo di rete esterna mediante l'endpoint IPAM fornito

È possibile creare un profilo di rete esterna per definire le proprietà della rete e un intervallo di indirizzi IP statici da utilizzare per il provisioning delle macchine che si trovano in una rete esterna.

È possibile definire uno o più intervalli di rete degli indirizzi IP statici nel profilo di rete da utilizzare nel provisioning di una macchina. Se non si specifica un intervallo, è possibile utilizzare un profilo di rete come criterio di prenotazione e selezionare un percorso per una scheda di rete di una macchina virtuale (vNIC).

Per informazioni sulla creazione di un profilo di rete esterna e l'utilizzo dell'endpoint di un provider IPAM esterno, vedere [Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti](#).

Procedura

1 [Specifica delle informazioni dei profili di rete esterna mediante l'endpoint IPAM fornito](#)

Un profilo di rete esterna identifica le proprietà di rete e le impostazioni per una rete esistente. Un profilo di rete esterna è un requisito dei profili di rete instradati e NAT.

2 [Configurazione degli intervalli IP dei profili di rete esterna mediante l'endpoint IPAM fornito](#)

È possibile definire uno o più intervalli di rete degli indirizzi IP statici nel profilo di rete da utilizzare nel provisioning di una macchina. Se non si specifica un intervallo, è possibile utilizzare un profilo di rete come criterio di prenotazione e selezionare un percorso per una scheda di rete di una macchina virtuale (vNIC).

Operazioni successive

I profili di rete possono essere assegnati a un percorso di rete in una prenotazione o specificati in un blueprint dagli architetti di blueprint. Il profilo della rete esterna può essere usato per la creazione di profili di rete NAT o instradati su richiesta.

Specifica delle informazioni dei profili di rete esterna mediante l'endpoint IPAM fornito. Un profilo di rete esterna identifica le proprietà di rete e le impostazioni per una rete esistente. Un profilo di rete esterna è un requisito dei profili di rete instradati e NAT.

Per informazioni su come creare un profilo di rete esterna ottenendo le informazioni sugli indirizzi IPAM da un endpoint IPAM di terze parti registrato, come Infoblox, vedere [Elenco di controllo per fornire il supporto del provider IPAM di terze parti](#) e [Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti](#). Attenersi alla seguente procedura per creare un profilo di rete utilizzando l'endpoint IPAM interno di VMware

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **Esterno** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Accettare il valore **Endpoint IPAM** predefinito per l'endpoint IPAM di **vRealize Automation**.
- 5 Immettere la subnet mask IP nella casella di testo **Subnet mask**.

La subnet mask indica la dimensione dell'intero spazio degli indirizzi instradabili che si desidera definire per il profilo di rete.

Ad esempio, immettere 255.255.0.0.

- 6 Immettere l'indirizzo di un gateway instradato, ad esempio 10.10.110.1, nella casella di testo **Gateway**.

L'indirizzo IP del gateway definito nel profilo di rete viene assegnato alla NIC durante l'allocazione. Il gateway è necessario per i profili di rete NAT.

Per NSX-T, il gateway predefinito del server DHCP corrisponde al gateway predefinito NAT One-to-Many. Il gateway predefinito del pool di IP corrisponde al gateway predefinito NAT One-to-Many in vRealize Automation.

Se nella casella di testo **Gateway** del profilo di rete non è assegnato alcun valore, è necessario utilizzare la proprietà personalizzata `VirtualMachine.Network0.Gateway` per assegnare un gateway.

- 7 Fare clic sulla scheda **DNS**.
- 8 Immettere i valori di DNS e WINS secondo necessità.

Utilizzare i valori DNS per la registrazione e la risoluzione dei nomi. I valori sono facoltativi per un IPAM interno. I valori vengono forniti dal provider IPAM di terze parti per un IPAM esterno.

- a (Facoltativo) Immettere un valore del server **DNS primario**.
- b (Facoltativo) Immettere un valore del server **DNS secondario**.

- c (Facoltativo) Immettere un valore per i **suffissi DNS**.
- d (Facoltativo) Immettere un valore per i **suffissi di ricerca DNS**.
- e (Facoltativo) Immettere un valore del server **WINS preferito**.
- f (Facoltativo) Immettere un valore del server **WINS alternativo**.

Operazioni successive

È possibile configurare intervalli di indirizzi IP statici. Vedere [Configurazione degli intervalli IP dei profili di rete esterna mediante l'endpoint IPAM fornito](#).

Configurazione degli intervalli IP dei profili di rete esterna mediante l'endpoint IPAM fornito
È possibile definire uno o più intervalli di rete degli indirizzi IP statici nel profilo di rete da utilizzare nel provisioning di una macchina. Se non si specifica un intervallo, è possibile utilizzare un profilo di rete come criterio di prenotazione e selezionare un percorso per una scheda di rete di una macchina virtuale (vNIC).

È possibile definire manualmente i valori degli intervalli di IP da un file CSV importato o dagli indirizzi IP forniti da un provider IPAM esterno. È possibile combinare intervalli IP definiti manualmente e indirizzi IP importati tramite CSV. Ad esempio, è possibile definire alcuni intervalli utilizzando l'interfaccia utente e altri mediante l'importazione da un file CSV.

Se si effettua l'importazione da un file CSV una seconda volta, indipendentemente dal nome del file CSV, gli intervalli IP importati dalla precedente importazione del file CSV vengono cancellati e vengono aggiunte le informazioni del nuovo intervallo IP. In tal modo, l'importazione precedente viene sovrascritta quando si effettua l'importazione una seconda volta o più volte. È possibile ripetere il processo di aggiornamento di un file CSV e reimportare il file CSV nel profilo di rete indefinitamente.

Se per un profilo di rete esterna non sono stati definiti intervalli di IP, è possibile utilizzarlo per specificare quale rete selezionare per una scheda di rete virtuale (vNIC). Se si sta utilizzando il profilo di rete esistente in un profilo di rete NAT o instradata, dovrà avere almeno un intervallo di IP statici.

Prerequisiti

[Specifica delle informazioni dei profili di rete esterna mediante l'endpoint IPAM fornito](#).

Procedura

- 1 Fare clic sulla scheda **Intervalli di rete**.
- 2 Per immettere manualmente un nuovo nome di intervallo di rete e un nuovo intervallo di indirizzi IP, fare clic su **Nuovo** o per importare le informazioni relative agli IP da un file CSV formattato correttamente, fare clic su **Importa da CSV**.
 - Fare clic su **Nuovo**.
 - a Assegnare un nome all'intervallo di rete.
 - b Immettere una descrizione dell'intervallo di rete.

- c Immettere l'indirizzo IP iniziale dell'intervallo.
- d Immettere l'indirizzo IP finale dell'intervallo.

■ Fare clic su **Importa da CSV**.

- a Individuare e selezionare il file CSV o trascinarlo nella finestra di dialogo **Importa da CSV**.

Una riga del file CSV ha il seguente formato: *ip_address, machine_name, status, NIC offset*. Ad esempio:

```
100.10.100.1,mymachine01,Allocated,0
```

Campo CSV	Descrizione
ip_address	Un indirizzo IP in formato IPv4.
machine_name	Nome di una macchina gestita in vRealize Automation. Se il campo è vuoto, il valore predefinito è senza nome. Se il campo è vuoto, il valore del campo status non può essere Allocated.
status	Allocato o Non allocato, viene fatta distinzione tra lettere maiuscole e minuscole. Se il campo è vuoto, il valore predefinito è Non allocato. Se lo stato è Allocated, il campo machine_name non può essere vuoto.
NIC_offset	Un numero intero non negativo. Lo scarto NIC indica la NIC della macchina virtuale a cui è assegnato l'indirizzo IP. Se una macchina virtuale alloca più indirizzi IP per NIC diverse, è presente una voce di indirizzo IP per ogni NIC che contiene lo scarto NIC corrispondente. Se si imposta il valore 0, non viene specificato alcuno scarto.

- b Fare clic su **Applica**.

3 Fare clic su **OK**.

Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP vengono visualizzati quando si fa clic su **Applica** o dopo che si salva e quindi si modifica il profilo di rete.

4 Per visualizzare i dati degli indirizzi IP per lo spazio di indirizzi dell'intervallo specificato, fare clic sulla scheda **Indirizzi IP**.

Se le informazioni degli indirizzi IP sono state importate da un file CSV, il nome dell'intervallo viene generato come *importato da CSV*.

5 (Facoltativo) Per filtrare le voci degli indirizzi IP, selezionare un indirizzo IP dal menu a discesa **Intervallo di rete**.

È possibile visualizzare informazioni relative agli intervalli di rete definiti, agli intervalli di rete importati da un file CSV oppure a un intervallo di rete denominato.

- 6** (Facoltativo) Per filtrare gli indirizzi IP che corrispondono allo stato dell'IP, selezionare un tipo di stato dal menu a discesa **Stato IP**.

Per gli indirizzi IP con stato Scaduto o Eliminato, fare clic su **Recupera** per renderli disponibili per l'allocazione. È necessario salvare il profilo affinché il recupero abbia effetto.

L'aggiornamento della colonna di stato da Expired o Destroyed a Allocated può richiedere qualche secondo.

- 7** Per completare il profilo di rete, fare clic su **OK**.

Risultati

I profili di rete possono essere assegnati a un percorso di rete in una prenotazione o specificati in un blueprint dagli architetti di blueprint. Se è stato creato un profilo di rete esterna, è possibile utilizzare il profilo di rete esterna quando si crea un profilo di rete NAT o instradata.

Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti

È possibile utilizzare una soluzione di un provider IPAM importata configurata e registrata in vRealize Orchestrator per ottenere indirizzi IP da tale provider di terze parti.

È possibile creare un profilo di rete esterna che utilizzi l'endpoint di un provider di soluzioni IPAM di terze parti registrato per ottenere le impostazioni di gateway, subnet mask e DHCP/WINS.

È possibile definire uno o più intervalli di rete degli indirizzi IP statici nel profilo di rete da utilizzare nel provisioning di una macchina. Se non si specifica un intervallo, è possibile utilizzare un profilo di rete come criterio di prenotazione e selezionare un percorso per una scheda di rete di una macchina virtuale (vNIC).

Per informazioni su come creare un profilo di rete esterna senza utilizzare un provider IPAM oppure utilizzando l'endpoint del provider IPAM interno fornito, vedere [Creazione di un profilo di rete esterna mediante l'endpoint IPAM fornito](#).

Procedura

- 1** [Specificare le informazioni del profilo di rete esterna utilizzando un endpoint IPAM di terze parti](#)

Un profilo di rete esterna identifica le proprietà di rete e le impostazioni per una rete esistente. Un profilo di rete esterna è un requisito dei profili di rete instradati e NAT. Se è stato registrato e configurato un endpoint IPAM in vRealize Orchestrator, è possibile specificare che le informazioni degli indirizzi IP vengano fornite da un provider IPAM.

- 2** [Configurazione di intervalli IP per un profilo di rete esterno mediante un endpoint IPAM di terze parti](#)

È possibile definire uno o più intervalli di rete degli indirizzi IP statici nel profilo di rete da utilizzare nel provisioning di una macchina. Se non si specifica un intervallo, è possibile utilizzare un profilo di rete come criterio di prenotazione e selezionare un percorso per una scheda di rete di una macchina virtuale (vNIC).

Operazioni successive

I profili di rete possono essere assegnati a un percorso di rete in una prenotazione o specificati in un blueprint dagli architetti di blueprint. Il profilo della rete esterna può essere usato per la creazione di profili di rete NAT o instradati su richiesta.

Specificare le informazioni del profilo di rete esterna utilizzando un endpoint IPAM di terze parti. Un profilo di rete esterna identifica le proprietà di rete e le impostazioni per una rete esistente. Un profilo di rete esterna è un requisito dei profili di rete instradati e NAT. Se è stato registrato e configurato un endpoint IPAM in vRealize Orchestrator, è possibile specificare che le informazioni degli indirizzi IP vengano fornite da un provider IPAM.

Prerequisiti

- Verificare di aver importato e configurato un plug-in del provider IPAM esterno in vRealize Orchestrator, nonché di aver registrato il tipo di endpoint del provider IPAM in vRealize Orchestrator. In questo esempio, il provider di soluzioni IPAM esterno supportato è Infoblox. Vedere [Elenco di controllo per fornire il supporto del provider IPAM di terze parti](#).
- [Creazione di un endpoint di un provider IPAM di terze parti](#).
- Configurare vRealize Orchestrator Appliance con il workflow dell'endpoint IPAM registrato come Orchestrator autonomo nel tenant globale (administrator@vsphere.local).
- Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **Esterno** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Se sono stati specificati uno o più endpoint di provider IPAM di terze parti, selezionare un endpoint IPAM di terze parti nel menu a discesa **Endpoint IPAM**.

Quando si seleziona l'endpoint di un provider IPAM di terze parti registrato in vRealize Orchestrator, gli indirizzi IP vengono ottenuti dal provider del servizio IPAM specificato.

Operazioni successive

È ora possibile definire gli intervalli di rete per gli indirizzi IP in modo da completare la definizione del profilo di rete.

Configurazione di intervalli IP per un profilo di rete esterno mediante un endpoint IPAM di terze parti

È possibile definire uno o più intervalli di rete degli indirizzi IP statici nel profilo di rete da utilizzare nel provisioning di una macchina. Se non si specifica un intervallo, è possibile utilizzare un profilo di rete come criterio di prenotazione e selezionare un percorso per una scheda di rete di una macchina virtuale (vNIC).

È possibile definire intervalli IP usando gli indirizzi IP forniti da un provider IPAM di terze parti.

vRealize Automation salva nel database soltanto gli ID degli intervalli di IPAM esterni, non i dettagli dell'intervallo. Se si modifica un profilo di rete in questa pagina o in un blueprint, vRealize Automation chiama il servizio IPAM per ottenere i dettagli dell'intervallo in base agli ID degli intervalli selezionati.

Nota Esiste un problema noto relativo ai provider IPAM di terze parti, per cui una query può scadere quando restituisce gli intervalli di rete, generando un elenco vuoto. Come soluzione alternativa, è possibile fornire criteri di ricerca per evitare il timeout e ricevere le informazioni relative all'intervallo di rete.

Ad esempio, a seconda del provider IPAM, è possibile aggiungere una proprietà denominata VLAN a ciascuna rete dell'applicazione del provider IPAM e assegnare un valore a tale proprietà, quale 4. È quindi possibile filtrare in base alla proprietà e al valore, ad esempio VLAN=4, nella casella di testo **Seleziona intervallo di rete** nella pagina del profilo di rete di vRealize Automation.

Come alternativa, è possibile aumentare il valore dell'impostazione del timeout mediante la seguente procedura:

- 1 In ogni cnode dell'appliance vRealize Automation, aprire il file `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml`.
- 2 Modificare il valore del timeout sostituendo 30 secondi con un numero superiore.
- 3 Riavviare il server vcac immettendo `service vcac-server restart`.

Prerequisiti

Specificare le informazioni del profilo di rete esterna utilizzando un endpoint IPAM di terze parti.

Procedura

- 1 Per creare un intervallo di rete o selezionare un intervallo di rete esistente, fare clic sulla scheda **Intervalli di rete**.
- 2 Selezionare uno spazio di indirizzi dall'elenco di tutti quelli disponibili per l'endpoint nel menu a discesa dello **spazio di indirizzi**.
- 3 Fare clic su **Aggiungi** e selezionare uno o più intervalli di rete disponibili per lo spazio di indirizzi specificato.

La selezione di un intervallo di rete potrebbe restituire un elenco vuoto quando si utilizza un provider IPAM di terze parti. Per informazioni dettagliate, vedere l'articolo 2148656 della Knowledge Base all'indirizzo <http://kb.vmware.com/kb/2148656>.

- 4 Fare clic su **OK**.

Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP vengono visualizzati quando si fa clic su **Applica** o dopo che si salva e quindi si modifica il profilo di rete.

- 5 Per completare il profilo di rete, fare clic su **OK**.

Operazioni successive

I profili di rete possono essere assegnati a un percorso di rete in una prenotazione o specificati in un blueprint dagli architetti di blueprint.

Creazione di un profilo di rete instradata per una rete su richiesta

È possibile creare un profilo di rete instradata su richiesta che usi l'endpoint IPAM di vRealize Automation fornito o un endpoint IPAM di terze parti adeguatamente configurato e registrato.

Un profilo di rete instradata rappresenta uno spazio IP instradabile diviso in più reti. Ciascuna nuova rete instradata alloca la subnet successiva disponibile dallo spazio IP instradabile. Una rete instradata può accedere a tutte le altre reti instradate che utilizzano lo stesso profilo di rete. Ciascuna subnet instradata può accedere a tutte le altre subnet create dallo stesso profilo di rete.

Nel caso di un provider IPAM di terze parti, lo spazio IP instradabile viene creato e gestito dal provider IPAM di terze parti. L'amministratore di rete usa un provider IPAM di terze parti per definire uno spazio IP instradabile e creare un blocco di indirizzi IP per tale spazio. È possibile selezionare uno o più blocchi di indirizzi IP recuperati dal provider IPAM di terze parti quando si crea o si modifica un profilo di rete instradata.

Quando una nuova istanza di un profilo di rete instradata viene allocata a partire da un provider IPAM di terze parti, vRealize Automation effettua una chiamata al provider per riservare la prima subnet disponibile e crea un intervallo utilizzando blocchi di indirizzi IP determinati dal profilo di rete instradata e dalle dimensioni della subnet. L'intervallo che ne risulta viene utilizzato per allocare gli indirizzi IP delle macchine assegnate alla rete instradata nella stessa distribuzione.

Creazione di un profilo di rete instradata mediante l'endpoint IPAM fornito

Quando si utilizza un profilo di rete instradata con l'endpoint IPAM fornito, è possibile definire uno spazio di indirizzi IP instradabili e le subnet disponibili per una rete instradata su richiesta.

Se si utilizza l'endpoint IPAM vRealize Automation fornito è possibile assegnare al profilo di rete instradata intervalli di indirizzi IP statici e un indirizzo IP di base.

È possibile utilizzare gli intervalli di indirizzi IP ricavati dall'endpoint IPAM di VMware specificato o da un endpoint del provider di servizi IPAM di terze parti registrato e configurato in vRealize Orchestrator, ad esempio Infoblox IPAM. Durante l'allocazione, viene creato un intervallo di indirizzi IP da un blocco IP.

Procedura

1 [Indicazione delle informazioni dei profili di rete instradate con l'endpoint IPAM di vRealize Automation](#)

Le informazioni di un profilo di rete identificano le proprietà della rete instradata, il relativo profilo di rete esterna sottostante e gli altri valori utilizzati nel provisioning della rete quando si utilizza l'endpoint IPAM fornito.

2 [Configurazione di intervalli di indirizzi IP di profili di rete instradate con l'endpoint IPAM di vRealize Automation](#)

È possibile definire uno o più intervalli di indirizzi IP statici da utilizzare nel provisioning di una rete.

Indicazione delle informazioni dei profili di rete instradate con l'endpoint IPAM di vRealize Automation

Le informazioni di un profilo di rete identificano le proprietà della rete instradata, il relativo profilo di rete esterna sottostante e gli altri valori utilizzati nel provisioning della rete quando si utilizza l'endpoint IPAM fornito.

Per creare un profilo di rete instradata utilizzando un endpoint IPAM di terze parti, vedere [Indicazione delle informazioni dei profili di rete instradate con un endpoint IPAM di terze parti](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Creare un profilo di rete esterna. Vedere [Creazione di un profilo di rete esterna mediante l'endpoint IPAM fornito](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **Instradato** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Accettare il valore **Endpoint IPAM** predefinito per l'endpoint IPAM di **vRealize Automation**.
- 5 Selezionare un profilo di rete esterno esistente dal menu a discesa **Profilo di rete esterno**.
- 6 Immettere la subnet mask nella casella di testo **Subnet mask** associata al profilo di rete esterno.

La subnet mask indica la dimensione dell'intero spazio degli indirizzi instradabili da definire per il profilo della rete.

Ad esempio, immettere 255.255.0.0.

- 7 Selezionare un valore nel menu a discesa della casella di testo **Subnet mask intervallo**.

Ad esempio, immettere 255.255.255.0.

La subnet mask dell'intervallo definisce il modo in cui si desidera eseguire la partizione dello spazio della rete in singoli blocchi di indirizzi. I blocchi vengono allocati a ogni istanza di distribuzione del profilo di rete.

Viene utilizzato un intervallo per ogni distribuzione che usa un profilo di rete instradata. Il numero di intervalli instradati disponibili corrisponde alla subnet mask diviso per la subnet mask dell'intervallo, ad esempio $255.255.0.0 / 255.255.255.0 = 256$.

- 8 Immettere il primo indirizzo IP disponibile nella casella di testo **IP base**.

Questa opzione non è disponibile per gli endpoint di terze parti.

Ad esempio, immettere 120.120.0.1.

- 9 Fare clic sulla scheda **DNS**.

10 Immettere i valori di DNS e WINS secondo necessità.

Utilizzare i valori DNS per la registrazione e la risoluzione dei nomi. I valori sono facoltativi per un IPAM interno. I valori vengono forniti dal provider IPAM di terze parti per un IPAM esterno.

- a (Facoltativo) Immettere un valore del server **DNS primario**.
- b (Facoltativo) Immettere un valore del server **DNS secondario**.
- c (Facoltativo) Immettere un valore per i **suffissi DNS**.
- d (Facoltativo) Immettere un valore per i **suffissi di ricerca DNS**.
- e (Facoltativo) Immettere un valore del server **WINS preferito**.
- f (Facoltativo) Immettere un valore del server **WINS alternativo**.

Operazioni successive

[Configurazione di intervalli di indirizzi IP di profili di rete instradate con l'endpoint IPAM di vRealize Automation.](#)

Configurazione di intervalli di indirizzi IP di profili di rete instradate con l'endpoint IPAM di vRealize Automation

È possibile definire uno o più intervalli di indirizzi IP statici da utilizzare nel provisioning di una rete.

Durante il provisioning, ogni nuova rete instradata alloca l'intervallo disponibile successivo e lo utilizza come proprio spazio di indirizzi IP.

Prerequisiti

[Indicazione delle informazioni dei profili di rete instradate con l'endpoint IPAM di vRealize Automation.](#)

Procedura

- 1** Per creare un intervallo di rete o selezionare un intervallo di rete esistente, fare clic sulla scheda **Intervalli di rete**.
- 2** Fare clic su **Genera intervalli** per generare gli intervalli di rete in base alla subnet mask, la subnet mask dell'intervallo e le informazioni degli indirizzi IP di base che sono state immesse nella scheda Generale.

A iniziare dall'indirizzo IP base, vRealize Automation genera intervalli sulla base della subnet mask dell'intervallo.

Ad esempio, vRealize Automation genera intervalli di 255 intervalli di IP se la subnet mask è 255.255.0.0 e la subnet mask dell'intervallo è 255.255.255.0 utilizzando il nome da Range1 a Rangen.

- 3** Fare clic su **OK**.

Creazione di un profilo di rete instradata mediante un endpoint IPAM di terze parti

Quando si utilizza un profilo di rete instradata con un endpoint IPAM di terze parti, lo spazio degli indirizzi IP instradabili viene creato e gestito dal provider IPAM di terze parti.

Quando si utilizza un endpoint IPAM di terze parti nel proprio profilo di rete instradata, il provider crea nuovi intervalli di indirizzi IP per ciascuna istanza della rete su richiesta.

È possibile utilizzare gli intervalli di indirizzi IP ricavati dall'endpoint IPAM di VMware specificato o da un endpoint del provider di servizi IPAM di terze parti registrato e configurato in vRealize Orchestrator, ad esempio Infoblox IPAM. Durante l'allocazione, viene creato un intervallo di indirizzi IP da un blocco IP.

Procedura

1 [Indicazione delle informazioni dei profili di rete instradate con un endpoint IPAM di terze parti](#)

Le informazioni di un profilo di rete identificano le proprietà della rete instradata, il relativo profilo di rete esterna sottostante e gli altri valori utilizzati nel provisioning della rete quando si utilizza un endpoint IPAM di terze parti.

2 [Configurazione di intervalli di indirizzi IP di profili di rete instradate con un endpoint IPAM di terze parti](#)

È possibile gestire uno o più intervalli denominati di indirizzi di rete IPv4 statici da utilizzare nel provisioning di una rete.

Indicazione delle informazioni dei profili di rete instradate con un endpoint IPAM di terze parti

Le informazioni di un profilo di rete identificano le proprietà della rete instradata, il relativo profilo di rete esterna sottostante e gli altri valori utilizzati nel provisioning della rete quando si utilizza un endpoint IPAM di terze parti.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Creare un profilo di rete esterna. Vedere [Creazione di un profilo di rete esterna mediante l'endpoint IPAM fornito](#) o [Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti](#).
- Creare e configurare un endpoint IPAM di terze parti. Vedere [Creazione di un endpoint di un provider IPAM di terze parti](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **Instradato** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Se sono stati specificati uno o più endpoint di provider IPAM di terze parti, selezionare un endpoint IPAM di terze parti nel menu a discesa **Endpoint IPAM**.

Quando si seleziona l'endpoint di un provider IPAM di terze parti registrato in vRealize Orchestrator, gli indirizzi IP vengono ottenuti dal provider del servizio IPAM specificato.

- 5 Selezionare un profilo di rete esterno esistente dal menu a discesa **Profilo di rete esterno**.

Sono elencati e disponibili per la selezione solo i profili di rete esterni configurati per l'utilizzo dell'endpoint IPAM specificato.

- 6 Per determinare il numero di subnet della rete da creare, selezionare un valore nel menu a discesa della casella di testo **Subnet mask intervallo**.

Ad esempio, immettere 255.255.255.0.

La subnet mask dell'intervallo definisce le modalità di partizionamento di tale spazio in singoli blocchi di indirizzi allocati a ogni istanza di distribuzione del profilo di rete specificato. Quando si sceglie un valore per la subnet mask dell'intervallo, tenere conto del numero di distribuzioni che si prevede venga utilizzato dalla rete instradata.

Viene utilizzato un intervallo per ciascuna distribuzione che utilizza un profilo di rete instradata. Il numero di intervalli instradati disponibili corrisponde alla subnet mask diviso per la subnet mask dell'intervallo, ad esempio $255.255.0.0/255.255.255.0 = 256$.

- 7 Per definire uno spazio di indirizzi e gestire uno o più intervalli denominati di indirizzi di rete IPv4 statici, fare clic sulla scheda **Blocchi IP**.

I blocchi IP disponibili sono l'origine degli intervalli di indirizzi IP creati o allocati per l'instradamento su richiesta.

Operazioni successive

[Configurazione di intervalli di indirizzi IP di profili di rete instradate con un endpoint IPAM di terze parti.](#)

Configurazione di intervalli di indirizzi IP di profili di rete instradate con un endpoint IPAM di terze parti

È possibile gestire uno o più intervalli denominati di indirizzi di rete IPv4 statici da utilizzare nel provisioning di una rete.

Durante il provisioning, ciascuna nuova rete instradata alloca l'intervallo disponibile successivo e lo utilizza come proprio spazio di indirizzi IP. I blocchi di indirizzi IP vengono ottenuti dal provider IPAM di terze parti. Durante il provisioning, una rete instradata viene allocata a partire dal blocco con la subnet mask che corrisponde alla subnet mask dell'intervallo fornito.

Prerequisiti

[Indicazione delle informazioni dei profili di rete instradate con un endpoint IPAM di terze parti.](#)

Procedura

- 1 Per limitare i blocchi IP disponibili per il provisioning, selezionare uno spazio di indirizzi dal menu a discesa **Spazio indirizzi**.

Non è possibile selezionare uno spazio di indirizzi dopo aver aggiunto blocchi IP. Un profilo di rete instradata non può estendersi oltre uno spazio di indirizzi.

2 Aggiungere uno o più blocchi IP o intervalli di provider IPAM.

I blocchi IP vengono recuperati dal provider IPAM di terze parti.

La selezione di un intervallo di rete potrebbe restituire un elenco vuoto quando si utilizza un provider IPAM di terze parti. Per informazioni dettagliate, vedere l'articolo 2148656 della Knowledge Base all'indirizzo <http://kb.vmware.com/kb/2148656>.

- a Fare clic su **Aggiungi**.
- b Fare clic su **Cerca**.
- c Immettere la sintassi di ricerca o selezionare blocchi di IP dal menu a discesa.
- d Fare clic su **OK**.

3 Fare clic su **Applica**.

4 Fare clic su **OK**.

Creazione di un profilo di rete NAT per una rete su richiesta

È possibile creare un profilo di rete NAT su richiesta che utilizzi l'endpoint IPAM di vRealize Automation fornito o un endpoint IPAM di terze parti correttamente configurato e registrato.

Creazione di un profilo di rete NAT mediante l'endpoint IPAM fornito

È possibile creare un profilo di rete NAT NSX su richiesta associato a un profilo di rete esterno. Quando si utilizza l'endpoint IPAM di vRealize Automation fornito, è possibile assegnare al profilo di rete NAT intervalli di indirizzi DHCP e IP statici.

Le reti NAT utilizzano un set di indirizzi IP per le comunicazioni esterne e un altro set per le comunicazioni interne. Gli indirizzi IP esterni vengono allocati da un profilo di rete esterno mentre gli indirizzi IP NAT interni vengono definiti da un profilo di rete NAT. Quando si esegue il provisioning di una nuova rete NAT viene creata una nuova istanza del profilo di rete NAT esterno e tale istanza viene utilizzata per l'allocazione degli indirizzi IP delle macchine.

È possibile utilizzare gli intervalli di indirizzi IP ricavati dall'endpoint IPAM di VMware specificato o da un endpoint del provider di servizi IPAM di terze parti registrato e configurato in vRealize Orchestrator, ad esempio Infoblox IPAM. Durante l'allocazione, viene creato un intervallo di indirizzi IP da un blocco IP.

Per una rete NAT One-to-Many, è possibile definire regole NAT che possono essere configurate quando si aggiunge un componente di rete NAT al blueprint. È possibile modificare una regola NAT quando si modifica la rete NAT in una distribuzione.

Procedura

1 [Indicazione delle informazioni del profilo di rete NAT con l'endpoint IPAM di vRealize Automation](#)

Il profilo di rete identifica le proprietà della rete NAT su richiesta, il profilo della rete esterna sottostante, il tipo di NAT e gli altri valori utilizzati per eseguire il provisioning della rete utilizzando l'IPAM vRealize Automation incorporato.

2 Configurazione di intervalli di indirizzi IP di profili di rete NAT con l'endpoint IPAM di vRealize Automation

È possibile definire uno o più intervalli di indirizzi IP statici da utilizzare nel provisioning di una rete.

Indicazione delle informazioni del profilo di rete NAT con l'endpoint IPAM di vRealize Automation
Il profilo di rete identifica le proprietà della rete NAT su richiesta, il profilo della rete esterna sottostante, il tipo di NAT e gli altri valori utilizzati per eseguire il provisioning della rete utilizzando l'IPAM vRealize Automation incorporato.

Se si desidera creare un profilo di rete NAT che utilizzi un endpoint IPAM di terze parti, vedere [Indicazione delle informazioni sul profilo di rete NAT con un endpoint IPAM di terze parti](#).

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Creare un profilo di rete esterna. Vedere [Creazione di un profilo di rete esterna mediante l'endpoint IPAM fornito](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **NAT** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Accettare il valore **Endpoint IPAM** predefinito per l'endpoint IPAM di **vRealize Automation**.
- 5 Selezionare un profilo di rete esterno esistente dal menu a discesa **Profilo di rete esterno**.
- 6 Selezionare un tipo di traduzione degli indirizzi di rete One-to-One o One-to-Many dal menu a discesa **Tipo NAT**.

Opzione	Descrizione
One-to-One	Assegnare un indirizzo IP statico esterno a ciascuna scheda di rete. Ogni macchina può accedere alla rete esterna ed è accessibile dalla rete esterna. Tutti gli indirizzi IP esterni assegnati a un uplink edge di NSX devono far parte della stessa subnet. Quando si utilizza NAT one-to-one in vRealize Automation, il profilo di rete esterno corrispondente deve contenere solo intervalli di indirizzi IP appartenenti a una singola subnet.
One-to-Many	Un indirizzo IP esterno è condiviso da tutte le macchine della rete. Una macchina interna può avere indirizzi IP statici o forniti tramite protocollo DHCP. Ogni macchina può accedere alla rete esterna, ma nessuna macchina è accessibile dalla rete esterna. Selezionando questa opzione viene selezionata la casella di controllo Attivato nel gruppo DHCP. Per NSX for vSphere, il tipo di traduzione NAT One-to-Many consente di definire regole NAT quando si aggiunge un componente di rete NAT a un blueprint. NSX for vSphere supporta reti NAT One-to-One e NAT One-to-Many, ma NSX-T supporta solo reti NAT one-to-many.

7 Immettere la subnet mask IP nella casella di testo **Subnet mask**.

La subnet mask indica la dimensione dell'intero spazio degli indirizzi instradabili che si desidera definire per il profilo di rete.

Ad esempio, immettere 255.255.0.0.

8 Immettere l'indirizzo di un gateway instradato, ad esempio 10.10.110.1, nella casella di testo **Gateway**.

L'indirizzo IP del gateway definito nel profilo di rete viene assegnato alla NIC durante l'allocazione. Il gateway è necessario per i profili di rete NAT.

Per NSX-T, il gateway predefinito del server DHCP corrisponde al gateway predefinito NAT One-to-Many. Il gateway predefinito del pool di IP corrisponde al gateway predefinito NAT One-to-Many in vRealize Automation.

Se nella casella di testo **Gateway** del profilo di rete non è assegnato alcun valore, è necessario utilizzare la proprietà personalizzata `VirtualMachine.Network0.Gateway` per assegnare un gateway.

9 (Facoltativo) Nel gruppo DHCP, selezionare la casella di controllo **Abilitato** e immettere i valori di **inizio intervallo IP** e **fine intervallo IP**.

È possibile selezionare la casella di controllo solo se si imposta il tipo di NAT su One-to-Many.

Per NSX-T, il primo IP nell'intervallo del pool di IP corrisponde all'indirizzo IP del server DHCP definito con l'impostazione `<FirstIpInPool>/<subnetMaskOfNat>`. Il pool di IP in NSX-T inizia con il secondo indirizzo IP.

10 (Facoltativo) Impostare una durata lease DHCP per definire per quanto tempo una macchina può utilizzare un indirizzo IP.**11** Fare clic sulla scheda **DNS**.**12** Immettere i valori di DNS e WINS secondo necessità.

Utilizzare i valori DNS per la registrazione e la risoluzione dei nomi. I valori sono facoltativi per un IPAM interno. I valori vengono forniti dal provider IPAM di terze parti per un IPAM esterno.

- a (Facoltativo) Immettere un valore del server **DNS primario**.
- b (Facoltativo) Immettere un valore del server **DNS secondario**.
- c (Facoltativo) Immettere un valore per i **suffissi DNS**.
- d (Facoltativo) Immettere un valore per i **suffissi di ricerca DNS**.
- e (Facoltativo) Immettere un valore del server **WINS preferito**.
- f (Facoltativo) Immettere un valore del server **WINS alternativo**.

Operazioni successive

[Configurazione di intervalli di indirizzi IP di profili di rete NAT con l'endpoint IPAM di vRealize Automation.](#)

Configurazione di intervalli di indirizzi IP di profili di rete NAT con l'endpoint IPAM di vRealize Automation

È possibile definire uno o più intervalli di indirizzi IP statici da utilizzare nel provisioning di una rete.

Non è possibile sovrapporre gli indirizzi IP iniziali e finali dell'intervallo di rete con gli indirizzi DHCP. Se si tenta di salvare un profilo che contiene intervalli di indirizzi che si sovrappongono, vRealize Automation mostra un errore di convalida.

Prerequisiti

[Indicazione delle informazioni del profilo di rete NAT con l'endpoint IPAM di vRealize Automation.](#)

Procedura

- 1 Per creare un intervallo di rete o selezionare un intervallo di rete esistente, fare clic sulla scheda **Intervalli di rete**.
- 2 Per immettere manualmente un nuovo nome di intervallo di rete e un nuovo intervallo di indirizzi IP, fare clic su **Nuovo** o per importare le informazioni relative agli IP da un file CSV formattato correttamente, fare clic su **Importa da CSV**.

- Fare clic su **Nuovo**.

- a Assegnare un nome all'intervallo di rete.
- b Immettere una descrizione dell'intervallo di rete.
- c Immettere l'indirizzo IP iniziale dell'intervallo.
- d Immettere l'indirizzo IP finale dell'intervallo.

- Fare clic su **Importa da CSV**.

- a Individuare e selezionare il file CSV o trascinarlo nella finestra di dialogo **Importa da CSV**.

Una riga del file CSV ha il seguente formato: *ip_address, machine_name, status, NIC offset*. Ad esempio:

```
100.10.100.1,mymachine01,Allocated,0
```

Campo CSV	Descrizione
ip_address	Un indirizzo IP in formato IPv4.
machine_name	Nome di una macchina gestita in vRealize Automation. Se il campo è vuoto, il valore predefinito è senza nome. Se il campo è vuoto, il valore del campo status non può essere Allocated.

Campo CSV	Descrizione
status	Allocato o Non allocato, viene fatta distinzione tra lettere maiuscole e minuscole. Se il campo è vuoto, il valore predefinito è Non allocato. Se lo stato è Allocato, il campo machine_name non può essere vuoto.
NIC_offset	Un numero intero non negativo. Lo scarto NIC indica la NIC della macchina virtuale a cui è assegnato l'indirizzo IP. Se una macchina virtuale alloca più indirizzi IP per NIC diverse, è presente una voce di indirizzo IP per ogni NIC che contiene lo scarto NIC corrispondente. Se si imposta il valore 0, non viene specificato alcuno scarto.

b Fare clic su **Applica**.

3 Fare clic su **OK**.

Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP vengono visualizzati quando si fa clic su **Applica** o dopo che si salva e quindi si modifica il profilo di rete.

4 Per visualizzare gli indirizzi IP per l'intervallo di rete denominato, fare clic sulla scheda **Indirizzi IP**.

5 (Facoltativo) Per filtrare le voci degli indirizzi IP, selezionare un indirizzo IP dal menu a discesa **Intervallo di rete**.

È possibile visualizzare informazioni relative agli intervalli di rete definiti, agli intervalli di rete importati da un file CSV oppure a un intervallo di rete denominato.

6 (Facoltativo) Per filtrare gli indirizzi IP che corrispondono allo stato dell'IP, selezionare un tipo di stato dal menu a discesa **Stato IP**.

Per gli indirizzi IP con stato Scaduto o Eliminato, fare clic su **Recupera** per renderli disponibili per l'allocazione. È necessario salvare il profilo affinché il recupero abbia effetto.

L'aggiornamento della colonna di stato da Expired o Destroyed a Allocated può richiedere qualche secondo.

7 Fare clic su **OK**.

Creazione di un profilo di rete NAT mediante un endpoint IPAM di terze parti in vRealize Automation

È possibile creare un profilo di rete NAT NSX su richiesta associato a un profilo di rete esterno in vRealize Automation. Quando si utilizza un profilo di rete NAT NSX con un provider IPAM di terze parti, lo spazio degli indirizzi IP viene creato e gestito dal provider IPAM di terze parti.

Quando si utilizza un endpoint IPAM di terze parti nel proprio profilo di rete NAT, il provider crea nuovi intervalli di indirizzi IP per ciascuna istanza della rete su richiesta. Per ogni istanza della rete, nell'endpoint del provider IPAM di terze parti viene creato un set interno di indirizzi IP definito con uno o più intervalli. Gli intervalli IP allocano gli indirizzi IP per le macchine nella rete nella stessa distribuzione. Poiché all'interno di un singolo spazio degli indirizzi non possono esistere indirizzi IP duplicati, per ciascuna istanza di una rete viene creato un nuovo spazio degli indirizzi. Quando una rete NAT viene eliminata i suoi intervalli vengono eliminati nel provider IPAM e nel nuovo spazio degli indirizzi.

È possibile utilizzare gli intervalli di indirizzi IP ricavati dall'endpoint IPAM di VMware specificato o da un endpoint del provider di servizi IPAM di terze parti registrato e configurato in vRealize Orchestrator, ad esempio Infoblox IPAM. Durante l'allocazione, viene creato un intervallo di indirizzi IP da un blocco IP.

Per una rete NAT One-to-Many, è possibile definire regole NAT che possono essere configurate quando si aggiunge un componente di rete NAT al blueprint. È possibile modificare una regola NAT quando si modifica la rete NAT in una distribuzione.

Procedura

1 [Indicazione delle informazioni sul profilo di rete NAT con un endpoint IPAM di terze parti](#)

Le informazioni di un profilo di rete identificano le proprietà della rete NAT, il profilo della rete esterna sottostante e altri valori utilizzati nel provisioning della rete quando si utilizza un endpoint IPAM di terze parti.

2 [Configurazione di intervalli di indirizzi IP di profili di rete NAT con un endpoint IPAM di terze parti](#)

È possibile definire uno o più intervalli di indirizzi IP da utilizzare nel provisioning di una rete utilizzando NAT.

Indicazione delle informazioni sul profilo di rete NAT con un endpoint IPAM di terze parti

Le informazioni di un profilo di rete identificano le proprietà della rete NAT, il profilo della rete esterna sottostante e altri valori utilizzati nel provisioning della rete quando si utilizza un endpoint IPAM di terze parti.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Creare un profilo di rete esterna. Vedere [Creazione di un profilo di rete esterna mediante l'endpoint IPAM fornito](#) o [Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti](#).
- Creare e configurare un endpoint IPAM di terze parti. Vedere [Creazione di un endpoint di un provider IPAM di terze parti](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **NAT** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Se sono stati specificati uno o più endpoint di provider IPAM di terze parti, selezionare un endpoint IPAM di terze parti nel menu a discesa **Endpoint IPAM**.

Quando si seleziona l'endpoint di un provider IPAM di terze parti registrato in vRealize Orchestrator, gli indirizzi IP vengono ottenuti dal provider del servizio IPAM specificato.

- 5 Selezionare un profilo di rete esterno esistente dal menu a discesa **Profilo di rete esterno**.

Sono elencati e disponibili per la selezione solo i profili di rete esterni configurati per l'utilizzo dell'endpoint IPAM specificato.

- 6 Selezionare un tipo di traduzione degli indirizzi di rete One-to-One o One-to-Many dal menu a discesa **Tipo NAT**.

Opzione	Descrizione
One-to-One	Assegnare un indirizzo IP statico esterno a ciascuna scheda di rete. Ogni macchina può accedere alla rete esterna ed è accessibile dalla rete esterna. Tutti gli indirizzi IP esterni assegnati a un uplink edge di NSX devono far parte della stessa subnet. Quando si utilizza NAT one-to-one in vRealize Automation, il profilo di rete esterno corrispondente deve contenere solo intervalli di indirizzi IP appartenenti a una singola subnet.
One-to-Many	<p>Un indirizzo IP esterno è condiviso da tutte le macchine della rete. Una macchina interna può utilizzare solo indirizzi IP statici. Ogni macchina può accedere alla rete esterna, ma nessuna macchina è accessibile dalla rete esterna.</p> <p>Il protocollo DHCP non è supportato quando si utilizza NAT con un provider IPAM di terze parti.</p> <p>Per NSX for vSphere, il tipo di traduzione NAT One-to-Many consente di definire regole NAT quando si aggiunge un componente di rete NAT a un blueprint.</p> <p>NSX for vSphere supporta reti NAT One-to-One e NAT One-to-Many, ma NSX-T supporta solo reti NAT one-to-many.</p>

- 7 Immettere la subnet mask IP nella casella di testo **Subnet mask**.

La subnet mask indica la dimensione dell'intero spazio degli indirizzi instradabili che si desidera definire per il profilo di rete.

Ad esempio, immettere 255.255.0.0.

- 8 Immettere l'indirizzo di un gateway instradato, ad esempio 10.10.110.1, nella casella di testo **Gateway**.

L'indirizzo IP del gateway definito nel profilo di rete viene assegnato alla NIC durante l'allocazione. Il gateway è necessario per i profili di rete NAT.

Per NSX-T, il gateway predefinito del server DHCP corrisponde al gateway predefinito NAT One-to-Many. Il gateway predefinito del pool di IP corrisponde al gateway predefinito NAT One-to-Many in vRealize Automation.

Se nella casella di testo **Gateway** del profilo di rete non è assegnato alcun valore, è necessario utilizzare la proprietà personalizzata `VirtualMachine.Network0.Gateway` per assegnare un gateway.

- 9 Fare clic sulla scheda **DNS**.

10 Immettere i valori di DNS e WINS secondo necessità.

Utilizzare i valori DNS per la registrazione e la risoluzione dei nomi. I valori sono facoltativi per un IPAM interno. I valori vengono forniti dal provider IPAM di terze parti per un IPAM esterno.

- a (Facoltativo) Immettere un valore del server **DNS primario**.
- b (Facoltativo) Immettere un valore del server **DNS secondario**.
- c (Facoltativo) Immettere un valore per i **suffissi DNS**.
- d (Facoltativo) Immettere un valore per i **suffissi di ricerca DNS**.
- e (Facoltativo) Immettere un valore del server **WINS preferito**.
- f (Facoltativo) Immettere un valore del server **WINS alternativo**.

Operazioni successive

[Configurazione di intervalli di indirizzi IP di profili di rete NAT con un endpoint IPAM di terze parti.](#)

Configurazione di intervalli di indirizzi IP di profili di rete NAT con un endpoint IPAM di terze parti
È possibile definire uno o più intervalli di indirizzi IP da utilizzare nel provisioning di una rete utilizzando NAT.

Prerequisiti

[Indicazione delle informazioni sul profilo di rete NAT con un endpoint IPAM di terze parti.](#)

Procedura

- 1** Per creare un intervallo di rete o selezionare un intervallo di rete esistente, fare clic sulla scheda **Intervalli di rete**.

- 2** Fare clic su **Nuovo** e definire un intervallo di rete.

- a Immettere un nome e una descrizione per l'intervallo di rete.
- b Immettere gli indirizzi IP iniziale e finale per definire l'intervallo.
- c Fare clic su **Applica**.

- 3** Fare clic su **OK**.

Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP vengono visualizzati quando si fa clic su **Applica** o dopo che si salva e quindi si modifica il profilo di rete.

- 4** Per visualizzare gli indirizzi IP per l'intervallo di rete denominato, fare clic sulla scheda **Indirizzi IP**.

- 5** (Facoltativo) Per filtrare le voci degli indirizzi IP, selezionare un indirizzo IP dal menu a discesa **Intervallo di rete**.

È possibile visualizzare informazioni relative agli intervalli di rete definiti, agli intervalli di rete importati da un file CSV oppure a un intervallo di rete denominato.

- 6** (Facoltativo) Per filtrare gli indirizzi IP che corrispondono allo stato dell'IP, selezionare un tipo di stato dal menu a discesa **Stato IP**.

Per gli indirizzi IP con stato Scaduto o Eliminato, fare clic su **Recupera** per renderli disponibili per l'allocazione. È necessario salvare il profilo affinché il recupero abbia effetto.

L'aggiornamento della colonna di stato da Expired o Destroyed a Allocated può richiedere qualche secondo.

- 7** Fare clic su **OK**.

Creazione di un profilo di rete privata per una rete su richiesta in vRealize Automation

È possibile creare una rete privata per NSX for vSphere che utilizza la specifica IPAM fornita con vRealize Automation.

È possibile creare un profilo di rete privata su richiesta per NSX for vSphere relativo a un profilo di rete esterno.

Le reti private non sono disponibili per NSX-T.

Le reti private non sono disponibili per IPAM di terze parti.

È possibile definire uno o più intervalli di indirizzi IP statici da utilizzare nel provisioning di una rete.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1** Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2** Fare clic su **Nuovo** e selezionare **Privato** dal menu a discesa.
- 3** Immettere un nome e, facoltativamente, una descrizione.
- 4** Accettare il valore **Endpoint IPAM** predefinito per l'endpoint IPAM di **vRealize Automation**.
- 5** Selezionare l'ID del tenant come richiesto.
- 6** Immettere la subnet mask IP nella casella di testo **Subnet mask**.

La subnet mask indica la dimensione dell'intero spazio degli indirizzi instradabili che si desidera definire per il profilo di rete.

Ad esempio, immettere 255.255.0.0.

- 7** Immettere l'indirizzo di un gateway instradato, ad esempio 10.10.110.1, nella casella di testo **Gateway**.

L'indirizzo IP del gateway definito nel profilo di rete viene assegnato alla NIC durante l'allocazione. Se nella casella di testo **Gateway** del profilo di rete non è assegnato alcun valore, è necessario utilizzare la proprietà personalizzata `VirtualMachine.Network0.Gateway` per assegnare un gateway.

- 8** Fare clic sulla scheda **DNS**.

9 Immettere i valori di DNS e WINS secondo necessità.

Se si tenta di salvare un profilo che contiene intervalli di indirizzi che si sovrappongono, vRealize Automation mostra un errore di convalida.

10 Per creare un intervallo di rete o selezionare un intervallo di rete esistente, fare clic sulla scheda **Intervalli di rete**.**11** Per immettere manualmente un nuovo nome di intervallo di rete e un nuovo intervallo di indirizzi IP, fare clic su **Nuovo** o per importare le informazioni relative agli IP da un file CSV formattato correttamente, fare clic su **Importa da CSV**.■ Fare clic su **Nuovo**.

- a Assegnare un nome all'intervallo di rete.
- b Immettere una descrizione dell'intervallo di rete.
- c Immettere l'indirizzo IP iniziale dell'intervallo.
- d Immettere l'indirizzo IP finale dell'intervallo.

■ Fare clic su **Importa da CSV**.

- a Individuare e selezionare il file CSV o trascinarlo nella finestra di dialogo **Importa da CSV**.

Una riga del file CSV ha il seguente formato: *ip_address, machine_name, status, NIC offset*. Ad esempio:

```
100.10.100.1,mymachine01,Allocated,0
```

Campo CSV	Descrizione
ip_address	Un indirizzo IP in formato IPv4.
machine_name	Nome di una macchina gestita in vRealize Automation. Se il campo è vuoto, il valore predefinito è senza nome. Se il campo è vuoto, il valore del campo status non può essere Allocated.
status	Allocato o Non allocato, viene fatta distinzione tra lettere maiuscole e minuscole. Se il campo è vuoto, il valore predefinito è Non allocato. Se lo stato è Allocated, il campo machine_name non può essere vuoto.
NIC_offset	Un numero intero non negativo. Lo scarto NIC indica la NIC della macchina virtuale a cui è assegnato l'indirizzo IP. Se una macchina virtuale alloca più indirizzi IP per NIC diverse, è presente una voce di indirizzo IP per ogni NIC che contiene lo scarto NIC corrispondente. Se si imposta il valore 0, non viene specificato alcuno scarto.

- b Fare clic su **Applica**.

12 Fare clic su **OK**.

Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP vengono visualizzati quando si fa clic su **Applica** o dopo che si salva e quindi si modifica il profilo di rete.

13 Per visualizzare gli indirizzi IP per l'intervallo di rete denominato, fare clic sulla scheda **Indirizzi IP**.

14 (Facoltativo) Per filtrare le voci degli indirizzi IP, selezionare un indirizzo IP dal menu a discesa **Intervallo di rete**.

È possibile visualizzare informazioni relative agli intervalli di rete definiti, agli intervalli di rete importati da un file CSV oppure a un intervallo di rete denominato.

15 (Facoltativo) Per filtrare gli indirizzi IP che corrispondono allo stato dell'IP, selezionare un tipo di stato dal menu a discesa **Stato IP**.

Per gli indirizzi IP con stato Scaduto o Eliminato, fare clic su **Recupera** per renderli disponibili per l'allocazione. È necessario salvare il profilo affinché il recupero abbia effetto.

L'aggiornamento della colonna di stato da Expired o Destroyed a Allocated può richiedere qualche secondo.

16 Fare clic su **OK**.

Rilascio di indirizzi IP mediante l'eliminazione di macchine con provisioning

Quando si elimina una distribuzione, gli indirizzi IP ad essa associati vengono eliminati. Gli indirizzi IP allocati, ad esempio gli indirizzi IP dell'intervallo di un profilo di rete, vengono rilasciati e resi disponibili per il provisioning successivo.

Quando si elimina una macchina che ha un indirizzo IP statico, il suo indirizzo IP viene reso disponibile per essere utilizzato da altre macchine. Gli indirizzi non utilizzati potrebbero non essere disponibili immediatamente in quanto il processo di recupero degli indirizzi IP statici viene eseguito ogni trenta minuti.

Se si utilizza un provider IPAM di terze parti, vRealize Automation elimina gli indirizzi IP associati utilizzando il workflow di vRealize Orchestrator disponibile nel plug-in o nel pacchetto del provider IPAM.

Configurazione di prenotazione e criteri di prenotazione

Una prenotazione di vRealize Automation può definire criteri, priorità e quote che determinano il posizionamento delle macchine per le richieste di provisioning.

I criteri di prenotazione limitano il provisioning delle macchine a un sottoinsieme di prenotazioni disponibili. I criteri di prenotazione storage consentono agli architetti di blueprint di assegnare volumi di macchine a datastore differenti.

Per eseguire il provisioning correttamente, la prenotazione deve avere spazio di storage disponibile sufficiente. La disponibilità dello spazio di storage della prenotazione dipende dai seguenti fattori:

- Quantità di storage disponibile sul datastore/cluster.
- Quantità di storage riservata per questo cluster di datastore/cluster.
- Quantità di storage già allocato in vRealize Automation

Ad esempio, anche se il vCenter Server dispone di spazio di storage disponibile per il datastore/cluster, se non è stato prenotato spazio di storage sufficiente, il provisioning non riesce e termina con un errore "Nessuna prenotazione disponibile per...". Lo storage allocato su una prenotazione dipende dal numero di macchine virtuali (indipendentemente dal loro stato) in quella specifica prenotazione. Vedere l'articolo della Knowledge Base di VMware *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* all'indirizzo <http://kb.vmware.com/kb/2151030> per ulteriori informazioni.

Prenotazioni

È possibile creare una prenotazione di vRealize Automation per allocare risorse con provisioning nel gruppo di strutture per un gruppo di business specifico.

Ad esempio, è possibile utilizzare le prenotazioni per specificare che una quota delle risorse di memoria, CPU, rete e storage di una singola risorsa di elaborazione appartenga a un gruppo di business specifico o che determinate macchine siano allocate a un gruppo di business specifico.

Un criterio di prenotazione della rete consente di gestire le comunicazioni di rete per le distribuzioni del blueprint. Quando si richiede il provisioning di una macchina, viene utilizzato il criterio di prenotazione per raggruppare le prenotazioni che possono essere considerate per la distribuzione.

Non è possibile condividere prenotazioni tra più gruppi di business.

Nota Lo storage e la memoria assegnati a una macchina sottoposta a provisioning da una prenotazione vengono rilasciati quando la macchina a cui sono assegnati viene eliminata in vRealize Automation dall'azione di eliminazione. La memoria e lo storage non vengono rilasciati se la macchina viene eliminata in vCenter Server.

È possibile creare una prenotazione per i seguenti tipi di macchine:

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Microsoft Azure
- Hyper V (SCVMM)
- Hyper-V autonomo
- KVM (RHEV)
- OpenStack
- XenServer

È possibile configurare le impostazioni di sicurezza specificando le informazioni in una prenotazione, in un blueprint o in uno script dell'agente guest. Se le macchine richiedono un agente guest, aggiungere una regola di sicurezza alla prenotazione o al blueprint.

Scelta di uno scenario di prenotazione

È possibile creare prenotazioni per allocare risorse destinate a gruppi di business. La procedura di creazione di una prenotazione varia in base allo scenario esistente.

Scegliere uno scenario di prenotazione in base al tipo di endpoint di destinazione.

Ogni gruppo di business deve avere almeno una prenotazione per i suoi membri per eseguire il provisioning di macchine di quel tipo. Ad esempio, un gruppo di business con una prenotazione OpenStack ma non una prenotazione Amazon, non può richiedere una macchina da Amazon. In questo esempio, al gruppo di business è necessario allocare una prenotazione specifica per risorse di Amazon.

Tabella 2-15. Scelta di uno scenario di prenotazione

Scenario	Procedura
Creare una prenotazione di vSphere.	Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer
Creare una prenotazione per allocare risorse per un endpoint vCloud Air.	Creazione di una prenotazione di vCloud Air
Creare una prenotazione per allocare risorse per un endpoint vCloud Director.	Creazione di una prenotazione di vCloud Director
Creare una prenotazione per allocare risorse su una risorsa di Amazon (con o senza l'uso di Amazon Virtual Private Cloud).	Creazione di una prenotazione Amazon EC2
Creare una prenotazione per allocare risorse su una risorsa OpenStack.	Creazione di una prenotazione di OpenStack
Creare una prenotazione per allocare risorse per Hyper-V.	Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer
Creare una prenotazione per allocare risorse per KVM.	Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer
Creare una prenotazione per allocare risorse su una risorsa OpenStack.	Creazione di una prenotazione di OpenStack
Creare una prenotazione per allocare risorse per SCVMM.	Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer
Creare una prenotazione per allocare risorse per XenServer.	Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer
Creare una prenotazione per allocare risorse per Microsoft Azure.	Creazione di una prenotazione per Microsoft Azure

Creazione di prenotazioni di categoria cloud

Una prenotazione di tipo categoria cloud fornisce l'accesso ai servizi di provisioning di un account di servizi cloud per un particolare gruppo di business di vRealize Automation. I tipi di prenotazioni cloud disponibili sono Amazon, OpenStack, vCloud Air e vCloud Director.

Una prenotazione è una condivisione di risorse di memoria, CPU, rete e storage di una singola risorsa di elaborazione allocata a un gruppo di business di vRealize Automation specifico.

Un gruppo di business può avere più prenotazioni su un endpoint o prenotazioni su più endpoint.

Il modello di allocazione di una prenotazione dipende dal modello di allocazione nel data center associato. I modelli di allocazione disponibili sono Pool allocazione, Pagamento a consumo e pool prenotazione. Per informazioni sui modelli di allocazione, vedere la documentazione di vCloud Director o vCloud Air.

Oltre a definire la quota di risorse di struttura allocate al gruppo di business, una prenotazione può definire criteri, priorità e quote che determinano il posizionamento della macchina.

Per eseguire il provisioning correttamente, la prenotazione deve avere spazio di storage disponibile sufficiente. La disponibilità dello spazio di storage della prenotazione dipende dai seguenti fattori:

- Quantità di storage disponibile sul datastore/cluster.
- Quantità di storage riservata per questo cluster di datastore/cluster.
- Quantità di storage già allocato in vRealize Automation

Ad esempio, anche se il vCenter Server dispone di spazio di storage disponibile per il datastore/cluster, se non è stato prenotato spazio di storage sufficiente, il provisioning non riesce e termina con un errore "Nessuna prenotazione disponibile per...". Lo storage allocato su una prenotazione dipende dal numero di macchine virtuali (indipendentemente dal loro stato) in quella specifica prenotazione. Vedere l'articolo della Knowledge Base di VMware *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* all'indirizzo <http://kb.vmware.com/kb/2151030> per ulteriori informazioni.

Logica di selezione delle prenotazioni cloud

Quando un membro di un gruppo di business crea una richiesta di provisioning per una macchina cloud, vRealize Automation seleziona una macchina da una delle prenotazioni disponibili per quel gruppo di business. Le prenotazioni cloud includono Amazon, OpenStack, vCloud Air e vCloud Director.

La prenotazione per cui viene eseguito il provisioning di una macchina deve soddisfare i seguenti criteri:

- La prenotazione deve essere dello stesso tipo di piattaforma del blueprint da cui la macchina è stata richiesta.
- La prenotazione deve essere attivata.
- La prenotazione deve avere capacità rimanente nella sua quota macchina o avere una quota illimitata.

La quota della macchina allocata include solo le macchine accese. Se ad esempio una prenotazione ha una quota pari a 50, e 40 macchine sono state fornite in provisioning ma solo 20 di esse sono accese, la quota della prenotazione è allocata per il 40 per cento, non per l'80 per cento.

- La prenotazione deve avere i gruppi di sicurezza specificati nella richiesta della macchina.
- La prenotazione deve essere associata a una regione con l'immagine della macchina specificata nel blueprint.

- La prenotazione deve avere risorse di memoria e storage non allocate sufficienti a eseguire il provisioning della macchina.

In una prenotazione con Pagamento a consumo, le risorse possono essere illimitate.

- Per le macchine Amazon, la richiesta specifica una zona di disponibilità e se alla macchina deve essere fornita una subnet in un Virtual Private Cloud (VPC) o in una posizione non VPC. La prenotazione deve corrispondere allo stesso tipo di rete (VPC o non VPC).
- Per vCloud Air o vCloud Director, se la richiesta specifica un modello di allocazione, il data center virtuale associato alla prenotazione deve avere lo stesso modello di allocazione.
- Per vCloud Director o vCloud Air, l'organizzazione specificata deve essere attivata.
- Tutti i modelli di blueprint devono essere disponibili sulla prenotazione. Se il criterio di prenotazione è associato a più di una risorsa, i modelli devono essere pubblici.
- Se il provider di cloud supporta la selezione di rete e il blueprint ha impostazioni di rete specifiche, la prenotazione deve avere le stesse reti.

Se il blueprint o la prenotazione presentano un profilo di rete con assegnazione di indirizzi IP statici, deve essere disponibile un indirizzo IP da assegnare alla nuova macchina.

- Se la richiesta specifica un modello di allocazione, il modello di allocazione nella prenotazione deve corrispondere al modello di allocazione nella richiesta.
- Se il blueprint specifica un criterio di prenotazione, la prenotazione deve appartenere a quel criterio di prenotazione.

I criteri di prenotazione permettono di assicurarsi che la prenotazione selezionata rispetti tutti i requisiti aggiuntivi per il provisioning di macchine da uno specifico blueprint. Ad esempio, se un blueprint utilizza una specifica immagine di macchina, è possibile utilizzare criteri di prenotazione per limitare il provisioning a prenotazioni associate alle regioni che hanno l'immagine richiesta.

Se non sono disponibili prenotazioni che soddisfano tutti i criteri di selezione, il provisioning non riesce.

Se i criteri sono soddisfatti da più prenotazioni, la prenotazione da cui eseguire il provisioning di una macchina richiesta viene determinata in base alla seguente logica.

- Una prenotazione con un valore di priorità minore viene selezionata prima di una prenotazione con un valore di priorità maggiore.
- Se ci sono più prenotazioni con la stessa priorità, viene selezionata la prenotazione con la percentuale più bassa della propria quota macchina allocata.
- Se più prenotazioni hanno la stessa priorità e lo stesso uso della quota, le macchine vengono distribuite tra le prenotazioni in modalità round robin.

Nota Sebbene la selezione round robin di profili di rete non sia supportata, la selezione round robin di reti (se esistente) è supportata ed è possibile associarla a diversi profili di rete.

Se su una prenotazione sono disponibili più percorsi di storage con capacità sufficienti al provisioning dei volumi delle macchine, i percorsi di storage vengono selezionati in base alla seguente logica.

- Un percorso di storage con un valore di priorità minore viene selezionato prima di un percorso di storage con un valore di priorità maggiore.
- Se il blueprint o la richiesta specificano un criterio di prenotazione storage, il percorso di storage deve appartenere a quel criterio di prenotazione storage.

Se la proprietà personalizzata `VirtualMachine.DiskN.StorageReservationPolicyMode` è impostata su `Not Exact` e non c'è un percorso di storage con capacità sufficiente all'interno del criterio di prenotazione storage, il provisioning procede con un percorso di storage esterno al criterio di prenotazione storage specificato. Il valore predefinito di `VirtualMachine.DiskN.StorageReservationPolicyMode` è `Exact`.

- Se più percorsi di storage hanno la stessa priorità, le macchine vengono distribuite tra percorsi di storage utilizzando una pianificazione round robin.

Creazione di una prenotazione Amazon EC2

È necessario allocare risorse per le macchine creando una prenotazione prima che i membri di un gruppo di business possano richiedere il provisioning della macchina.

È possibile lavorare con prenotazioni Amazon per Amazon Virtual Private Cloud o non VPC Amazon. Gli utenti di Amazon Web Services possono creare un Amazon Virtual Private Cloud per progettare una topologia di rete virtuale in base alle specifiche richieste. Se si intende utilizzare Amazon VPC, è necessario assegnare un Amazon VPC a una prenotazione di vRealize Automation.

Quando si crea una prenotazione Amazon o si configura un componente macchina nel blueprint, è possibile scegliere nell'elenco dei gruppi di sicurezza disponibili per la regione Amazon specificata. I gruppi di sicurezza vengono importati durante la raccolta dati.

Nota dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business o risorse di elaborazione.

Per informazioni sulla creazione di un Amazon VPC utilizzando la AWS Management Console, vedere la documentazione di Amazon Web Services.

Procedura

1 Definizione di informazioni sulle prenotazioni Amazon

Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

2 Definizione delle impostazioni di risorse e rete per prenotazioni Amazon

Specificare le impostazioni delle risorse e della rete disponibili per il provisioning di macchine da questa prenotazione di vRealize Automation.

3 Definizione di proprietà personalizzate e avvisi per prenotazioni Amazon

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Definizione di informazioni sulle prenotazioni Amazon

Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

Nota dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business o risorse di elaborazione.

È possibile controllare la visualizzazione delle prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per categoria** della pagina Prenotazioni. Si noti che le prenotazioni dell'agente di test non vengono riportate nell'elenco delle prenotazioni quando viene applicato il filtro per categoria.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Verificare che un amministratore tenant abbia creato almeno un gruppo di business.
- Verificare che esista una risorsa di elaborazione.
- Configurare le impostazioni di rete.
- (Facoltativo) Configurare le informazioni del profilo di rete.
- Assicurarsi di avere accesso a una rete Amazon desiderata. Ad esempio, se si desidera utilizzare VPC, assicurarsi di avere accesso a una rete Amazon Virtual Private Cloud (VPC).
- Verificare l'esistenza di tutte le coppie di chiavi richieste. Vedere [Gestione delle coppie di chiavi](#).

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Fare clic sull'icona **Nuovo** (+) e selezionare il tipo di prenotazione da creare.
Selezionare **Amazon EC2**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare un tenant dal menu a discesa **Tenant**.
- 5 Selezionare un gruppo di business dal menu a discesa **Gruppo di business**.

Solo gli utenti appartenenti a questo gruppo di business possono eseguire il provisioning di macchine utilizzando questa prenotazione.

6 (Facoltativo) Selezionare un criterio di prenotazione dal menu a discesa **Criterio di prenotazione**.

Questa opzione richiede l'esistenza di uno o più criteri di prenotazione. È possibile modificare la prenotazione in un secondo momento per specificare un criterio di prenotazione.

Il criterio di prenotazione consente di limitare il provisioning a prenotazioni specifiche.

7 Immettere un numero nella casella di testo **Priorità** per impostare la priorità per la prenotazione.

La priorità viene utilizzata quando un gruppo di business ha più di una prenotazione. Per il provisioning viene utilizzata una prenotazione con priorità 1 rispetto a una con priorità 2.

8 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

Risultati

Non lasciare questa pagina. La prenotazione non è completa.

Definizione delle impostazioni di risorse e rete per prenotazioni Amazon

Specificare le impostazioni delle risorse e della rete disponibili per il provisioning di macchine da questa prenotazione di vRealize Automation.

Quando si crea una prenotazione Amazon o si configura un componente macchina nel blueprint, è possibile scegliere dall'elenco dei gruppi di sicurezza che sono disponibili nella regione dell'account Amazon specificato. I gruppi di sicurezza vengono importati durante la raccolta dati. Un gruppo di sicurezza agisce come un firewall per controllare l'accesso a una macchina. Ogni regione include almeno il gruppo di sicurezza predefinito. Gli amministratori possono utilizzare la Amazon Web Services Management Console per creare gruppi di sicurezza aggiuntivi, configurare porte per Microsoft Remote Desktop Protocol o SSH e configurare una rete privata virtuale per una Amazon VPN. Per informazioni sulla creazione e l'uso dei gruppi di sicurezza in Amazon Web Services, consultare la documentazione di Amazon.

Per informazioni correlate ai bilanciamenti del carico, vedere *Configurazione di vRealize Automation*.

Prerequisiti

[Definizione di informazioni sulle prenotazioni Amazon.](#)

Procedura

- 1** Fare clic sulla scheda **Risorse**.
- 2** Selezionare una risorsa di elaborazione su cui eseguire il provisioning delle macchine dal menu a discesa **Risorse di elaborazione**.

Vengono elencate le regioni di Amazon disponibili.

- 3 (Facoltativo) Immettere un numero nella casella di testo **Quota macchina** per impostare il numero massimo di macchine di cui è possibile eseguire il provisioning con questa prenotazione.

Nella quota vengono conteggiate solo le macchine accese. Lasciare vuoto il campo per rendere illimitata la prenotazione.

- 4 Selezionare un metodo di assegnazione delle coppie di chiavi alle istanze di elaborazione dal menu a discesa **Coppia di chiavi**.

Opzione	Descrizione
Non specificato	Controlla il comportamento della coppia di chiavi al livello del blueprint invece che al livello di prenotazione.
Generato automaticamente per gruppo di business	Ogni macchina fornita in provisioning nello stesso gruppo di business ha la stessa coppia di chiavi, incluse le macchine fornite in provisioning su altre prenotazioni quando la macchina ha la stessa risorsa di elaborazione e lo stesso gruppo di business. Dato che le coppie di chiavi generate con questa modalità sono associate a un gruppo di business, le coppie di chiavi vengono eliminate quando il gruppo di business viene eliminato.
Generato automaticamente per macchina	Ogni macchina ha una coppia di chiavi univoca. Questo è il metodo più sicuro perché non vengono condivise coppie di chiave tra macchine.
Coppia chiavi specifica	Tutte le macchine fornite in provisioning su questa prenotazione hanno la stessa coppia di chiavi. Selezionare la coppia di chiavi da utilizzare per la prenotazione.

- 5 Se è stata selezionata l'opzione **Coppia chiavi specifica** nel menu a discesa **Coppia di chiavi**, selezionare il valore della coppia di chiavi dal menu a discesa **Coppia chiavi specifica**.

- 6 Se la propria configurazione prevede un Virtual Private Cloud di Amazon, selezionare la casella di controllo **Assegna a una subnet in un VPC**. In caso contrario, lasciare la casella deselezionata.

Se si seleziona **Assegna a una subnet in un VPC**, le seguenti opzioni di posizioni o subnet, gruppi di sicurezza e bilanciamenti del carico vengono visualizzate all'interno di un menu di scelta rapida e non nella stessa pagina.

Per la prenotazione di un VPC, specificare i gruppi di sicurezza e le subnet per ciascun VPC consentito nella prenotazione.

- 7 Selezionare una o più posizioni (non VPC) o subnet (VPC) disponibili dall'elenco **Posizioni o Subnet**.

Selezionare tutte le posizioni o subnet disponibili che si desidera rendere utilizzabili per il provisioning.

- 8 Selezionare uno o più gruppi di sicurezza che possono essere assegnati a una macchina durante il provisioning dall'elenco **Gruppi di sicurezza**.

Selezionare tutti i gruppi di sicurezza che possono essere assegnati a una macchina durante il provisioning. Ogni regione disponibile richiede almeno un gruppo di sicurezza specificato.

- 9 Selezionare uno o più bilanciamenti del carico disponibili dall'elenco **Bilanciamenti del carico**.

Se si utilizza una funzione di bilanciamento del carico flessibile, selezionare uno o più bilanciamenti del carico disponibili da applicare alle posizioni o alle subnet selezionate.

Risultati

A questo punto è possibile salvare la prenotazione facendo clic su **Salva**. Oppure è possibile aggiungere proprietà personalizzate per controllare ulteriormente le specifiche della prenotazione. Inoltre è possibile configurare avvisi via email da inviare quando le risorse allocate a questa prenotazione si approssimano all'esaurimento.

Definizione di proprietà personalizzate e avvisi per prenotazioni Amazon

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Le proprietà personalizzate e gli avvisi via email sono configurazioni opzionali per la prenotazione. Se non si desidera associare proprietà personalizzate o impostare avvisi, fare clic su **Salva** per completare la creazione della prenotazione.

È possibile aggiungere tutte le proprietà personalizzate di cui si ha bisogno.

Se configurati, gli avvisi vengono generati quotidianamente e non al raggiungimento delle soglie specificate.

Importante le notifiche vengono inviate solo se gli avvisi via email sono configurati e le notifiche attivate.

Prerequisiti

[Definizione delle impostazioni di risorse e rete per prenotazioni Amazon.](#)

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Fare clic su **Nuovo**.
- 3 Immettere un nome valido per la proprietà personalizzata.
- 4 Se applicabile, immettere un valore per la proprietà.
- 5 Fare clic su **Salva**.
- 6 (Facoltativo) Aggiungere eventuali proprietà personalizzate aggiuntive.
- 7 Fare clic sulla scheda **Avvisi**.
- 8 Selezionare la casella di controllo **Avvisi capacità** per configurare gli avvisi da inviare.
- 9 Utilizzare il cursore per impostare le soglie per l'allocazione delle risorse disponibili.

- 10** Nella casella di testo **Destinatari**, immettere i nomi dei gruppi o degli utenti di AD (non gli indirizzi email) a cui inviare le notifiche di avviso.

Immettere un nome in ogni riga. Premere Invio per separare voci multiple.

- 11** Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.

Gli avvisi tramite email vengono inviati agli utenti inclusi nell'elenco **Invia email manager a** del gruppo di business.

- 12** Specificare una frequenza per i promemoria (giorni).

- 13** Fare clic su **Salva**.

Risultati

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Operazioni successive

È possibile configurare criteri di prenotazione opzionali o iniziare la preparazione per il provisioning.

Gli utenti autorizzati a creare blueprint a questo punto possono farlo.

Creazione di una prenotazione di OpenStack

È necessario allocare risorse per le macchine creando una prenotazione prima che i membri di un gruppo di business possano richiedere il provisioning della macchina.

Creare una prenotazione di OpenStack.

Procedura

1 Definizione di informazioni sulle prenotazioni di OpenStack

Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

2 Definizione delle impostazioni di risorse e rete per prenotazioni di OpenStack

Specificare le impostazioni delle risorse e della rete disponibili per le macchine di cui viene eseguito il provisioning da questa prenotazione di vRealize Automation.

3 Definizione di proprietà personalizzate e avvisi per prenotazioni OpenStack

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Definizione di informazioni sulle prenotazioni di OpenStack

Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

Nota dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business o risorse di elaborazione.

È possibile controllare la visualizzazione delle prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per categoria** della pagina Prenotazioni. Si noti che le prenotazioni dell'agente di test non vengono riportate nell'elenco delle prenotazioni quando viene applicato il filtro per categoria.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Verificare che un amministratore tenant abbia creato almeno un gruppo di business.
- Verificare che esista una risorsa di elaborazione.
- Verificare che siano configurati i gruppi di sicurezza facoltativi o gli indirizzi IP mobili necessari.
- Verificare l'esistenza di tutte le coppie di chiavi richieste. Vedere [Gestione delle coppie di chiavi](#).
- Verificare che esista una risorsa di elaborazione.
- Configurare le impostazioni di rete.

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Fare clic sull'icona **Nuovo** (+) e selezionare il tipo di prenotazione da creare.
Selezionare **OpenStack**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare un tenant dal menu a discesa **Tenant**.
- 5 Selezionare un gruppo di business dal menu a discesa **Gruppo di business**.
Solo gli utenti appartenenti a questo gruppo di business possono eseguire il provisioning di macchine utilizzando questa prenotazione.
- 6 (Facoltativo) Selezionare un criterio di prenotazione dal menu a discesa **Criterio di prenotazione**.

Questa opzione richiede l'esistenza di uno o più criteri di prenotazione. È possibile modificare la prenotazione in un secondo momento per specificare un criterio di prenotazione.

Il criterio di prenotazione consente di limitare il provisioning a prenotazioni specifiche.

- 7 Immettere un numero nella casella di testo **Priorità** per impostare la priorità per la prenotazione.

La priorità viene utilizzata quando un gruppo di business ha più di una prenotazione. Per il provisioning viene utilizzata una prenotazione con priorità 1 rispetto a una con priorità 2.

- 8 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

Risultati

Non lasciare questa pagina. La prenotazione non è completa.

Definizione delle impostazioni di risorse e rete per prenotazioni di OpenStack

Specificare le impostazioni delle risorse e della rete disponibili per le macchine di cui viene eseguito il provisioning da questa prenotazione di vRealize Automation.

Prerequisiti

[Definizione di informazioni sulle prenotazioni di OpenStack.](#)

Procedura

- 1 Fare clic sulla scheda **Risorse**.
- 2 Selezionare una risorsa di elaborazione su cui eseguire il provisioning delle macchine dal menu a discesa **Risorse di elaborazione**.

Per la clonazione con questa prenotazione sono disponibili solo i modelli localizzati sul cluster selezionato.

Durante il provisioning, le macchine vengono posizionate in un host collegato allo storage locale. Se la prenotazione utilizza lo storage locale, tutte le macchine sottoposte a provisioning dalla prenotazione vengono create nell'host che contiene lo storage locale specificato. Tuttavia, se si utilizza la proprietà personalizzata di `VirtualMachine.Admin.ForceHost`, che forza il provisioning di una macchina in un altro host, il provisioning non riesce. Il provisioning non riesce neanche nel caso in cui il modello da cui viene clonata la macchina si trova nello storage locale, ma collegato a una macchina in un altro cluster. In tal caso, il provisioning non riesce poiché non è in grado di accedere al modello.

- 3 (Facoltativo) Immettere un numero nella casella di testo **Quota macchina** per impostare il numero massimo di macchine di cui è possibile eseguire il provisioning con questa prenotazione.

Nella quota vengono conteggiate solo le macchine accese. Lasciare vuoto il campo per rendere illimitata la prenotazione.

- 4 Selezionare un metodo di assegnazione delle coppie di chiavi alle istanze di elaborazione dal menu a discesa **Coppia di chiavi**.

Opzione	Descrizione
Non specificato	Controlla il comportamento della coppia di chiavi al livello del blueprint invece che al livello di prenotazione.
Generato automaticamente per gruppo di business	Ogni macchina fornita in provisioning nello stesso gruppo di business ha la stessa coppia di chiavi, incluse le macchine fornite in provisioning su altre prenotazioni quando la macchina ha la stessa risorsa di elaborazione e lo stesso gruppo di business. Dato che le coppie di chiavi generate con questa modalità sono associate a un gruppo di business, le coppie di chiavi vengono eliminate quando il gruppo di business viene eliminato.
Generato automaticamente per macchina	Ogni macchina ha una coppia di chiavi univoca. Questo è il metodo più sicuro perché non vengono condivise coppie di chiave tra macchine.
Coppia chiavi specifica	Tutte le macchine fornite in provisioning su questa prenotazione hanno la stessa coppia di chiavi. Selezionare la coppia di chiavi da utilizzare per la prenotazione.

- 5 Se è stata selezionata l'opzione **Coppia chiavi specifica** nel menu a discesa **Coppia di chiavi**, selezionare il valore della coppia di chiavi dal menu a discesa **Coppia chiavi specifica**.

- 6 Selezionare uno o più gruppi di sicurezza che possono essere assegnati a una macchina durante il provisioning dall'elenco **Gruppi di sicurezza**.

- 7 Fare clic sulla scheda **Rete**.

- 8 Configurare un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.

- a (Facoltativo) Se l'opzione è disponibile, selezionare un endpoint di storage dal menu a discesa **Endpoint**.

L'opzione FlexClone è mostrata nella colonna dell'endpoint se esiste un endpoint NetApp ONTAP e se l'host è virtuale. Se c'è un endpoint NetApp ONTAP, la pagina della prenotazione mostra l'endpoint assegnato al percorso di storage. Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile in tutte le prenotazioni applicabili.

Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile nella pagina della prenotazione.

- b Selezionare una o più **Schede di rete** per le macchine da sottoporre a provisioning per questa prenotazione.

- c (Facoltativo) Selezionare un **Profilo di rete** disponibile per ciascuna scheda di rete selezionata.
- d (Facoltativo) Se sono disponibili le impostazioni avanzate, selezionare una **Zona di trasporto** e uno o più **Router logici di livello 0** da utilizzare quando si distribuisce un blueprint che contiene i bilanciamenti del carico.

Una zona di trasporto definisce quali cluster possono rientrare nelle schede di rete. Se si specifica una zona di trasporto in una prenotazione e in un blueprint, i valori della zona di trasporto devono corrispondere.

È possibile selezionare più di una scheda di rete in una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

Risultati

A questo punto è possibile salvare la prenotazione facendo clic su **Salva**. Oppure è possibile aggiungere proprietà personalizzate per controllare ulteriormente le specifiche della prenotazione. Inoltre è possibile configurare avvisi via email da inviare quando le risorse allocate a questa prenotazione si approssimano all'esaurimento.

Definizione di proprietà personalizzate e avvisi per prenotazioni OpenStack

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Le proprietà personalizzate e gli avvisi via email sono configurazioni opzionali per la prenotazione. Se non si desidera associare proprietà personalizzate o impostare avvisi, fare clic su **Salva** per completare la creazione della prenotazione.

È possibile aggiungere tutte le proprietà personalizzate di cui si ha bisogno.

Importante le notifiche vengono inviate solo se gli avvisi via email sono configurati e le notifiche attivate.

Se configurati, gli avvisi vengono generati quotidianamente e non al raggiungimento delle soglie specificate.

Prerequisiti

[Definizione delle impostazioni di risorse e rete per prenotazioni di OpenStack.](#)

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Fare clic su **Nuovo**.
- 3 Immettere un nome valido per la proprietà personalizzata.
- 4 Se applicabile, immettere un valore per la proprietà.
- 5 Fare clic su **Salva**.

- 6 (Facoltativo) Aggiungere eventuali proprietà personalizzate aggiuntive.
- 7 Fare clic sulla scheda **Avvisi**.
- 8 Selezionare la casella di controllo **Avvisi capacità** per configurare gli avvisi da inviare.
- 9 Utilizzare il cursore per impostare le soglie per l'allocazione delle risorse disponibili.
- 10 Nella casella di testo **Destinatari**, immettere i nomi dei gruppi o degli utenti di AD (non gli indirizzi email) a cui inviare le notifiche di avviso.

Immettere un nome in ogni riga. Premere Invio per separare voci multiple.
- 11 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.

Gli avvisi tramite email vengono inviati agli utenti inclusi nell'elenco **Invia email manager a** del gruppo di business.
- 12 Specificare una frequenza per i promemoria (giorni).
- 13 Fare clic su **Salva**.

Risultati

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Operazioni successive

È possibile configurare criteri di prenotazione opzionali o iniziare la preparazione per il provisioning.

Gli utenti autorizzati a creare blueprint a questo punto possono farlo.

Creazione di una prenotazione di vCloud Air

È necessario allocare risorse per le macchine creando una prenotazione di vRealize Automation prima che i membri di un gruppo di business possano richiedere il provisioning della macchina.

Ogni gruppo di business deve avere almeno una prenotazione per i suoi membri per eseguire il provisioning di macchine di quel tipo.

Procedura

1 Definizione delle informazioni sulle prenotazioni di vCloud Air

È possibile creare una prenotazione per ogni sottoscrizione di macchina di vCloud Air o risorsa OnDemand. Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste.

2 Definizione delle impostazioni di risorse e rete per una prenotazione di vCloud Air

Specificare le impostazioni delle risorse e della rete disponibili per le macchine vCloud Air di cui viene eseguito il provisioning da questa prenotazione di vRealize Automation.

3 Definizione di proprietà personalizzate e avvisi per una prenotazione di vCloud Air

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Definizione delle informazioni sulle prenotazioni di vCloud Air

È possibile creare una prenotazione per ogni sottoscrizione di macchina di vCloud Air o risorsa OnDemand. Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste.

È possibile controllare la visualizzazione delle prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per categoria** della pagina Prenotazioni. Si noti che le prenotazioni dell'agente di test non vengono riportate nell'elenco delle prenotazioni quando viene applicato il filtro per categoria.

Nota dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business o risorse di elaborazione.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Verificare che un amministratore tenant abbia creato almeno un gruppo di business.
- Verificare che esista una risorsa di elaborazione.
- Configurare le impostazioni di rete.
- (Facoltativo) Configurare le informazioni del profilo di rete.

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Fare clic sull'icona **Nuovo** (+) e selezionare il tipo di prenotazione da creare.
I tipi di prenotazioni cloud disponibili sono Amazon, OpenStack, vCloud Air e vCloud Director.
Selezionare **vCloud Air**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare un tenant dal menu a discesa **Tenant**.
- 5 Selezionare un gruppo di business dal menu a discesa **Gruppo di business**.
Solo gli utenti appartenenti a questo gruppo di business possono eseguire il provisioning di macchine utilizzando questa prenotazione.
- 6 (Facoltativo) Selezionare un criterio di prenotazione dal menu a discesa **Criterio di prenotazione**.
Questa opzione richiede l'esistenza di uno o più criteri di prenotazione. È possibile modificare la prenotazione in un secondo momento per specificare un criterio di prenotazione.

Il criterio di prenotazione consente di limitare il provisioning a prenotazioni specifiche.

- 7 Immettere un numero nella casella di testo **Priorità** per impostare la priorità per la prenotazione.

La priorità viene utilizzata quando un gruppo di business ha più di una prenotazione. Per il provisioning viene utilizzata una prenotazione con priorità 1 rispetto a una con priorità 2.

- 8 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

Risultati

Non lasciare questa pagina. La prenotazione non è completa.

Definizione delle impostazioni di risorse e rete per una prenotazione di vCloud Air

Specificare le impostazioni delle risorse e della rete disponibili per le macchine vCloud Air di cui viene eseguito il provisioning da questa prenotazione di vRealize Automation.

I modelli di allocazione risorse disponibili per le macchine fornite in provisioning da una prenotazione di vCloud Director sono Pool allocazione, Pagamento a consumo e Pool prenotazione. Per il Pagamento a consumo non è necessario specificare le quantità di storage o memoria, ma è necessario specificare una priorità per il percorso di storage. Per informazioni dettagliate su questi modelli di allocazione, vedere la documentazione di vCloud Air.

È possibile specificare un profilo di storage standard o a livello di disco. Lo storage su disco multilivello è disponibile per gli endpoint vCloud Air.

Per integrazioni che utilizzano lo storage Storage Distributed Resource Scheduler (SDRS), è possibile selezionare un cluster di storage per consentire a SDRS di gestire automaticamente la disposizione dello storage e il bilanciamento del carico per le macchine fornite in provisioning da questa prenotazione. La modalità di automazione SDRS deve essere impostata su Automatico. Altrimenti, selezionare un datastore all'interno del cluster per un funzionamento da datastore autonomo. SDRS non è supportata per i dispositivi di storage FlexClone.

Nota Le prenotazioni definite per gli endpoint vCloud Air e gli endpoint vCloud Director non supportano l'uso di profili di rete per il provisioning delle macchine.

Prerequisiti

[Definizione delle informazioni sulle prenotazioni di vCloud Director.](#)

Procedura

- 1 Fare clic sulla scheda **Risorse**.
- 2 Selezionare una risorsa di elaborazione su cui eseguire il provisioning delle macchine dal menu a discesa **Risorse di elaborazione**.

Per la clonazione con questa prenotazione sono disponibili solo i modelli localizzati sul cluster selezionato.

- 3 Selezionare un modello di allocazione.

- 4 (Facoltativo) Immettere un numero nella casella di testo **Quota macchina** per impostare il numero massimo di macchine di cui è possibile eseguire il provisioning con questa prenotazione.

Nella quota vengono conteggiate solo le macchine accese. Lasciare vuoto il campo per rendere illimitata la prenotazione.

- 5 Specificare la quantità di memoria, espressa in GB, da allocare per questa prenotazione dalla tabella Memoria.

Il valore di memoria totale per la prenotazione dipende dalla risorsa di elaborazione selezionata.

- 6 Selezionare uno o più percorsi di storage elencati.

Le opzioni del percorso di storage disponibili dipendono dalla risorsa di elaborazione selezionata.

- a Immettere un valore nella casella di testo **Questa prenotazione riservata** per specificare la quantità di storage da allocare per la prenotazione.
- b Immettere un valore nella casella di testo **Priorità** per specificare il valore di priorità per il percorso di storage in relazione agli altri percorsi di storage correlati a questa prenotazione.

La priorità è utilizzata quando ci sono percorsi di storage multipli. Un percorso di storage con priorità 0 viene utilizzato prima di uno con priorità 1.

- c Fare clic sull'opzione **Disattiva** se non si desidera tenere attivo il percorso di storage per essere utilizzato da parte di questa prenotazione.
- d Ripetere questo passaggio per configurare cluster e datastore secondo necessità.

- 7 Fare clic sulla scheda **Rete**.

- 8 Configurare un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.

- a (Facoltativo) Se l'opzione è disponibile, selezionare un endpoint di storage dal menu a discesa **Endpoint**.

L'opzione FlexClone è mostrata nella colonna dell'endpoint se esiste un endpoint NetApp ONTAP e se l'host è virtuale. Se c'è un endpoint NetApp ONTAP, la pagina della prenotazione mostra l'endpoint assegnato al percorso di storage. Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile in tutte le prenotazioni applicabili.

Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile nella pagina della prenotazione.

- b Selezionare una o più **Schede di rete** per le macchine da sottoporre a provisioning per questa prenotazione.

- c (Facoltativo) Selezionare un **Profilo di rete** disponibile per ciascuna scheda di rete selezionata.
- d (Facoltativo) Se sono disponibili le impostazioni avanzate, selezionare una **Zona di trasporto** e uno o più **Router logici di livello 0** da utilizzare quando si distribuisce un blueprint che contiene i bilanciamenti del carico.

Una zona di trasporto definisce quali cluster possono rientrare nelle schede di rete. Se si specifica una zona di trasporto in una prenotazione e in un blueprint, i valori della zona di trasporto devono corrispondere.

È possibile selezionare più di una scheda di rete in una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

Risultati

A questo punto è possibile salvare la prenotazione facendo clic su **Salva**. Oppure è possibile aggiungere proprietà personalizzate per controllare ulteriormente le specifiche della prenotazione. Inoltre è possibile configurare avvisi via email da inviare quando le risorse allocate a questa prenotazione si approssimano all'esaurimento.

Definizione di proprietà personalizzate e avvisi per una prenotazione di vCloud Air

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Le proprietà personalizzate e gli avvisi via email sono configurazioni opzionali per la prenotazione. Se non si desidera associare proprietà personalizzate o impostare avvisi, fare clic su **Salva** per completare la creazione della prenotazione.

È possibile aggiungere tutte le proprietà personalizzate di cui si ha bisogno.

Se configurati, gli avvisi vengono generati quotidianamente e non al raggiungimento delle soglie specificate.

Importante le notifiche vengono inviate solo se gli avvisi via email sono configurati e le notifiche attivate.

Gli avvisi non sono disponibili per le prenotazioni Pagamento a consumo che sono state create senza specificare limiti.

Prerequisiti

[Definizione delle impostazioni di risorse e rete per una prenotazione di vCloud Air](#)

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Fare clic su **Nuovo**.
- 3 Immettere un nome valido per la proprietà personalizzata.
- 4 Se applicabile, immettere un valore per la proprietà.

- 5 (Facoltativo) Selezionare la casella di controllo **Codificato** per crittografare il valore della proprietà.
- 6 (Facoltativo) Selezionare la casella di controllo **Richiedi conferma** per richiedere l'immissione di un valore da parte dell'utente.
Questa opzione non può essere sovrascritta durante il provisioning.
- 7 Fare clic su **Salva**.
- 8 (Facoltativo) Aggiungere eventuali proprietà personalizzate aggiuntive.
- 9 Fare clic sulla scheda **Avvisi**.
- 10 Selezionare la casella di controllo **Avvisi capacità** per configurare gli avvisi da inviare.
- 11 Utilizzare il cursore per impostare le soglie per l'allocazione delle risorse disponibili.
- 12 Nella casella di testo **Destinatari**, immettere i nomi dei gruppi o degli utenti di AD (non gli indirizzi email) a cui inviare le notifiche di avviso.
Immettere un nome in ogni riga. Premere Invio per separare voci multiple.
- 13 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.
Gli avvisi tramite email vengono inviati agli utenti inclusi nell'elenco **Invia email manager a** del gruppo di business.
- 14 Specificare una frequenza per i promemoria (giorni).
- 15 Fare clic su **Salva**.

Risultati

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Creazione di una prenotazione di vCloud Director

È necessario allocare risorse per le macchine creando una prenotazione di vRealize Automation prima che i membri di un gruppo di business possano richiedere il provisioning della macchina.

Ogni gruppo di business deve avere almeno una prenotazione per i suoi membri per eseguire il provisioning di macchine di quel tipo.

Procedura

1 Definizione delle informazioni sulle prenotazioni di vCloud Director

È possibile creare una prenotazione per ogni virtual data center (VDC) di organizzazione di vCloud Director. Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

2 Definizione delle impostazioni di risorse e rete per una prenotazione di vCloud Director

Specificare le impostazioni delle risorse e della rete disponibili per le macchine vCloud Director di cui viene eseguito il provisioning da questa prenotazione di vRealize Automation.

3 Definizione di proprietà personalizzate e avvisi per le prenotazioni di vCloud Director

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Operazioni successive

È possibile configurare criteri di prenotazione opzionali o iniziare la preparazione per il provisioning.

Gli utenti autorizzati a creare blueprint a questo punto possono farlo.

Definizione delle informazioni sulle prenotazioni di vCloud Director

È possibile creare una prenotazione per ogni virtual data center (VDC) di organizzazione di vCloud Director. Ogni prenotazione è configurata per concedere a un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

È possibile controllare la visualizzazione delle prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per categoria** della pagina Prenotazioni. Si noti che le prenotazioni dell'agente di test non vengono riportate nell'elenco delle prenotazioni quando viene applicato il filtro per categoria.

Nota dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business o risorse di elaborazione.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Verificare che un amministratore tenant abbia creato almeno un gruppo di business.
- Verificare che esista una risorsa di elaborazione.
- Configurare le impostazioni di rete.
- (Facoltativo) Configurare le informazioni del profilo di rete.

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Fare clic sull'icona **Nuovo** (+) e selezionare il tipo di prenotazione da creare.
I tipi di prenotazioni cloud disponibili sono Amazon, OpenStack, vCloud Air e vCloud Director.
Selezionare **vCloud Director**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare un tenant dal menu a discesa **Tenant**.
- 5 Selezionare un gruppo di business dal menu a discesa **Gruppo di business**.
Solo gli utenti appartenenti a questo gruppo di business possono eseguire il provisioning di macchine utilizzando questa prenotazione.

6 (Facoltativo) Selezionare un criterio di prenotazione dal menu a discesa **Criterio di prenotazione**.

Questa opzione richiede l'esistenza di uno o più criteri di prenotazione. È possibile modificare la prenotazione in un secondo momento per specificare un criterio di prenotazione.

Il criterio di prenotazione consente di limitare il provisioning a prenotazioni specifiche.

7 Immettere un numero nella casella di testo **Priorità** per impostare la priorità per la prenotazione.

La priorità viene utilizzata quando un gruppo di business ha più di una prenotazione. Per il provisioning viene utilizzata una prenotazione con priorità 1 rispetto a una con priorità 2.

8 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

Risultati

Non lasciare questa pagina. La prenotazione non è completa.

Definizione delle impostazioni di risorse e rete per una prenotazione di vCloud Director
Specificare le impostazioni delle risorse e della rete disponibili per le macchine vCloud Director di cui viene eseguito il provisioning da questa prenotazione di vRealize Automation.

I modelli di allocazione risorse disponibili per le macchine fornite in provisioning da una prenotazione di vCloud Director sono Pool allocazione, Pagamento a consumo e Pool prenotazione. Per il Pagamento a consumo non è necessario specificare le quantità di storage o memoria, ma è necessario specificare una priorità per il percorso di storage. Per informazioni dettagliate su questi modelli di allocazione, vedere la documentazione di vCloud Director.

È possibile specificare un profilo di storage standard o a livello di disco. Lo storage su disco multilivello è disponibile per gli endpoint vCloud Director 5.6 e superiori. Lo storage su disco multilivello non è supportato per gli endpoint vCloud Director 5.5.

Per integrazioni che utilizzano lo storage Storage Distributed Resource Scheduler (SDRS), è possibile selezionare un cluster di storage per consentire a SDRS di gestire automaticamente la disposizione dello storage e il bilanciamento del carico per le macchine fornite in provisioning da questa prenotazione. La modalità di automazione SDRS deve essere impostata su Automatico. Altrimenti, selezionare un datastore all'interno del cluster per un funzionamento da datastore autonomo. SDRS non è supportata per i dispositivi di storage FlexClone.

Nota Le prenotazioni definite per gli endpoint vCloud Air e gli endpoint vCloud Director non supportano l'uso di profili di rete per il provisioning delle macchine.

Prerequisiti

[Definizione delle informazioni sulle prenotazioni di vCloud Director.](#)

Procedura

1 Fare clic sulla scheda **Risorse**.

- 2 Selezionare una risorsa di elaborazione su cui eseguire il provisioning delle macchine dal menu a discesa **Risorse di elaborazione**.

Per la clonazione con questa prenotazione sono disponibili solo i modelli localizzati sul cluster selezionato.

- 3 Selezionare un modello di allocazione.

- 4 (Facoltativo) Immettere un numero nella casella di testo **Quota macchina** per impostare il numero massimo di macchine di cui è possibile eseguire il provisioning con questa prenotazione.

Nella quota vengono conteggiate solo le macchine accese. Lasciare vuoto il campo per rendere illimitata la prenotazione.

- 5 Specificare la quantità di memoria, espressa in GB, da allocare per questa prenotazione dalla tabella Memoria.

Il valore di memoria totale per la prenotazione dipende dalla risorsa di elaborazione selezionata.

- 6 Selezionare uno o più percorsi di storage elencati.

Le opzioni del percorso di storage disponibili dipendono dalla risorsa di elaborazione selezionata.

- a Immettere un valore nella casella di testo **Questa prenotazione riservata** per specificare la quantità di storage da allocare per la prenotazione.
- b Immettere un valore nella casella di testo **Priorità** per specificare il valore di priorità per il percorso di storage in relazione agli altri percorsi di storage correlati a questa prenotazione.

La priorità è utilizzata quando ci sono percorsi di storage multipli. Un percorso di storage con priorità 0 viene utilizzato prima di uno con priorità 1.

- c Fare clic sull'opzione **Disattiva** se non si desidera tenere attivo il percorso di storage per essere utilizzato da parte di questa prenotazione.
- d Ripetere questo passaggio per configurare cluster e datastore secondo necessità.

- 7 Fare clic sulla scheda **Rete**.

8 Configurare un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.

- a (Facoltativo) Se l'opzione è disponibile, selezionare un endpoint di storage dal menu a discesa **Endpoint**.

L'opzione FlexClone è mostrata nella colonna dell'endpoint se esiste un endpoint NetApp ONTAP e se l'host è virtuale. Se c'è un endpoint NetApp ONTAP, la pagina della prenotazione mostra l'endpoint assegnato al percorso di storage. Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile in tutte le prenotazioni applicabili.

Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile nella pagina della prenotazione.

- b Selezionare una o più **Schede di rete** per le macchine da sottoporre a provisioning per questa prenotazione.
- c (Facoltativo) Selezionare un **Profilo di rete** disponibile per ciascuna scheda di rete selezionata.
- d (Facoltativo) Se sono disponibili le impostazioni avanzate, selezionare una **Zona di trasporto** e uno o più **Router logici di livello 0** da utilizzare quando si distribuisce un blueprint che contiene i bilanciamenti del carico.

Una zona di trasporto definisce quali cluster possono rientrare nelle schede di rete. Se si specifica una zona di trasporto in una prenotazione e in un blueprint, i valori della zona di trasporto devono corrispondere.

È possibile selezionare più di una scheda di rete in una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

Risultati

A questo punto è possibile salvare la prenotazione facendo clic su **Salva**. Oppure è possibile aggiungere proprietà personalizzate per controllare ulteriormente le specifiche della prenotazione. Inoltre è possibile configurare avvisi via email da inviare quando le risorse allocate a questa prenotazione si approssimano all'esaurimento.

Definizione di proprietà personalizzate e avvisi per le prenotazioni di vCloud Director

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Le proprietà personalizzate e gli avvisi via email sono configurazioni opzionali per la prenotazione. Se non si desidera associare proprietà personalizzate o impostare avvisi, fare clic su **Salva** per completare la creazione della prenotazione.

È possibile aggiungere tutte le proprietà personalizzate di cui si ha bisogno.

Se configurati, gli avvisi vengono generati quotidianamente e non al raggiungimento delle soglie specificate.

Importante le notifiche vengono inviate solo se gli avvisi via email sono configurati e le notifiche attivate.

Gli avvisi non sono disponibili per le prenotazioni Pagamento a consumo che sono state create senza specificare limiti.

Prerequisiti

[Definizione delle impostazioni di risorse e rete per una prenotazione di vCloud Director.](#)

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Fare clic su **Nuovo**.
- 3 Immettere un nome valido per la proprietà personalizzata.
- 4 Se applicabile, immettere un valore per la proprietà.
- 5 (Facoltativo) Selezionare la casella di controllo **Codificato** per crittografare il valore della proprietà.
- 6 (Facoltativo) Selezionare la casella di controllo **Richiedi conferma** per richiedere l'immissione di un valore da parte dell'utente.

Questa opzione non può essere sovrascritta durante il provisioning.

- 7 Fare clic su **Salva**.
- 8 (Facoltativo) Aggiungere eventuali proprietà personalizzate aggiuntive.
- 9 Fare clic sulla scheda **Avvisi**.
- 10 Selezionare la casella di controllo **Avvisi capacità** per configurare gli avvisi da inviare.
- 11 Utilizzare il cursore per impostare le soglie per l'allocazione delle risorse disponibili.
- 12 Nella casella di testo **Destinatari**, immettere i nomi dei gruppi o degli utenti di AD (non gli indirizzi email) a cui inviare le notifiche di avviso.

Immettere un nome in ogni riga. Premere Invio per separare voci multiple.

- 13 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.

Gli avvisi tramite email vengono inviati agli utenti inclusi nell'elenco **Invia email manager a** del gruppo di business.

- 14 Specificare una frequenza per i promemoria (giorni).
- 15 Fare clic su **Salva**.

Risultati

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Creazione di una prenotazione per Microsoft Azure

Creare una prenotazione Azure per uno specifico gruppo di business in modo da consentire agli utenti di tale gruppo di richiedere macchine virtuali Azure su una determinata risorsa di elaborazione.

Se la distribuzione supporta il Single Sign-On tramite un tunnel VPN, è possibile configurare il supporto per questa funzionalità sulle macchine virtuali Azure utilizzando le impostazioni nella scheda Proprietà.

Nota Ignorare la scheda Avvisi durante la creazione di prenotazioni Azure in quanto non è applicabile. Dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business. Inoltre, a differenza di altri tipi di macchina, non vi è un collegamento diretto fra una prenotazione e un blueprint Azure.

È possibile controllare la visualizzazione delle prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per categoria** della pagina Prenotazioni. Si noti che le prenotazioni dell'agente di test non vengono riportate nell'elenco delle prenotazioni quando viene applicato il filtro per categoria.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Verificare che un amministratore tenant abbia creato almeno un gruppo di business.
- (Facoltativo) Configurare le informazioni del profilo di rete.
- Verificare di avere accesso alle risorse Azure desiderate.
- Verificare l'esistenza di tutte le coppie di chiavi richieste. Vedere *Configurazione di vRealize Automation* per informazioni sulle coppie di chiavi.
- Richiedere un ID sottoscrizione di Azure che corrisponda a quello utilizzato con l'endpoint Azure pertinente. Se si utilizzano più sottoscrizioni per Azure, è necessario creare una prenotazione per ciascun ID sottoscrizione.
- Se la distribuzione supporta il Single Sign-On tramite un tunnel VPN, è necessario configurare la connettività VPC appropriata prima di creare una prenotazione. Vedere [Configurazione della connettività VPC da rete ad Azure](#).

Procedura

- 1 [Configurazione delle informazioni di prenotazione di base di Microsoft Azure](#)
Specificare le informazioni di base per una prenotazione di Microsoft Azure.

2 Configurazione delle informazioni sulle risorse per le prenotazioni Azure

Quando si configura una prenotazione Azure, è possibile specificare informazioni su un gruppo di risorse e un account di storage in base all'istanza di Azure in uso. In fase di configurazione, la logica di provisioning di vRealize Automation tenta di allocare le risorse, ad esempio account di storage e gruppi di risorse, in base alle informazioni sulle risorse specificate nella prenotazione durante il provisioning di una macchina virtuale.

3 Configurazione delle proprietà di Azure

È possibile aggiungere proprietà personalizzate a una prenotazione Azure per supportare opzioni quali il tunneling VPN e consentire la comunicazione tra più reti. Questa funzionalità facilita inoltre l'aggiunta di componenti software ai blueprint.

4 Configurazione delle informazioni sulla rete per le prenotazioni Azure

È possibile configurare le informazioni sulla rete virtuale e sul bilanciamento del carico per una macchina virtuale Azure nella prenotazione.

Configurazione delle informazioni di prenotazione di base di Microsoft Azure

Specificare le informazioni di base per una prenotazione di Microsoft Azure.

Tutte le informazioni nella pagina Informazioni prenotazione sono obbligatorie, ad eccezione del criterio di prenotazione. Tutte le informazioni nelle pagine delle prenotazioni Azure successive sono opzionali.

Procedura

1 Selezionare **Infrastrutture > Amministrazione > Prenotazioni**.

2 Fare clic sull'icona **Nuovo** (+) e selezionare il tipo di prenotazione da creare.

Selezionare **Azure**.

3 Immettere un nome nella casella di testo **Nome**.

4 Selezionare un gruppo di business dal menu a discesa **Gruppo di business**.

Solo gli utenti appartenenti a questo gruppo di business possono eseguire il provisioning di macchine utilizzando questa prenotazione.

5 Ignorare la casella di testo **Criterio di prenotazione**, poiché non si applica alle prenotazioni di Azure.

6 Immettere un numero nella casella di testo **Priorità** per impostare la priorità per la prenotazione.

La priorità viene utilizzata quando un gruppo di business ha più di una prenotazione. Per il provisioning viene utilizzata una prenotazione con priorità 1 rispetto a una con priorità 2.

7 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

8 Fare clic su **OK**.

Configurazione delle informazioni sulle risorse per le prenotazioni Azure

Quando si configura una prenotazione Azure, è possibile specificare informazioni su un gruppo di risorse e un account di storage in base all'istanza di Azure in uso. In fase di configurazione, la logica di provisioning di vRealize Automation tenta di allocare le risorse, ad esempio account di storage e gruppi di risorse, in base alle informazioni sulle risorse specificate nella prenotazione durante il provisioning di una macchina virtuale.

È possibile configurare le informazioni sul Gruppo di risorse e sull'Account di storage per una macchina virtuale Azure nella prenotazione, ma è anche possibile scegliere di lasciare vuoti questi campi. Se non si specifica alcun valore, per i blueprint correlati vengono utilizzate le informazioni predefinite sul gruppo di risorse e sull'account di storage associate all'ID della sottoscrizione ad Azure specificato. È anche possibile aggiornare queste informazioni durante la creazione di un blueprint o l'esecuzione del provisioning di una macchina virtuale.

Prerequisiti

Ottenere l'ID della sottoscrizione all'istanza di Azure.

Procedura

- 1 Immettere l'ID di sottoscrizione ad Azure nella casella di testo **ID sottoscrizione**.
- 2 Selezionare la posizione della prenotazione facendo clic sull'elenco a discesa **Posizione**.
È possibile lasciare vuoto questo campo per creare una prenotazione senza posizione. Se invece si sceglie di specificare la posizione, le informazioni devono essere immesse durante la creazione di un blueprint o durante il provisioning di una macchina virtuale Azure.
- 3 Fare clic su **Nuovo** nella tabella Gruppi di risorse.
 - a Immettere le informazioni appropriate sul nome del gruppo di risorse dall'istanza di Azure nella casella di testo **Nome**.

Nota La casella **Nome** non può essere vuota.

- b Assegnare un valore di priorità numerica nella casella di testo **Priorità**.
Questa assegnazione consente di determinare la priorità quando un gruppo di risorse include più gruppi di risorse, a partire dai numeri più bassi che hanno la precedenza.
 - c Fare clic su **Salva** per aggiungere il gruppo di risorse alla prenotazione.
- 4 Fare clic su **Nuovo** nella tabella Account di storage.
 - a Immettere le informazioni appropriate sul nome dell'account di storage dall'istanza di Azure nella casella di testo **Nome**.

Nota La casella **Nome** non può essere vuota.

- b Assegnare un valore di priorità numerica nella casella di testo **Priorità**.
 - c Far clic su **Salva** per aggiungere l'account di storage alla prenotazione.
Questa assegnazione consente di determinare la priorità quando una prenotazione include più account di storage, a partire dai numeri più bassi che hanno la precedenza.

5 Fare clic su **OK** per passare alla scheda successiva.

Configurazione delle proprietà di Azure

È possibile aggiungere proprietà personalizzate a una prenotazione Azure per supportare opzioni quali il tunneling VPN e consentire la comunicazione tra più reti. Questa funzionalità facilita inoltre l'aggiunta di componenti software ai blueprint.

È necessario creare proprietà personalizzate che definiscono gli URL appropriati per supportare il tunneling VPN nella propria rete. Inoltre, è necessario creare proprietà che definiscono il percorso degli script di configurazione del tunneling Azure scaricati in precedenza.

Utilizzare l'indirizzo IP privato della macchina fisica del tunnel di Azure e la porta 1443, assegnata per *vRealize_automation_appliance_fqdn* quando è stato invocato il tunnel SSH.

Nella tabella seguente vengono riportati i nomi e i valori delle proprietà richieste per supportare il tunneling VPN.

Nome	Valore
Azure.Windows.ScriptPath	Specifica il percorso dello script scaricato che configura il tunneling per i sistemi basati su Windows. Aggiornare il percorso in base alla propria distribuzione.
Azure.Linux.ScriptPath	Specifica il percorso dello script scaricato che configura il tunneling per i sistemi basati su Linux. Aggiornare il percorso in base alla propria distribuzione.
agent.download.url	Specifica l'URL dell'agente VPN nella propria distribuzione. Il formato dell'URL è <code>https:// Private_IP:1443/software-service/resources/noble-agent.jar</code>
software.agent.service.url	Immettere l'URL del servizio dell'agente software VPN per la propria distribuzione, utilizzando il seguente formato URL: <code>https:// Private_IP:1443/software-service/api</code>
software.ebs.url	Immettere l'URL del servizio del gestore degli eventi per la propria distribuzione. Il formato URL è <code>https:// Private_IP:1443/event-broker-service/api</code>

Prerequisiti

- Scaricare gli script Azure forniti da VMware dalla pagina **Guest and Software Agent Installers** (Programmi di installazione degli agenti guest e software) nella propria appliance vRealize Automation.

Questi script consentono di installare le estensioni Azure richieste per supportare il tunneling VPN. Sono disponibili due script: `script.ps1` e `script.sh`. Il file `.ps1` è destinato ai sistemi Windows, mentre il file `.sh` è destinato ai sistemi Linux.

- Eseguire `https://vrealize-automation-appliance-fqdn/software` per aprire la pagina dell'appliance vRealize Automation VMware.
- Fare clic sul collegamento **Guest and software agents** (Agenti guest e software) sotto l'intestazione Per installare i componenti vRealize Automation (IaaS, agenti guest e software, strumenti).

- c Scaricare i file di script Azure sotto l'intestazione Macchine Azure. Salvare i file di script in una posizione appropriata. È necessario puntare a questa posizione quando vengono configurate le proprietà personalizzate delle prenotazioni Azure.

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Fare clic su **Nuovo**.
- 3 Immettere Nome e Valore appropriati per la proprietà personalizzata nella finestra di dialogo Proprietà.
- 4 Mentre viene creata ciascuna proprietà, fare clic su **OK** nella finestra di dialogo per aggiungerla.
- 5 Quando si termina di aggiungere tutte le proprietà richieste, fare clic su **OK** per salvare le impostazioni.

Operazioni successive

Una volta create le proprietà personalizzate per supportare il tunneling VPN, è possibile creare componenti software per i blueprint Azure. Vedere *Configurazione di vRealize Automation* per ulteriori informazioni.

Quando viene impostato un componente software per Azure, selezionare **Macchina virtuale Azure** nel menu a discesa Contenitore nella pagina Nuovo software.

Configurazione delle informazioni sulla rete per le prenotazioni Azure

È possibile configurare le informazioni sulla rete virtuale e sul bilanciamento del carico per una macchina virtuale Azure nella prenotazione.

È anche possibile scegliere di lasciare completamente o parzialmente vuota questa pagina e configurare le informazioni sulla rete virtuale e sul bilanciamento del carico durante il provisioning di una macchina virtuale.

Se si specifica un profilo di rete senza indicare una subnet, viene utilizzato come nome di subnet il nome del primo intervallo di rete esistente del profilo di rete specificato. Se si specifica un profilo di rete, è possibile scegliere di lasciare vuota la casella di testo Rete virtuale. In questo caso, come nome di subnet viene utilizzato il nome del primo intervallo di rete del profilo di rete specificato e il nome della Rete virtuale viene risolto nella prima rete virtuale di Azure contenente una subnet valida.

Prerequisiti

Ottenere le informazioni appropriate sulla rete virtuale e sul bilanciamento del carico dall'istanza di Azure, se disponibili.

Procedura

- 1 Fare clic su **Nuovo** nella tabella Reti per configurare la rete virtuale di Azure appropriata da utilizzare con la macchina virtuale.

- a Incollare le informazioni corrette sul nome della rete virtuale dall'istanza di Azure nella casella di testo **Rete virtuale**.
- b Incollare le informazioni corrette sul nome della subnet dall'istanza di Azure nella casella di testo **Subnet**.

La specifica della subnet è facoltativa. Se si lascia vuota questa casella, per impostazione predefinita viene utilizzata la subnet della rete virtuale specificata.

- c Digitare o incollare il nome corretto nella casella di testo **Profilo di rete**. È possibile utilizzare il profilo di rete del blueprint per associare una scheda di interfaccia di rete a una rete.

La specifica del profilo di rete è facoltativa. Utilizzarla se si desidera creare il blueprint in base al profilo di rete definito in vRealize Automation anziché abbinarlo ai costrutti di rete di Azure.

- d Assegnare un valore numerico di priorità nella casella di testo **Priorità**, se applicabile.

Questa assegnazione consente di determinare la priorità quando una rete virtuale include più prenotazioni, a partire dai numeri più bassi che hanno la precedenza.

- e Fare clic su **Salva** per aggiungere il gruppo di risorse alla prenotazione.

- 2 Fare clic su **Nuovo** nella tabella Bilanciamenti del carico se si stanno distribuendo più macchine e si utilizza un bilanciamento del carico.

- a Incollare il nome corretto del bilanciamento del carico dall'istanza di Azure nella casella di testo **Nome**.
- b Incollare il nome corretto dall'istanza di Azure nella casella di testo **Pool di indirizzi back-end**.
- c Assegnare un valore numerico di priorità nella casella di testo **Priorità**, se applicabile.

Questa assegnazione consente di determinare la priorità quando una rete virtuale include più bilanciamenti del carico, a partire dai numeri più bassi che hanno la precedenza.

- d Fare clic su **Salva** per aggiungere il bilanciamento del carico alla prenotazione.

- 3 Fare clic su **Nuovo** nella tabella Gruppi di sicurezza se si stanno distribuendo più macchine che devono comunicare tramite un firewall.

- a Incollare il nome del gruppo di sicurezza dall'istanza di Azure nella casella di testo **Nome**.
- b Assegnare un valore numerico di priorità nella casella di testo **Priorità**, se applicabile.

Questa assegnazione consente di determinare la priorità quando una rete virtuale include più gruppi di sicurezza, a partire dai numeri più bassi che hanno la precedenza.

- c Fare clic su **Salva** per aggiungere il gruppo di sicurezza alla prenotazione.

4 Fare clic su **OK**.

Scenario: creazione di una prenotazione Amazon per un ambiente di prototipazione
Poiché è stato utilizzato un tunnel SSH per stabilire temporaneamente la connettività VPC da rete ad Amazon per l'ambiente di prototipazione, è necessario aggiungere proprietà personalizzate alle prenotazioni Amazon per assicurarsi che l'agente di avvio automatico di Software e l'agente guest comunichino attraverso il tunnel.

La connettività VPC da rete ad Amazon è richiesta solo se si desidera utilizzare l'agente guest per personalizzare macchine di cui è stato eseguito il provisioning o se si desidera includere componenti Software nei blueprint. Per un ambiente di produzione, questa connettività dovrebbe essere configurata ufficialmente tramite Amazon Web Services, ma poiché il lavoro si svolge in un ambiente di prototipazione, è stato configurato un tunnel SSH temporaneo.

Utilizzando i privilegi di amministratore di struttura è possibile creare una prenotazione per allocare le risorse di Amazon Web Services e includere diverse proprietà personalizzate per supportare il tunnel SSH. È inoltre possibile configurare la prenotazione con la stessa regione e la stessa VPC della macchina del tunnel.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Configurare un tunnel SSH per stabilire connettività VPC da rete ad Amazon. Annotare la subnet, il gruppo di sicurezza e l'indirizzo IP privato della macchina del tunnel di Amazon Web Services. Vedere [Configurazione della connettività VPC da rete ad Amazon per un ambiente di prototipazione](#).
- Creare un gruppo di per i membri dell'organizzazione IT che devono progettare blueprint nell'ambiente di prototipazione. Vedere [Creazione di un gruppo di business](#).
- Verificare che un amministratore tenant abbia creato almeno un gruppo di business.

Procedura

1 [Scenario: definizione delle informazioni di prenotazione di Amazon Web Services per un ambiente di prototipazione](#)

È possibile riservare risorse per il proprio team di architetti di blueprint per offrire loro la possibilità di testare il funzionamento in un ambiente di prototipazione, procedendo nella configurazione della prenotazione per allocare risorse per il gruppo di business degli architetti.

2 [Scenario: definizione delle impostazioni di rete di Amazon Web Services per un ambiente di prototipazione](#)

È possibile configurare la prenotazione per utilizzare la stessa regione e le stesse impostazioni di rete utilizzate dalla macchina del tunnel, nonché restringere il numero di macchine che possono essere accese per la prenotazione al fine di gestire l'uso delle risorse.

3 Scenario: definizione di proprietà personalizzate per veicolare le comunicazioni degli agenti attraverso un tunnel

Quando è stata configurata la connettività VPC da rete ad Amazon, è stato configurato l'inoltro della porta per consentire alla macchina del tunnel di Amazon Web Services di accedere alle risorse di vRealize Automation.

Scenario: definizione delle informazioni di prenotazione di Amazon Web Services per un ambiente di prototipazione

È possibile riservare risorse per il proprio team di architetti di blueprint per offrire loro la possibilità di testare il funzionamento in un ambiente di prototipazione, procedendo nella configurazione della prenotazione per allocare risorse per il gruppo di business degli architetti.

Nota dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business o risorse di elaborazione.

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Fare clic sull'icona **Nuovo** (+) e selezionare il tipo di prenotazione da creare.
Selezionare **Amazon**.
- 3 Immettere **Amazon Tunnel POC** nella casella di testo **Nome**.
- 4 Selezionare il gruppo di business creato per gli architetti di blueprint dal menu a discesa **Gruppo di business**.
- 5 Immettere un numero **1** nella casella di testo **Priorità** per impostare la prenotazione alla priorità più elevata.

Risultati

Sono stati configurati il gruppo di business e la priorità per la prenotazione, ma occorre ancora allocare le risorse e configurare le proprietà personalizzate per il tunnel SSH.

Scenario: definizione delle impostazioni di rete di Amazon Web Services per un ambiente di prototipazione

È possibile configurare la prenotazione per utilizzare la stessa regione e le stesse impostazioni di rete utilizzate dalla macchina del tunnel, nonché restringere il numero di macchine che possono essere accese per la prenotazione al fine di gestire l'uso delle risorse.

Procedura

- 1 Fare clic sulla scheda **Risorse**.
- 2 Selezionare una risorsa di elaborazione su cui eseguire il provisioning delle macchine dal menu a discesa **Risorse di elaborazione**.

Selezionare la regione di Amazon Web Services in cui è localizzata la macchina del tunnel.

- 3 (Facoltativo) Immettere un numero nella casella di testo **Quota macchina** per impostare il numero massimo di macchine di cui è possibile eseguire il provisioning con questa prenotazione.

Nella quota vengono conteggiate solo le macchine accese. Lasciare vuoto il campo per rendere illimitata la prenotazione.

- 4 Selezionare **Coppia chiavi specifica** dal menu a discesa **Coppia di chiavi**.

Poiché questo è un ambiente di prototipazione, si può scegliere di condividere una singola coppia di chiavi per tutte le macchine con provisioning eseguito utilizzando questa prenotazione.

- 5 Selezionare la coppia di chiavi da condividere con gli utenti architetti dal menu **Coppia di chiavi**.

- 6 Selezionare la casella di controllo **Assegna a una subnet in un VPC**.

- 7 Selezionare la stessa subnet e gli stessi gruppi di sicurezza utilizzati dalla macchina del tunnel.

Risultati

La prenotazione è stata configurata per utilizzare la stessa regione e le stesse impostazioni di rete della macchina del tunnel, ma a questo punto è necessario aggiungere proprietà personalizzate per assicurarsi che l'agente di avvio automatico di Software e l'agente guest comunichino attraverso il tunnel.

Scenario: definizione di proprietà personalizzate per veicolare le comunicazioni degli agenti attraverso un tunnel

Quando è stata configurata la connettività VPC da rete ad Amazon, è stato configurato l'inoltro della porta per consentire alla macchina del tunnel di Amazon Web Services di accedere alle risorse di vRealize Automation.

È necessario aggiungere proprietà personalizzate di tunnel alla prenotazione per configurare gli agenti per accedere a dette porte.

Nota Se si utilizza una rete di sistema PAT o NAT tra la rete dell'organizzazione e la rete di vRealize Automation, è possibile utilizzare tali proprietà per accedere all'indirizzo IP e alla porta privati.

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Fare clic su **Nuovo**.

3 Configurare le proprietà personalizzate del tunnel.

Utilizzare l'indirizzo IP privato della macchina del tunnel di Amazon Web Services e la porta 1443, assegnata per *vRealize_automation_appliance_fqdn* quando è stato invocato il tunnel SSH.

Opzione	Valore
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

4 Fare clic su **Salva**.

Risultati

È stata creata una prenotazione per allocare risorse di Amazon Web Services al gruppo di business degli architetti. È stata configurata la prenotazione per supportare l'agente guest e l'agente di avvio automatico di Software. Gli architetti possono creare blueprint che sfruttano l'agente guest per personalizzare macchine distribuite o includere componenti di Software.

Creazione di prenotazioni di categoria virtuale

Una prenotazione di tipo categoria virtuale fornisce l'accesso ai servizi di provisioning di una distribuzione di macchine virtuali per un particolare gruppo di business di vRealize Automation. I tipi di prenotazioni virtuali disponibili sono vSphere, Hyper-V, KVM, SCVMM e XenServer.

Una prenotazione è una condivisione di risorse di memoria, CPU, rete e storage di una singola risorsa di elaborazione allocata a un gruppo di business di vRealize Automation specifico.

Un gruppo di business può avere più prenotazioni su un endpoint o prenotazioni su più endpoint.

Per eseguire il provisioning di macchine virtuali, un gruppo di business ha bisogno di almeno una prenotazione su una risorsa di elaborazione virtuale. Ogni prenotazione è relativa a un solo gruppo di business, ma un gruppo di business può avere più prenotazioni su una singola risorsa di elaborazione o più prenotazioni su risorse di elaborazione di tipi diversi.

Oltre a definire la quota di risorse di struttura allocate al gruppo di business, una prenotazione può definire criteri, priorità e quote che determinano il posizionamento della macchina.

Per eseguire il provisioning correttamente, la prenotazione deve avere spazio di storage disponibile sufficiente. La disponibilità dello spazio di storage della prenotazione dipende dai seguenti fattori:

- Quantità di storage disponibile sul datastore/cluster.
- Quantità di storage riservata per questo cluster di datastore/cluster.
- Quantità di storage già allocato in vRealize Automation

Ad esempio, anche se il vCenter Server dispone di spazio di storage disponibile per il datastore/cluster, se non è stato prenotato spazio di storage sufficiente, il provisioning non riesce e termina con un errore "Nessuna prenotazione disponibile per...". Lo storage allocato su una prenotazione dipende dal numero di macchine virtuali (indipendentemente dal loro stato) in quella specifica prenotazione. Vedere l'articolo della Knowledge Base di VMware *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* all'indirizzo <http://kb.vmware.com/kb/2151030> per ulteriori informazioni.

Logica di selezione delle prenotazioni

Quando un membro di un gruppo di business crea una richiesta di provisioning per una macchina virtuale, vRealize Automation seleziona una macchina da una delle prenotazioni disponibili per quel gruppo di business.

La prenotazione per cui viene eseguito il provisioning di una macchina deve soddisfare i seguenti criteri:

- La prenotazione deve essere dello stesso tipo di piattaforma del blueprint da cui la macchina è stata richiesta.

È possibile eseguire il provisioning di un blueprint virtuale generico su qualsiasi tipo di prenotazione virtuale.

- La prenotazione deve essere attivata.
- La risorsa di elaborazione deve essere accessibile e non in modalità manutenzione.
- La prenotazione deve avere capacità rimanente nella sua quota macchina o avere una quota illimitata.

La quota della macchina allocata include solo le macchine accese. Se ad esempio una prenotazione ha una quota pari a 50, e 40 macchine sono state fornite in provisioning ma solo 20 di esse sono accese, la quota della prenotazione è allocata per il 40 per cento, non per l'80 per cento.

- La prenotazione deve avere risorse di memoria e storage non allocate sufficienti a eseguire il provisioning della macchina.

Quando la quota, lo storage o la memoria di una macchina di una prenotazione virtuale è completamente allocata, da essa non è possibile eseguire il provisioning di altre macchine virtuali. Le risorse possono essere riservate oltre la capacità fisica di una risorsa di elaborazione virtualizzata (overcommit), ma quando la capacità fisica di una risorsa di elaborazione è allocata al 100%, non è possibile eseguire il provisioning di altre prenotazioni con quella risorsa di elaborazione finché le risorse non vengono recuperate.

- Se il blueprint ha impostazioni di rete specifiche, la prenotazione deve avere le stesse reti.

Se il blueprint o la prenotazione presentano un profilo di rete con assegnazione di indirizzi IP statici, deve essere disponibile un indirizzo IP da assegnare alla nuova macchina.

- Se il blueprint o la richiesta specificano una posizione, la risorsa di elaborazione deve essere associata a quella posizione.

Se il valore della proprietà personalizzata `Vrm.DataCenter.Policy` è **Exact** e non ci sono prenotazioni per una risorsa di elaborazione associata a tale posizione che soddisfino tutti gli altri criteri, il provisioning non riesce.

Se il valore di `Vrm.DataCenter.Policy` è **NotExact** e non ci sono prenotazioni per una risorsa di elaborazione associata a tale posizione che soddisfino tutti gli altri criteri, il provisioning può proseguire per un'altra prenotazione, indipendentemente dalla posizione. Questa è l'opzione predefinita.

- Se il blueprint o la richiesta specifica la proprietà personalizzata `VirtualMachine.Host.TpmEnabled`, è necessario installare hardware attendibile nella risorsa di elaborazione per la prenotazione.
- Se il blueprint specifica un criterio di prenotazione, la prenotazione deve appartenere a quel criterio di prenotazione.

I criteri di prenotazione permettono di assicurarsi che la prenotazione selezionata rispetti tutti i requisiti aggiuntivi per il provisioning di macchine da uno specifico blueprint. Ad esempio è possibile utilizzare criteri di prenotazione per limitare il provisioning a risorse di elaborazione con un modello specifico per la clonazione.

Se non sono disponibili prenotazioni che soddisfano tutti i criteri di selezione, il provisioning non riesce.

Se i criteri sono soddisfatti da più prenotazioni, la prenotazione da cui eseguire il provisioning di una macchina richiesta viene determinata in base alla seguente logica.

- Una prenotazione con un valore di priorità minore viene selezionata prima di una prenotazione con un valore di priorità maggiore.
- Se ci sono più prenotazioni con la stessa priorità, viene selezionata la prenotazione con la percentuale più bassa della propria quota macchina allocata.
- Se più prenotazioni hanno la stessa priorità e lo stesso uso della quota, le macchine vengono distribuite tra le prenotazioni in modalità round robin.

Nota Sebbene la selezione round robin di profili di rete non sia supportata, la selezione round robin di reti (se esistente) è supportata ed è possibile associarla a diversi profili di rete.

Se su una prenotazione sono disponibili più percorsi di storage con capacità sufficienti al provisioning dei volumi delle macchine, i percorsi di storage vengono selezionati in base alla seguente logica:

- Se il blueprint o la richiesta specificano un criterio di prenotazione storage, il percorso di storage deve appartenere a quel criterio di prenotazione storage.

Se il valore della proprietà personalizzata

`VirtualMachine.DiskN.StorageReservationPolicyMode` è **NotExact** e non esiste un percorso di storage con capacità sufficiente all'interno del criterio di prenotazione dello storage, il provisioning può procedere con un percorso di storage esterno al criterio di prenotazione dello storage specificato. Il valore predefinito di `VirtualMachine.DiskN.StorageReservationPolicyMode` è **Exact**.

- Un percorso di storage con un valore di priorità minore viene selezionato prima di un percorso di storage con un valore di priorità maggiore.
- Se più percorsi di storage hanno la stessa priorità, le macchine vengono distribuite tra percorsi di storage in una modalità round robin.

Creazione di una prenotazione di vSphere per la rete e la sicurezza di NSX in vRealize Automation
È possibile creare una prenotazione vSphere per operare con l'endpoint NSX-T o NSX for vSphere associato in vRealize Automation.

Considerazioni generali su NSX

Se è stato configurato NSX, quando si crea o si modifica un blueprint è possibile specificare le impostazioni di NSX relative a zona di trasporto, criterio di prenotazione della rete e isolamento app. Queste impostazioni sono disponibili nella scheda **Impostazioni NSX** nelle pagine **Blueprint** e **Proprietà blueprint**.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere e NSX-T. Per informazioni sulla configurazione di NSX, vedere *Administration Guide* nella [documentazione del prodotto NSX for vSphere](#) o nella [documentazione del prodotto NSX-T](#), a seconda dell'applicazione utilizzata.

L'esito positivo del provisioning richiede che la zona di trasporto della prenotazione corrisponda alla zona di trasporto di un blueprint di macchina quando quel blueprint definisce le reti delle macchine. Allo stesso modo, il provisioning del gateway instradato di una macchina richiede che la zona di trasporto definita nella prenotazione corrisponda alla zona di trasporto definita per il blueprint.

Per considerazioni sulla topologia specifica di NSX-T nelle proprie distribuzioni, vedere [Informazioni sulle topologie di distribuzione di NSX-T per i servizi di rete, la sicurezza e le configurazioni del bilanciamento del carico](#).

Considerazioni su NSX for vSphere

Quando vRealize Automation esegue il provisioning di macchine con networking NAT o instradato, esegue il provisioning di un gateway instradato come router di rete. L'Edge o il gateway instradato è una macchina di gestione che consuma risorse di elaborazione. Essa inoltre gestisce le comunicazioni di rete per i componenti macchina di cui è stato eseguito il provisioning. La prenotazione utilizzata per eseguire il provisioning dell'Edge o del gateway instradato determina la rete esterna utilizzata per i profili di rete NAT e instradata. Essa determina anche l'Edge o il gateway instradato della prenotazione utilizzato per configurare le reti instradate. Il gateway instradato della prenotazione collega tra loro le reti instradate utilizzando le voci contenute nella tabella di routing.

Quando si seleziona un gateway edge o instradato e un profilo di rete su una prenotazione per reti instradate, selezionare il percorso di rete da utilizzare per collegare insieme le reti instradate. Assegnare il percorso di rete al profilo di rete esterno utilizzato per configurare il profilo di rete instradata. L'elenco dei profili di rete disponibili per essere assegnati a un percorso di rete viene filtrato per riflettere la subnet del percorso di rete, in base alla subnet mask e all'indirizzo IP primario selezionati per l'interfaccia di rete.

È possibile specificare un criterio di prenotazione dell'Edge o del gateway instradato per identificare quali prenotazioni utilizzare quando viene eseguito il provisioning delle macchine utilizzando l'Edge o il gateway instradato. Per impostazione predefinita, vRealize Automation utilizza le stesse prenotazioni per il gateway instradato e i componenti macchina.

Se si desidera utilizzare un gateway Edge o instradato nelle prenotazioni di vRealize Automation, configurare il gateway instradato esternamente nell'ambiente di NSX, quindi eseguire la raccolta di dati dell'inventario. Per NSX, è necessario avere un'istanza Edge NSX funzionante prima di poter configurare il gateway predefinito per route statiche o i dettagli di routing dinamico per un Services Gateway o Distributed Router Edge. Vedere la *guida di amministrazione di NSX*.

È possibile selezionare uno o più gruppi di sicurezza nella prenotazione per applicare un criterio di protezione di base per tutte le macchine dei componenti fornite in provisioning con quella prenotazione in vRealize Automation. Ogni macchina con provisioning eseguito viene aggiunta a questi gruppi di sicurezza specificati.

Considerazioni su NSX-T

Quando si crea una prenotazione per un endpoint vSphere associato a un endpoint NSX-T, è necessario configurare le seguenti informazioni per la prenotazione:

- Definire una zona di trasporto per il blueprint.
- Selezionare un router logico di livello 0 per la distribuzione con provisioning a cui connettersi.
- Mappare un profilo di rete esterno per il router logico di livello 0.

I gruppi NS NSX-T non sono supportati nelle prenotazioni.

Per ulteriori informazioni sulle considerazioni relative a distribuzione e topologia specifiche di NSX-T, vedere [Informazioni sulle topologie di distribuzione di NSX-T per i servizi di rete, la sicurezza e le configurazioni del bilanciamento del carico](#).

Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer

È necessario allocare risorse per le macchine creando una prenotazione prima che i membri di un gruppo di business possano richiedere il provisioning della macchina.

Ogni gruppo di business deve avere almeno una prenotazione per i suoi membri per eseguire il provisioning di macchine di quel tipo. Ad esempio, un gruppo di business con una prenotazione vSphere ma non una prenotazione KVM (RHEV), non può richiedere una macchina virtuale KVM (RHEV). In questo esempio, al gruppo di business è necessario allocare una prenotazione specifica per risorse di KVM (RHEV).

Procedura

1 Definizione di informazioni sulle prenotazioni virtuali

Ogni prenotazione è configurata per concedere agli utenti di un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

2 Definizione delle impostazioni di risorse e rete per una prenotazione virtuale

Specificare le impostazioni delle risorse e della rete disponibili per il provisioning di macchine da questa prenotazione di vRealize Automation.

3 Definizione di proprietà personalizzate e avvisi per prenotazioni virtuali

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Definizione di informazioni sulle prenotazioni virtuali

Ogni prenotazione è configurata per concedere agli utenti di un dato gruppo di business l'accesso alle macchine richieste su una risorsa di elaborazione specificata.

È possibile controllare la visualizzazione delle prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per categoria** della pagina Prenotazioni. Si noti che le prenotazioni dell'agente di test non vengono riportate nell'elenco delle prenotazioni quando viene applicato il filtro per categoria.

Nota dopo aver creato una prenotazione non è possibile cambiare le associazioni di gruppi di business o risorse di elaborazione.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Verificare che un amministratore tenant abbia creato almeno un gruppo di business.
- Verificare che esista una risorsa di elaborazione.
- Configurare le impostazioni di rete.
- (Facoltativo) Configurare le informazioni del profilo di rete.

Procedura

1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.

- 2 Fare clic sull'icona **Nuovo** (+) e selezionare il tipo di prenotazione da creare.

I tipi di prenotazioni virtuali disponibili sono Hyper-V, KVM, SCVMM, vSphere e XenServer.
Ad esempio selezionare **vSphere**.

- 3 Immettere un nome nella casella di testo **Nome**.

- 4 Selezionare un tenant dal menu a discesa **Tenant**.

- 5 Selezionare un gruppo di business dal menu a discesa **Gruppo di business**.

Solo gli utenti appartenenti a questo gruppo di business possono eseguire il provisioning di macchine utilizzando questa prenotazione.

- 6 (Facoltativo) Selezionare un criterio di prenotazione dal menu a discesa **Criterio di prenotazione**.

Questa opzione richiede l'esistenza di uno o più criteri di prenotazione. È possibile modificare la prenotazione in un secondo momento per specificare un criterio di prenotazione.

Il criterio di prenotazione consente di limitare il provisioning a prenotazioni specifiche.

- 7 Immettere un numero nella casella di testo **Priorità** per impostare la priorità per la prenotazione.

La priorità viene utilizzata quando un gruppo di business ha più di una prenotazione. Per il provisioning viene utilizzata una prenotazione con priorità 1 rispetto a una con priorità 2.

- 8 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

Risultati

Non lasciare questa pagina. La prenotazione non è completa.

Definizione delle impostazioni di risorse e rete per una prenotazione virtuale

Specificare le impostazioni delle risorse e della rete disponibili per il provisioning di macchine da questa prenotazione di vRealize Automation.

È possibile selezionare un datastore FlexClone nella prenotazione se si hanno un ambiente vSphere e dispositivi di storage che utilizzano tecnologia Net App FlexClone. SDRS non è supportata per i dispositivi di storage FlexClone.

Per eseguire il provisioning correttamente, la prenotazione deve avere spazio di storage disponibile sufficiente. La disponibilità dello spazio di storage della prenotazione dipende dai seguenti fattori:

- Quantità di storage disponibile sul datastore/cluster.
- Quantità di storage riservata per questo cluster di datastore/cluster.
- Quantità di storage già allocato in vRealize Automation

Ad esempio, anche se il vCenter Server dispone di spazio di storage disponibile per il datastore/cluster, se non è stato prenotato spazio di storage sufficiente, il provisioning non riesce e termina con un errore "Nessuna prenotazione disponibile per...". Lo storage allocato su una prenotazione dipende dal numero di macchine virtuali (indipendentemente dal loro stato) in quella specifica prenotazione. Vedere l'articolo della Knowledge Base di VMware *Machine XXX: No reservation is available to allocate within the group XXX. Total XX GB of storage was requested (2151030)* all'indirizzo <http://kb.vmware.com/kb/2151030> per ulteriori informazioni.

Se si crea o modifica una prenotazione vSphere (vCenter) per l'uso con NSX for vSphere o NSX-T, è possibile specificare le informazioni del router logico di livello 1 e zona di trasferimento utilizzando opzioni avanzate per la rete selezionata.

Prerequisiti

[Definizione di informazioni sulle prenotazioni virtuali.](#)

Procedura

- 1 Fare clic sulla scheda **Risorse**.
- 2 Selezionare una risorsa di elaborazione su cui eseguire il provisioning delle macchine dal menu a discesa **Risorse di elaborazione**.

Per la clonazione con questa prenotazione sono disponibili solo i modelli localizzati sul cluster selezionato.

Durante il provisioning, le macchine vengono posizionate in un host collegato allo storage locale. Se la prenotazione utilizza lo storage locale, tutte le macchine sottoposte a provisioning dalla prenotazione vengono create nell'host che contiene lo storage locale specificato. Tuttavia, se si utilizza la proprietà personalizzata di `VirtualMachine.Admin.ForceHost`, che forza il provisioning di una macchina in un altro host, il provisioning non riesce. Il provisioning non riesce neanche nel caso in cui il modello da cui viene clonata la macchina si trova nello storage locale, ma collegato a una macchina in un altro cluster. In tal caso, il provisioning non riesce poiché non è in grado di accedere al modello.

- 3 (Facoltativo) Immettere un numero nella casella di testo **Quota macchina** per impostare il numero massimo di macchine di cui è possibile eseguire il provisioning con questa prenotazione.

Nella quota vengono conteggiate solo le macchine accese. Lasciare vuoto il campo per rendere illimitata la prenotazione.

- 4 Specificare la quantità di memoria, espressa in GB, da allocare per questa prenotazione dalla tabella Memoria.

Il valore di memoria totale per la prenotazione dipende dalla risorsa di elaborazione selezionata.

- 5 Specificare la quantità di memoria, espressa in GB, da allocare per questa prenotazione dalla tabella Memoria.

Il valore di memoria totale per la prenotazione dipende dalla risorsa di elaborazione selezionata.

- 6 Selezionare uno o più percorsi di storage elencati.

Le opzioni del percorso di storage disponibili dipendono dalla risorsa di elaborazione selezionata.

Per integrazioni che utilizzano lo storage Storage Distributed Resource Scheduler (SDRS), è possibile selezionare un cluster di storage per consentire a SDRS di gestire automaticamente la disposizione dello storage e il bilanciamento del carico per le macchine fornite in provisioning da questa prenotazione. La modalità di automazione SDRS deve essere impostata su Automatico. Altrimenti, selezionare un datastore all'interno del cluster per un funzionamento da datastore autonomo. SDRS non è supportata per i dispositivi di storage FlexClone.

È possibile selezionare un cluster di storage o singoli dischi all'interno del cluster, ma non entrambi. Se si seleziona un cluster di storage, SDRS controllerà la disposizione dello storage e il bilanciamento del carico per le macchine di cui è stato eseguito il provisioning a partire dalla prenotazione in fase di definizione.

- 7 Se disponibile per la risorsa di elaborazione, selezionare un pool di risorse dal menu a discesa **Pool di risorse**.
- 8 Fare clic sulla scheda **Rete**.
- 9 Configurare un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.

- a (Facoltativo) Se l'opzione è disponibile, selezionare un endpoint di storage dal menu a discesa **Endpoint**.

L'opzione FlexClone è mostrata nella colonna dell'endpoint se esiste un endpoint NetApp ONTAP e se l'host è virtuale. Se c'è un endpoint NetApp ONTAP, la pagina della prenotazione mostra l'endpoint assegnato al percorso di storage. Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile in tutte le prenotazioni applicabili.

Quando si aggiunge, si aggiorna o si elimina un endpoint per un percorso di storage, il cambiamento è visibile nella pagina della prenotazione.

- b Selezionare una o più **Schede di rete** per le macchine da sottoporre a provisioning per questa prenotazione.

- c (Facoltativo) Selezionare un **Profilo di rete** disponibile per ciascuna scheda di rete selezionata.
- d (Facoltativo) Se sono disponibili le impostazioni avanzate, selezionare una **Zona di trasporto** e uno o più **Router logici di livello 0** da utilizzare quando si distribuisce un blueprint che contiene i bilanciamenti del carico.

Una zona di trasporto definisce quali cluster possono rientrare nelle schede di rete. Se si specifica una zona di trasporto in una prenotazione e in un blueprint, i valori della zona di trasporto devono corrispondere.

È possibile selezionare più di una scheda di rete in una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

Risultati

A questo punto è possibile salvare la prenotazione facendo clic su **Salva**. Oppure è possibile aggiungere proprietà personalizzate per controllare ulteriormente le specifiche della prenotazione. Inoltre è possibile configurare avvisi via email da inviare quando le risorse allocate a questa prenotazione si approssimano all'esaurimento.

Definizione di proprietà personalizzate e avvisi per prenotazioni virtuali

È possibile associare proprietà personalizzate a una prenotazione di vRealize Automation. Inoltre è possibile configurare avvisi per inviare notifiche via email quando le risorse della prenotazione si stanno esaurendo.

Le proprietà personalizzate e gli avvisi via email sono configurazioni opzionali per la prenotazione. Se non si desidera associare proprietà personalizzate o impostare avvisi, fare clic su **Salva** per completare la creazione della prenotazione.

È possibile aggiungere tutte le proprietà personalizzate di cui si ha bisogno.

Importante le notifiche vengono inviate solo se gli avvisi via email sono configurati e le notifiche attivate.

Se configurati, gli avvisi vengono generati quotidianamente e non al raggiungimento delle soglie specificate.

Prerequisiti

[Definizione delle impostazioni di risorse e rete per una prenotazione virtuale.](#)

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Fare clic su **Nuovo**.
- 3 Immettere un nome valido per la proprietà personalizzata.
- 4 Se applicabile, immettere un valore per la proprietà.
- 5 (Facoltativo) Selezionare la casella di controllo **Codificato** per crittografare il valore della proprietà.

- 6 (Facoltativo) Selezionare la casella di controllo **Richiedi conferma** per richiedere l'immissione di un valore da parte dell'utente.

Questa opzione non può essere sovrascritta durante il provisioning.

- 7 (Facoltativo) Aggiungere eventuali proprietà personalizzate aggiuntive.

- 8 Fare clic sulla scheda **Avvisi**.

- 9 Selezionare la casella di controllo **Avvisi capacità** per configurare gli avvisi da inviare.

- 10 Utilizzare il cursore per impostare le soglie per l'allocazione delle risorse disponibili.

- 11 Nella casella di testo **Destinatari**, immettere i nomi dei gruppi o degli utenti di AD (non gli indirizzi email) a cui inviare le notifiche di avviso.

Immettere un nome in ogni riga. Premere Invio per separare voci multiple.

- 12 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.

Gli avvisi tramite email vengono inviati agli utenti inclusi nell'elenco **Invia email manager a** del gruppo di business.

- 13 Specificare una frequenza per i promemoria (giorni).

- 14 Fare clic su **Salva**.

Risultati

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Operazioni successive

È possibile configurare criteri di prenotazione opzionali o iniziare la preparazione per il provisioning.

Gli utenti autorizzati a creare blueprint a questo punto possono farlo.

Modifica di una prenotazione per assegnare un profilo di rete

È possibile assegnare un profilo di rete a una prenotazione, ad esempio per abilitare l'assegnazione di IP statici per macchine di cui viene effettuato il provisioning in quella prenotazione.

È anche possibile assegnare un profilo di rete a un blueprint utilizzando la proprietà personalizzata `VirtualMachine.NetworkN.ProfileName` nella scheda **Proprietà** della pagina **Nuovo blueprint** o **Proprietà blueprint**.

Se viene specificato un profilo di rete in una prenotazione e un blueprint, i valori del blueprint hanno la precedenza.

Nota queste informazioni non riguardano i Amazon Web Services.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.

- Creare un profilo di rete. Vedere [Creazione di un profilo di rete in vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Selezionare la prenotazione desiderata e fare clic su **Modifica**.
- 3 Fare clic sulla scheda **Rete**.
- 4 Assegnare un profilo di rete a un percorso di rete.
 - a Selezionare un percorso di rete su cui abilitare gli indirizzi IP statici.
Le opzioni del percorso di rete dipendono dalle impostazioni della scheda **Risorse**.
 - b Mappare un profilo di rete disponibile al percorso selezionando il profilo dal menu a discesa **Profilo di rete**.
 - c (Facoltativo) Ripetere questo passaggio per assegnare profili di rete ad altri percorsi di rete su questa prenotazione.
- 5 Fare clic su **OK**.

Criteri di prenotazione

È possibile utilizzare un criterio di prenotazione per controllare come vengono elaborate le richieste di prenotazione. Quando viene eseguito il provisioning di macchine dal blueprint, il provisioning viene limitato alle risorse specificate nel criterio di prenotazione.

I criteri di prenotazione forniscono un ulteriore metodo per controllare il modo in cui vengono elaborate le richieste di prenotazione. È possibile applicare un criterio di prenotazione a un blueprint per limitare le macchine con provisioning da quel blueprint a un sottoinsieme di prenotazioni disponibili.

È possibile utilizzare un criterio di prenotazione per raggruppare le risorse per diversi livelli di servizi oppure per rendere più facilmente disponibile un tipo di risorsa specifica per uno scopo particolare. Quando un utente richiede una macchina, questa può essere sottoposta a provisioning su qualsiasi prenotazione di tipo appropriato che abbia capacità sufficiente per la macchina. Gli scenari seguenti forniscono alcuni esempi di usi possibili dei criteri di prenotazione:

- Garantire che le macchine fornite in provisioning siano collocate su prenotazioni con dispositivi specifici che supportano NetApp FlexClone.
- Limitare il provisioning delle macchine cloud a una regione specifica contenente l'immagine delle macchine obbligatoria per un blueprint specifico.
- Costituire un ulteriore mezzo per l'uso di un modello di allocazione con Pagamento a consumo per tipi di macchine che supportano tale funzionalità.

A un criterio di prenotazione è possibile aggiungere più prenotazioni, ma una prenotazione può appartenere a un solo criterio. È possibile assegnare un singolo criterio di prenotazione a più blueprint. Un blueprint può avere solo un criterio di prenotazione.

Nota Le prenotazioni definite per gli endpoint vCloud Air e gli endpoint vCloud Director non supportano l'uso di profili di rete per il provisioning delle macchine.

Nota se nella piattaforma è attivato l'SDRS, è possibile consentire a quest'ultimo di bilanciare il carico dello storage per i dischi delle singole macchine virtuali o di tutto lo spazio di storage della macchina virtuale. Se si lavora con i datastore cluster SDRS, possono verificarsi dei conflitti quando vengono utilizzati i criteri delle prenotazioni e i criteri delle prenotazioni di storage. Ad esempio, se un datastore autonomo o uno all'interno di un cluster SDRS viene selezionato su una delle prenotazioni in un criterio o in un criterio di storage, lo storage della macchina virtuale potrebbe essere bloccato anziché avviato dall'SDRS. Quando si richiede la riesecuzione del provisioning di una macchina con storage in un cluster SDRS, se il livello di automazione SDRS è disattivato la macchina viene eliminata. Per informazioni correlate su provisioning e SDRS, vedere la proprietà personalizzata

`VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec.`

Configurazione di un criterio di prenotazione

È possibile creare criteri di prenotazione per raggruppare le risorse per diversi livelli di servizi oppure per rendere più facilmente disponibile un tipo di risorsa specifica per uno scopo particolare. Dopo aver creato il criterio di prenotazione, è necessario popolarlo con le prenotazioni prima che gli amministratori tenant e i manager dei gruppi di business possano di fatto utilizzare il criterio in un blueprint.

Un criterio di prenotazione può includere prenotazioni di tipo diverso ma vengono considerate solo le prenotazioni che corrispondono al tipo di blueprint quando la prenotazione viene selezionata per una richiesta particolare.

Procedura

1 Creazione di un criterio di prenotazione

È possibile utilizzare i criteri di prenotazione per raggruppare prenotazioni simili.

2 Assegnazione di un criterio di prenotazione a una prenotazione

È possibile assegnare un criterio di prenotazione a una prenotazione durante la sua creazione. Anche una prenotazione esistente può essere modificata per aggiungere o cambiare l'assegnazione di un criterio di prenotazione.

Creazione di un criterio di prenotazione

È possibile utilizzare i criteri di prenotazione per raggruppare prenotazioni simili.

Creare prima il criterio di prenotazione, quindi aggiungere il criterio alle prenotazioni per consentire agli autori dei blueprint di utilizzare il criterio di prenotazione all'interno di un blueprint.

Il criterio viene creato come contenitore vuoto.

È possibile controllare la visualizzazione dei criteri di prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per tipo** della pagina Criteri di prenotazione.

Prerequisiti

Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Criteri di prenotazione**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare **Criterio di prenotazione** dal menu a discesa **Tipo**.
- 5 Immettere una descrizione nella casella di testo **Descrizione**.
- 6 Fare clic su **OK**.

Assegnazione di un criterio di prenotazione a una prenotazione

È possibile assegnare un criterio di prenotazione a una prenotazione durante la sua creazione. Anche una prenotazione esistente può essere modificata per aggiungere o cambiare l'assegnazione di un criterio di prenotazione.

Prerequisiti

[Creazione di un criterio di prenotazione.](#)

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Selezionare la prenotazione desiderata e fare clic su **Modifica**.
- 3 Selezionare un criterio di prenotazione dal menu a discesa **Criterio di prenotazione**.
- 4 Fare clic su **Salva**.

Criteri di prenotazione storage

È possibile creare criteri di prenotazione storage per consentire agli architetti dei blueprint di assegnare i volumi di una macchina virtuale a data store differenti per i tipi di piattaforme vSphere, KVM (RHEV) e SCVMM o a profili di storage differenti per altre risorse, come ad esempio risorse vCloud Air o vCloud Director.

L'assegnazione dei volumi di una macchina virtuale a data store differenti o a profili di storage differenti consente gli architetti dei blueprint di controllare e utilizzare in modo più efficace lo spazio di storage. Essi possono ad esempio distribuire il volume del sistema operativo su un data store o un profilo di storage più lento e meno costoso e il volume del database su un data store o profilo di storage più veloce.

Alcuni endpoint macchina supportano solo un singolo profilo di storage, mentre altri supportano storage su disco multilivello. Lo storage su disco multilivello è disponibile per gli endpoint vCloud Director 5.6 e superiori e per gli endpoint vCloud Air. Lo storage su disco multilivello non è supportato per gli endpoint vCloud Director 5.5.

Quando si crea un blueprint, è possibile assegnare un singolo data store o un criterio di prenotazione di storage che rappresenta più data store in un volume. Quando si assegna un singolo data store o profilo di storage a un volume, vRealize Automation utilizza quel data store o profilo di storage al momento del provisioning, se possibile. Quando si assegna un criterio di prenotazione storage a un volume, vRealize Automation utilizza uno dei suoi data store, o profili di storage se si sta lavorando con altre risorse, come ad esempio vCloud Air o vCloud Director, al momento del provisioning.

Un criterio di prenotazione storage è essenzialmente un tag applicato a uno o più data store o profili di storage da un amministratore di struttura per raggruppare i data store o i profili di storage che hanno caratteristiche simili, ad esempio la velocità o il prezzo. È possibile assegnare un data store o un profilo di storage a un solo criterio di prenotazione storage alla volta, ma un criterio di prenotazione storage può avere molti data store o profili di storage differenti.

È possibile creare un criterio di prenotazione storage e assegnarlo a uno o più data store o profili di storage. L'autore di un blueprint può quindi assegnare il criterio di prenotazione storage a un volume in un blueprint virtuale. Quando un utente richiede una macchina che utilizza il blueprint, vRealize Automation utilizza il criterio di prenotazione storage specificato nel blueprint per selezionare un data store o profilo di storage per il volume della macchina.

Nota se nella piattaforma è attivato l'SDRS, è possibile consentire a quest'ultimo di bilanciare il carico dello storage per i dischi delle singole macchine virtuali o di tutto lo spazio di storage della macchina virtuale. Se si lavora con i datastore cluster SDRS, possono verificarsi dei conflitti quando vengono utilizzati i criteri delle prenotazioni e i criteri delle prenotazioni di storage. Ad esempio, se un datastore autonomo o uno all'interno di un cluster SDRS viene selezionato su una delle prenotazioni in un criterio o in un criterio di storage, lo storage della macchina virtuale potrebbe essere bloccato anziché avviato dall'SDRS. Quando si richiede la riesecuzione del provisioning di una macchina con storage in un cluster SDRS, se il livello di automazione SDRS è disattivato la macchina viene eliminata. Per informazioni correlate su provisioning e SDRS, vedere la proprietà personalizzata

`VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec.`

Lo storage e la memoria assegnati a una macchina sottoposta a provisioning da una prenotazione vengono rilasciati quando la macchina a cui sono assegnati viene eliminata in vRealize Automation dall'azione di eliminazione. La memoria e lo storage non vengono rilasciati se la macchina viene eliminata in vCenter Server.

Ad esempio, non è possibile eliminare una prenotazione associata alle macchine in una distribuzione esistente. Se si spostano o si eliminano manualmente macchine distribuite in vCenter Server, vRealize Automation continua a riconoscere le macchine distribuite come funzionanti e impedisce l'eliminazione delle prenotazioni associate.

Configurazione di un criterio di prenotazione storage

È possibile creare criteri di prenotazione storage per raggruppare i datastore con caratteristiche simili, come ad esempio la velocità o il prezzo. Dopo aver creato il criterio di prenotazione storage, è necessario popolarlo con i datastore prima di utilizzare il criterio in un blueprint.

Procedura

1 Creazione di un criterio di prenotazione storage

È possibile utilizzare un criterio di prenotazione storage per raggruppare i datastore con caratteristiche simili, come ad esempio la velocità o il prezzo.

2 Assegnazione di un criterio di prenotazione storage a un datastore

È possibile associare un criterio di prenotazione storage a una risorsa di elaborazione. Dopo aver creato il criterio di prenotazione storage, popolarlo con i datastore. Un datastore può appartenere a un solo criterio di prenotazione storage. Aggiungere più datastore per creare un gruppo di datastore da utilizzare con un blueprint.

Creazione di un criterio di prenotazione storage

È possibile utilizzare un criterio di prenotazione storage per raggruppare i datastore con caratteristiche simili, come ad esempio la velocità o il prezzo.

Il criterio viene creato come contenitore vuoto.

È possibile controllare la visualizzazione dei criteri di prenotazioni durante l'aggiunta, la modifica o l'eliminazione utilizzando l'opzione **Filtra per tipo** della pagina Criteri di prenotazione.

Prerequisiti

Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Criteri di prenotazione**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare **Criterio di prenotazione storage** dal menu a discesa **Tipo**.
- 5 Immettere una descrizione nella casella di testo **Descrizione**.
- 6 Fare clic su **OK**.


Assegnazione di un criterio di prenotazione storage a un datastore

È possibile associare un criterio di prenotazione storage a una risorsa di elaborazione. Dopo aver creato il criterio di prenotazione storage, popolarlo con i datastore. Un datastore può appartenere a un solo criterio di prenotazione storage. Aggiungere più datastore per creare un gruppo di datastore da utilizzare con un blueprint.

Prerequisiti

[Creazione di un criterio di prenotazione storage](#).

Procedura

- 1 Selezionare **Infrastruttura > Risorse di elaborazione > Risorse di elaborazione**.
- 2 Selezionare una risorsa di elaborazione e fare clic su **Modifica**.
- 3 Fare clic sulla scheda **Configurazione**.
- 4 Individuare il datastore da aggiungere al criterio di prenotazione storage nella tabella Storage.
- 5 Fare clic sull'icona **Modifica** () accanto all'oggetto **Percorso di storage** desiderato.
- 6 Selezionare un criterio di prenotazione storage dal menu a discesa della colonna **Criterio di prenotazione storage**.

Dopo aver eseguito il provisioning di una macchina, non è possibile cambiare il suo criterio di prenotazione storage se ciò dovesse modificare il profilo di storage su un disco.

- 7 Fare clic su **OK**.
- 8 (Facoltativo) Assegnare datastore aggiuntivi al criterio di prenotazione storage.
- 9 Fare clic su **OK**.

Posizionamento dei carichi di lavoro

Quando si distribuisce un blueprint, il posizionamento dei carichi di lavoro utilizza i dati raccolti per suggerire la posizione in cui distribuire il blueprint in base alle risorse disponibili. vRealize Automation e vRealize Operations Manager lavorano insieme per fornire suggerimenti di posizionamento sui carichi di lavoro nella distribuzione di nuovi blueprint.

Oltre a gestire criteri organizzativi, quali gruppi di business, prenotazioni e quote, vRealize Automation si integra con le analisi delle capacità di vRealize Operations Manager per posizionare le macchine. Il posizionamento dei carichi di lavoro è disponibile solo per gli endpoint vSphere.

Termini utilizzati nelle operazioni di posizionamento dei carichi di lavoro

Per le operazioni di posizionamento dei carichi di lavoro, vengono utilizzati diversi termini.

- I cluster in vSphere sono mappati a risorse di elaborazione in vRealize Automation.
- Le prenotazioni includono la risorsa di elaborazione e lo storage; lo storage può essere composto da singoli datastore o cluster di datastore. Una prenotazione può includere più datastore, cluster di datastore o entrambi.
- Più prenotazioni possono fare riferimento allo stesso cluster.
- Le macchine virtuali possono essere spostate in più cluster.
- Quando si attiva il posizionamento dei carichi di lavoro, il workflow di provisioning utilizza il criterio di posizionamento per suggerire la posizione in cui distribuire il blueprint.

Provisioning dei blueprint con posizionamento dei carichi di lavoro

Quando si utilizza il posizionamento dei carichi di lavoro per eseguire il provisioning dei blueprint, il workflow di provisioning utilizza le prenotazioni in vRealize Automation, e l'ottimizzazione del posizionamento da vRealize Operations Manager.

- 1 vRealize Automation fornisce le regole di governance per consentire le destinazioni di posizionamento.
- 2 vRealize Operations Manager fornisce i consigli sull'ottimizzazione del posizionamento in base ai dati di analisi.
- 3 vRealize Automation continua il processo di provisioning in base ai consigli di posizionamento suggeriti da vRealize Operations Manager.

Se vRealize Operations Manager non è in grado di fornire un suggerimento oppure se il suggerimento non può essere applicato, viene ripristinata la logica di posizionamento predefinita di vRealize Automation.

Quando uno sviluppatore seleziona un elemento del catalogo e compila il modulo per richiedere tale elemento, vRealize Automation tiene conto delle seguenti considerazioni per effettuare il provisioning delle macchine virtuali.

Tabella 2-16. Considerazioni sul provisioning delle macchine virtuali

Considerazione	Effetto
Criteri	Il criterio di prenotazione di vRealize Automation potrebbe indicare più prenotazioni.
Prenotazioni	<p>vRealize Automation valuta la richiesta e determina quali prenotazioni possono soddisfarne i vincoli.</p> <ul style="list-style-type: none"> ■ Se il posizionamento è attivato e si basa sulle analisi di vRealize Operations Manager, vRealize Automation trasmette l'elenco di prenotazioni a vRealize Operations Manager per determinare quale sia la prenotazione migliore per il posizionamento secondo le metriche operative. ■ Se il posizionamento non si basa su vRealize Operations Manager, vRealize Automation decide il posizionamento secondo le priorità e la disponibilità. <p>Le prenotazioni vengono aggiornate per tenere traccia delle risorse consumate.</p> <p>Se vRealize Operations Manager consiglia un cluster o un datastore che vRealize Automation considera pieno o non più applicabile, vRealize Automation registra l'eccezione. vRealize Automation consente al provisioning di continuare in base ai propri meccanismi di posizionamento predefiniti.</p>

Per identificare le risorse per una macchina virtuale, vRealize Automation fornisce un elenco di prenotazioni candidato. Ciascun candidato nell'elenco può includere un cluster e uno o più datastore o cluster di datastore. vRealize Operations Manager utilizza le prenotazioni candidato per creare l'elenco di candidati di destinazione e individuare la migliore destinazione.

Il criterio in vRealize Operations Manager imposta il livello di bilanciamento, utilizzo e spazio di buffer per il cluster. Per un'unica prenotazione, che è un cluster o un cluster di datastore, vRealize Automation verifica che il suggerimento rappresenti una destinazione di posizionamento fattibile.

- Se la destinazione è fattibile, vRealize Automation distribuisce il blueprint seguendo il suggerimento.
- Se la destinazione non è fattibile, vRealize Automation utilizza il comportamento di posizionamento predefinito per posizionare le macchine virtuali.

Le considerazioni sul posizionamento devono anche tenere in conto i problemi di integrità e utilizzo. Mentre l'amministratore del cloud e l'amministratore dell'infrastruttura virtuale gestiscono l'infrastruttura, gli sviluppatori si preoccupano dell'integrità delle applicazioni. Per supportare gli sviluppatori, la strategia di bilanciamento del carico deve anche considerare i problemi di integrità e utilizzo.

Tabella 2-17. Considerazioni sui problemi di integrità e utilizzo

Problema relativo al carico di lavoro	Soluzione di posizionamento
Problema di integrità nell'ambiente scoperto da uno sviluppatore.	vRealize Automation sta effettuando il provisioning dei blueprint in cluster che presentano problemi o sono eccessivamente utilizzati a causa di grandi carichi di lavoro. vRealize Automation deve essere integrato con le funzionalità di analisi della capacità di vRealize Operations Manager per garantire che il provisioning dei blueprint venga effettuato in cluster con capacità sufficiente.
Problema di utilizzo scoperto da uno sviluppatore.	I cluster dell'ambiente non vengono utilizzati a sufficienza. vRealize Automation deve essere integrato con le funzionalità di analisi della capacità offerte da vRealize Operations Manager per garantire che il provisioning dei blueprint venga effettuato in un cluster in cui l'utilizzo sia ottimizzato.

Utenti che eseguono il provisioning di blueprint

I seguenti utenti eseguono azioni per effettuare il provisioning dei blueprint.

Tabella 2-18. Utenti e ruoli per il provisioning di blueprint

Passaggio	Utente	Azione	Ruolo necessario
1	Amministratore del cloud o amministratore dell'infrastruttura virtuale	Garantisce che il posizionamento iniziale delle macchine virtuali soddisfi i criteri organizzativi e che le macchine virtuali vengano ottimizzate in base a dati analitici operativi.	Ruolo di amministratore IaaS
1	Amministratore struttura	Definisce le prenotazioni, i criteri di prenotazione e i criteri di posizionamento in vRealize Automation.	Ruolo Amministratore struttura e Architetto dell'infrastruttura
1	Amministratore IaaS	Definisce gli endpoint per vSphere e vRealize Operations Manager, necessari per il posizionamento del carico di lavoro.	Ruolo di amministratore IaaS

Tabella 2-18. Utenti e ruoli per il provisioning di blueprint (continua)

Passaggio	Utente	Azione	Ruolo necessario
2	Architetto dell'infrastruttura	In qualità di architetto dei blueprint che lavora direttamente con i tipi di componenti delle macchine virtuali, assegna i criteri di prenotazione alle macchine virtuali durante la creazione dei blueprint. Specifica il criterio di prenotazione come proprietà del componente della macchina nel blueprint.	Architetto dell'infrastruttura
3	Architetto dell'infrastruttura, Architetto dell'applicazione, Architetto del software e Architetto XaaS	<p>Crea e pubblica il blueprint per effettuare il provisioning delle macchine virtuali. Solo l'Architetto dell'infrastruttura lavora direttamente con i componenti delle macchine. Gli altri ruoli di architetto possono riutilizzare i blueprint dell'infrastruttura in nidificazioni, ma non possono modificare le impostazioni dei componenti delle macchine.</p> <p>Il blueprint può includere un unico componente oppure blueprint nidificati, componenti XaaS, più macchine virtuali in un'applicazione su tre livelli e così via.</p> <p>vRealize Automation posiziona le macchine virtuali in base alla configurazione delle prenotazioni e, facoltativamente, include il criterio di prenotazione a livello del componente della macchina per il blueprint. Ad esempio, il blueprint potrebbe includere due macchine a ciascuna delle quali è applicato un criterio diverso.</p> <p>vRealize Automation ottimizza inoltre le macchine virtuali in base ai dati analitici operativi forniti da vRealize Operations Manager.</p>	Architetto dell'infrastruttura
4	Amministratore del cloud o amministratore dell'infrastruttura virtuale	<p>Seleziona i criteri che regolano il posizionamento iniziale delle macchine virtuali il cui provisioning viene effettuato da vRealize Automation.</p> <p>L'amministratore può:</p> <ul style="list-style-type: none"> ■ Selezionare i criteri utilizzando un'interfaccia API. ■ Utilizzare il criterio di posizionamento predefinito, che utilizza i server in vRealize Automation uno alla volta per bilanciare i carichi di lavoro. Questo approccio non richiede l'input da vRealize Operations Manager. 	Ruolo Amministratore IaaS e Architetto dell'infrastruttura
5	Amministratore dell'infrastruttura virtuale	Crea gruppi di data center personalizzati e gruppi personalizzati in vRealize Operations Manager. Poi applica il criterio utilizzato per consolidare e bilanciare i carichi di lavoro nei data center personalizzati.	Ruolo Amministratore IaaS e Architetto dell'infrastruttura
6	Amministratore di struttura	<p>Seleziona il criterio di posizionamento in vRealize Automation.</p> <p>Utilizza il criterio di posizionamento del carico di lavoro per fare in modo che vRealize Automation stabilisca dove posizionare le macchine quando si distribuiscono nuovi blueprint. Il criterio di posizionamento richiede l'input di vRealize Operations Manager</p>	Ruolo amministratore della struttura

Tabella 2-18. Utenti e ruoli per il provisioning di blueprint (continua)

Passaggio	Utente	Azione	Ruolo necessario
7	Sviluppatore	Richiede un blueprint per effettuare il provisioning delle macchine virtuali. Il blueprint può essere composto da più macchine per eseguire un'applicazione su tre livelli.	
8	Sviluppatore	Quando lo sviluppatore distribuisce il blueprint, vRealize Operations Manager cerca un criterio di posizionamento compatibile con i cluster rilevanti per la richiesta.	

Per ulteriori informazioni sul criterio di posizionamento, vedere [Criterio di posizionamento](#).

Per configurare il posizionamento dei carichi di lavoro, vedere [Configurazione del posizionamento dei carichi di lavoro](#).

Necessità di Distributed Resource Scheduler (DRS) per il posizionamento delle macchine virtuali

vSphere DRS è il motore di posizionamento utilizzato da vRealize Automation e vRealize Operations Manager per eseguire il provisioning e posizionare le macchine virtuali.

Per fare in modo che vRealize Automation suggerisca il migliore posizionamento per le macchine virtuali, è necessario attivare DRS nel cluster e impostarlo nella modalità completamente automatizzata. vRealize Automation utilizza quindi le API DRS di vSphere per determinare il corretto posizionamento delle macchine virtuali.

vRealize Automation si integra con il servizio di posizionamento di vRealize Operations Manager. vRealize Operations Manager fornisce unicamente consigli di posizionamento per i cluster in cui DRS è attivato e completamente automatizzato.

Effetto dei criteri di prenotazione storage di vRealize Automation

La presenza di criteri di prenotazione storage di vRealize Automation riguarda il posizionamento del carico di lavoro con vRealize Operations Manager.

Quando si abilita il posizionamento del carico di lavoro con vRealize Operations Manager, vRealize Automation passa un elenco di prenotazioni disponibili a vRealize Operations Manager e vRealize Operations Manager le valuta per il posizionamento dello storage in base all'analisi operativa.

Nota Il posizionamento del carico di lavoro con vRealize Operations Manager supporta solo le macchine virtuali con uno o più dischi, in cui è presente un solo criterio di prenotazione storage. Più combinazioni di criteri non sono supportate per il posizionamento del disco perché il posizionamento di un singolo disco non è supportato.

Quando un blueprint contiene criteri di prenotazione storage, i consigli di posizionamento del carico di lavoro di vRealize Operations Manager cambiano nel modo seguente.

Configurazione	Posizionamento
Macchine virtuali con uno o più dischi, laddove nessuno specifica un criterio di prenotazione storage	Il posizionamento viene eseguito come di consueto. vRealize Operations Manager valuta l'elenco completo e non filtrato di prenotazioni disponibili.
Macchine virtuali con uno o più dischi, che specificano tutti lo stesso criterio di prenotazione storage	Le prenotazioni disponibili vengono filtrate a livello di storage in modo che vRealize Operations Manager valuti solo i datastore che corrispondono a tale criterio di prenotazione storage.
Macchine virtuali con più dischi, alcuni dei quali specificano lo stesso criterio di prenotazione storage mentre altri non specificano alcun criterio di prenotazione storage	<ul style="list-style-type: none"> ■ Quando il tipo di allocazione dello storage è COLLECTED, l'impostazione predefinita, tutti i dischi vengono trattati come se condividessero lo stesso criterio. vRealize Operations Manager valuta i datastore che corrispondono a tale criterio di prenotazione storage. ■ Quando il tipo di allocazione dello storage è DISTRIBUTED, le macchine virtuali non possono essere posizionate in base ai consigli di vRealize Operations Manager perché il posizionamento di un singolo disco non è supportato. Il posizionamento viene invece eseguito per impostazione predefinita in base agli algoritmi di posizionamento di vRealize Automation. <p>È possibile impostare il tipo di allocazione dello storage mediante una proprietà personalizzata.</p>
Macchine virtuali con più dischi, in cui i dischi specificano criteri di prenotazione storage diversi	Poiché hanno requisiti relativi ai criteri di prenotazione storage in conflitto, queste macchine virtuali non possono essere posizionate in base ai consigli di vRealize Operations Manager. Il posizionamento viene invece eseguito per impostazione predefinita in base agli algoritmi di posizionamento di vRealize Automation.
Macchine virtuali che richiedono un percorso di storage specifico	<p>Queste macchine virtuali non vengono posizionate tramite un consiglio di vRealize Operations Manager perché è già stato specificato un percorso di storage. Il posizionamento potrebbe o meno corrispondere a quello consigliato da vRealize Operations Manager.</p> <p>È possibile impostare il percorso di storage mediante una proprietà personalizzata.</p>

Errori di posizionamento: quando non è possibile eseguire il posizionamento basato su vRealize Operations Manager, un messaggio di errore descrive il motivo. I motivi potrebbero includere le condizioni non supportate descritte nell'elenco precedente o fattori ambientali quali comunicazione non riuscita tra vRealize Operations Manager e vRealize Automation.

Per esaminare gli errori, passare a **Richieste > Esecuzione**. In alto a destra, fare clic su **Visualizza errori di posizionamento**.

Limitazioni relative al posizionamento dei carichi di lavoro

Quando si utilizza il criterio di posizionamento dei carichi di lavoro per posizionare le macchine durante la distribuzione di nuovi blueprint, prestare attenzione ai limiti.

- In vRealize Operations Manager, la soluzione vRealize Automation identifica i cluster e le macchine virtuali gestiti da vRealize Automation.
- Quando vRealize Automation gestisce gli oggetti figlio del contenitore di un data center o di un data center personalizzato in vRealize Operations Manager, non è possibile bilanciare di nuovo o spostare gli oggetti. Non è possibile attivare o disattivare l'esclusione di azioni su oggetti gestiti da vRealize Automation.

- Per gli oggetti gestiti da vRealize Automation, il comportamento relativo al posizionamento dei carichi di lavoro può essere riassunto come segue:
 - Quando un data center o un data center personalizzato include un cluster gestito da vRealize Automation, il posizionamento dei carichi di lavoro non consente di bilanciare di nuovo il cluster.
 - Quando un cluster include macchine virtuali gestite da vRealize Automation, il posizionamento dei carichi di lavoro non consente di spostare tali macchine virtuali.
- vRealize Operations Manager non supporta il posizionamento di carichi di lavoro su pool di risorse in vCenter Server.
- vRealize Operations Manager 7.5 e versione successiva supportano gli archivi dati vSAN per il posizionamento dei carichi di lavoro. Per informazioni correlate, vedere le [note di rilascio](#) di vRealize Operations Manager 7.5.

Autorizzazioni per configurare il posizionamento del carico di lavoro

È necessario disporre di autorizzazioni in vRealize Automation e vRealize Operations Manager per configurare il posizionamento del carico di lavoro e il criterio di posizionamento.

Per configurare il posizionamento del carico di lavoro in vRealize Automation, è necessario disporre del ruolo Amministratore struttura. Vedere la panoramica sui ruoli dell'utente nel centro informazioni di vRealize Automation.

In vRealize Operations Manager, è necessario creare un ruolo utente per il posizionamento del carico di lavoro e assegnare autorizzazioni al ruolo.

- Assegnare l'autorizzazione di sola lettura all'account utente per host e cluster vSphere e per storage vSphere nella gerarchia degli oggetti.
- Per far sì che il ruolo utente possa utilizzare chiamate API nel posizionamento del carico di lavoro, assegnare autorizzazioni di lettura e scrittura sulle API. Selezionare **Amministrazione > Controllo accesso > Autorizzazioni** e scegliere **API REST > Tutte le altre API di lettura scrittura**.

vRealize Automation utilizza il ruolo vRealize Operations Manager quando si registra l'endpoint e per richiedere suggerimenti di posizionamento durante il provisioning per conto degli utenti che richiedono elementi del catalogo.

Per ulteriori informazioni, vedere la sezione sul controllo degli accessi del centro informazioni di vRealize Operations Manager.

Criterio di posizionamento

È possibile utilizzare il criterio di posizionamento per fare in modo che vRealize Automation stabilisca dove posizionare le macchine quando si distribuiscono nuovi blueprint. Il criterio di posizionamento utilizza l'analisi di vRealize Operations Manager per identificare i carichi di lavoro nei cluster e suggerire le destinazioni di posizionamento.

Prima di utilizzare il criterio di posizionamento, è necessario eseguire diversi passaggi. In vRealize Automation, creare endpoint per le istanze vRealize Operations Manager e vCenter Server. Quindi creare un gruppo di strutture e aggiungere prenotazioni all'endpoint vCenter Server.

Per garantire che vRealize Operations Manager fornisca analisi di posizionamento dei carichi di lavoro a vRealize Automation, è necessario:

- Installare la soluzione vRealize Automation nell'istanza di vRealize Operations Manager utilizzata per il posizionamento dei carichi di lavoro.
- Configurare vRealize Operations Manager per il monitoraggio del vCenter Server.

Per configurare vRealize Automation e vRealize Operations Manager per il posizionamento dei carichi di lavoro, vedere [Configurazione del posizionamento dei carichi di lavoro](#).

Individuazione del criterio di posizionamento

Nell'istanza di vRealize Automation selezionare **Infrastruttura > Prenotazioni > Criterio di posizionamento**.

Per utilizzare l'analisi di posizionamento dei carichi di lavoro che vRealize Operations Manager mette a disposizione, selezionare **Usa vRealize Operations Manager per suggerimenti di posizionamento**.

Se non si utilizza il criterio di posizionamento dei carichi di lavoro, vRealize Automation utilizzerà il metodo di posizionamento predefinito.

Configurazione del posizionamento dei carichi di lavoro

Per utilizzare il criterio di posizionamento in modo da posizionare le macchine quando si distribuiscono nuovi blueprint, è necessario configurare vRealize Automation per l'uso dei dati di analisi forniti da vRealize Operations Manager. È inoltre necessario configurare vRealize Operations Manager in modo da applicare un criterio per consolidare e bilanciare i carichi di lavoro sulle risorse di elaborazione cluster.

In vRealize Automation è possibile configurare gli endpoint, creare un gruppo di strutture e aggiungere prenotazioni. In vRealize Operations Manager è possibile configurare un criterio per il supporto del bilanciamento del carico di lavoro, da applicare successivamente a un gruppo personalizzato che include le proprie risorse di elaborazione personalizzate.

Prerequisiti

Prima che il criterio di posizionamento possa suggerire destinazioni di posizionamento per i blueprint, è necessario eseguire diversi passaggi.

- Comprendere il criterio di posizionamento. Vedere [Criterio di posizionamento](#).
- Verificare che in vRealize Automation sia disponibile un endpoint per l'istanza di vRealize Operations Manager utilizzata per il posizionamento dei carichi di lavoro. Vedere [Creazione di un endpoint vRealize Operations Manager](#).

- Verificare che in vRealize Automation sia disponibile un endpoint per l'istanza di vCenter Server. Vedere [Creazione di un endpoint vSphere in vRealize Automation e associazione a NSX](#).
- Aggiungere le prenotazioni all'endpoint vCenter Server. Vedere [Prenotazioni](#).
- Aggiungere un gruppo di strutture e verificare che l'utente sia un amministratore dei gruppi di strutture. Vedere [Creazione di un gruppo di strutture](#).
- Verificare che vRealize Operations Manager stia monitorando la stessa infrastruttura monitorata da vRealize Automation, per assicurarsi che includano le stesse istanze di vCenter Server. Vedere [VMware vSphere Solution in vRealize Operations Manager](#) nel centro informazioni di vRealize Operations Manager.
- Comprendere i concetti di prenotazione, prenotazione storage, blueprint e provider di delegati. Vedere il centro informazioni di vRealize Automation.
- Comprendere e definire le impostazioni di riempimento e bilanciamento nel criterio vRealize Operations Manager utilizzato per il posizionamento dei carichi di lavoro. Vedere il documento relativo ai [dettagli sull'automazione dei carichi di lavoro](#) (Workload Automation Details) nel centro informazioni di vRealize Operations Manager.

Procedura

1 [Configurazione di vRealize Automation per il posizionamento dei carichi di lavoro](#)

Per utilizzare analisi di posizionamento dei carichi di lavoro per posizionare macchine quando vengono distribuiti nuovi blueprint, è necessario preparare l'istanza di vRealize Automation.

2 [Configurazione di vRealize Operations Manager per posizionare carichi di lavoro in vRealize Automation](#)

Per fornire a vRealize Automation le analisi relative al posizionamento dei carichi di lavoro in modo da posizionare le macchine quando si distribuiscono nuovi blueprint, è necessario preparare l'istanza di vRealize Operations Manager.

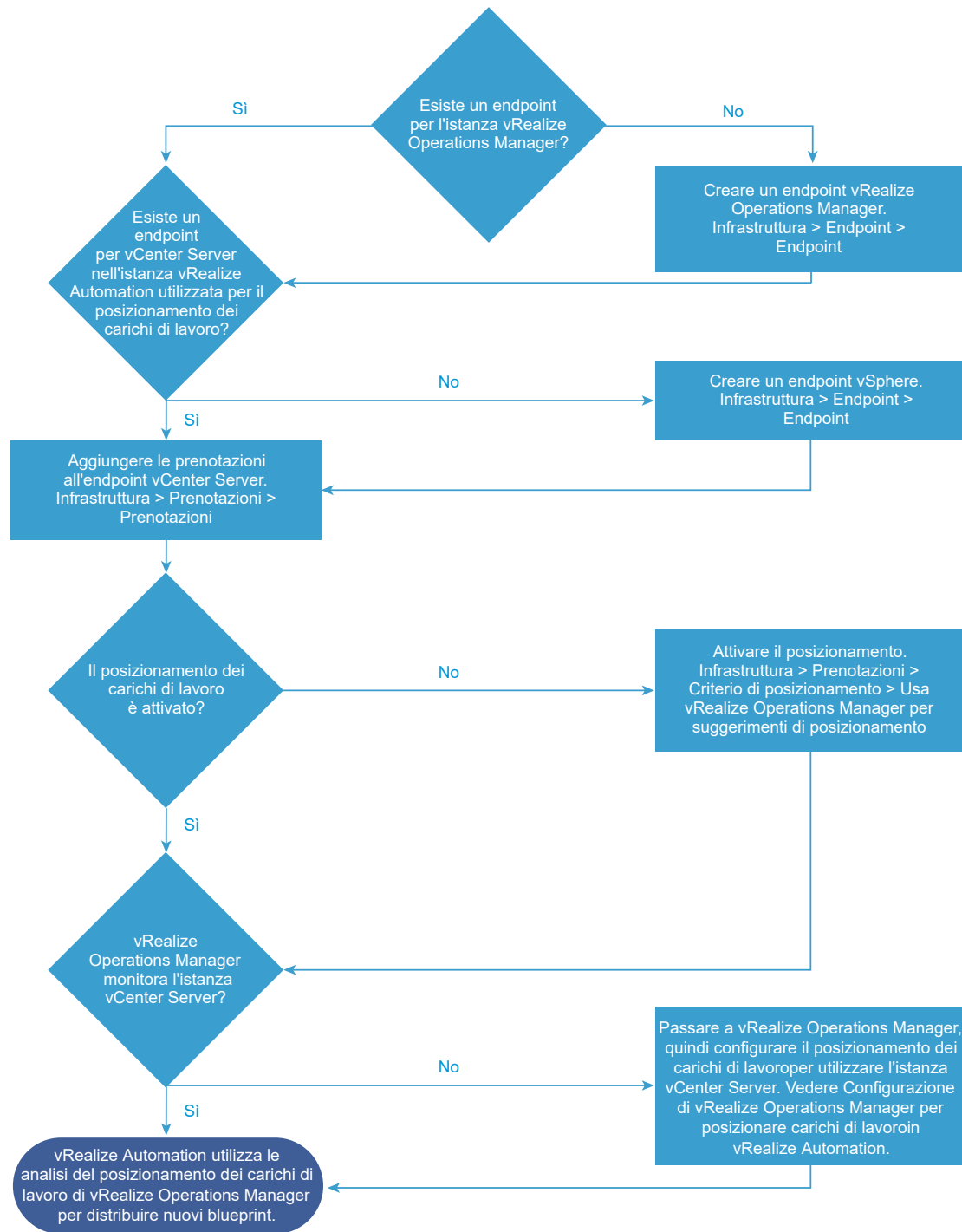
Risultati

vRealize Automation e vRealize Operations Manager sono stati configurati per l'uso dei dati di analisi del posizionamento dei carichi di lavoro per suggerire destinazioni di posizionamento per i nuovi blueprint.

Configurazione di vRealize Automation per il posizionamento dei carichi di lavoro

Per utilizzare analisi di posizionamento dei carichi di lavoro per posizionare macchine quando vengono distribuiti nuovi blueprint, è necessario preparare l'istanza di vRealize Automation.

Per preparare l'istanza di vRealize Automation per l'uso dei criteri di posizionamento, è necessario configurare gli endpoint, creare un gruppo di strutture e aggiungere prenotazioni.



Prerequisiti

- Per utilizzare il posizionamento dei carichi di lavoro, è necessario comprendere i requisiti. Vedere [Configurazione del posizionamento dei carichi di lavoro](#).
- In vRealize Automation, aggiungere un ruolo utente e autorizzazioni specifici per consentire a vRealize Operations Manager di convalidare le credenziali. Vedere la panoramica sui ruoli dell'utente nel centro informazioni di vRealize Automation.

Procedura

- 1 Nella propria istanza di vRealize Automation, aggiungere un endpoint per l'istanza di vRealize Operations Manager e fare clic su **OK**.
 - a Selezionare **Infrastruttura > Endpoint > Endpoint**.
 - b Selezionare **Nuovo > Gestione > vRealize Operations Manager**.
 - c Immettere le informazioni generali per l'endpoint **vRealize Operations Manager**.

Non è necessario specificare le proprietà per l'endpoint.

- 2 Nella propria istanza di vRealize Automation, aggiungere un endpoint per l'istanza di vCenter Server e fare clic su **OK**.
 - a Selezionare **Infrastruttura > Endpoint > Endpoint**.
 - b Selezionare **Nuovo > Virtuale > vSphere (vCenter)**.
 - c Immettere informazioni generali, proprietà e associazioni per l'endpoint di vCenter Server.

Una volta aggiunti gli endpoint, e al termine della raccolta dati da parte di vRealize Automation, saranno disponibili le risorse di elaborazione per tali endpoint. Sarà quindi possibile aggiungere le risorse di elaborazione al gruppo di strutture creato.

- 3 Creare un gruppo di strutture per consentire ad altri utenti di creare prenotazioni e consentire il criterio di posizionamento.
 - a Selezionare **Infrastruttura > Endpoint > Gruppi di strutture**.
 - b Fare clic su **Nuovo** e immettere le informazioni relative al gruppo di strutture.

Opzione	Descrizione
Nome	Immettere un nome significativo per il gruppo di strutture.
Descrizione	Immettere una descrizione utile.
Amministratori di struttura	Immettere l'indirizzo e-mail per ciascuna persona da indicare come amministratore della struttura.
Risorse di elaborazione	Selezionare i cluster della risorsa di elaborazione che gli amministratori possono gestire.

Una volta aggiunte risorse di elaborazione a un gruppo di strutture, e al termine della raccolta dati da parte di vRealize Automation, gli amministratori della struttura potranno creare prenotazioni per le risorse di elaborazione.

4 Creare prenotazioni per le risorse di elaborazione nell'istanza di vCenter Server.

- a Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- b Selezionare **Nuovo > vSphere (vCenter)**.
- c In ciascuna scheda, immettere le informazioni per la prenotazione.

Opzione	Azione
Generale	Selezionare un criterio di prenotazione, la priorità del criterio e fare clic su Attiva questa prenotazione .
Risorse	Selezionare quota macchina, memoria e storage. Non è necessario selezionare un pool di risorse.
Rete	Selezionare la scheda di rete. Non è necessario selezionare un profilo di rete.
Proprietà	Se necessario, aggiungere proprietà personalizzate alla prenotazione.
Avviso	Se necessario, selezionare Avvisi capacità per avvisare i destinatari quando la capacità supera la soglia della prenotazione.

5 Attivare il criterio di posizionamento.

- a Selezionare **Infrastruttura > Prenotazioni > Criterio di posizionamento**.
- b Selezionare la casella di controllo **Usa vRealize Operations Manager per consigli di posizionamento**.

Risultati

vRealize Automation è stato configurato per utilizzare le analisi di vRealize Operations Manager per posizionare le macchine quando gli utenti distribuiscono blueprint.

Operazioni successive

Configurare vRealize Operations Manager per monitorare l'istanza di vCenter Server e applicare un criterio di posizionamento dei carichi di lavoro alle risorse di elaborazione del cluster. Vedere [Configurazione di vRealize Operations Manager per posizionare carichi di lavoro in vRealize Automation](#).

Configurazione di vRealize Operations Manager per posizionare carichi di lavoro in vRealize Automation

Per fornire a vRealize Automation le analisi relative al posizionamento dei carichi di lavoro in modo da posizionare le macchine quando si distribuiscono nuovi blueprint, è necessario preparare l'istanza di vRealize Operations Manager.

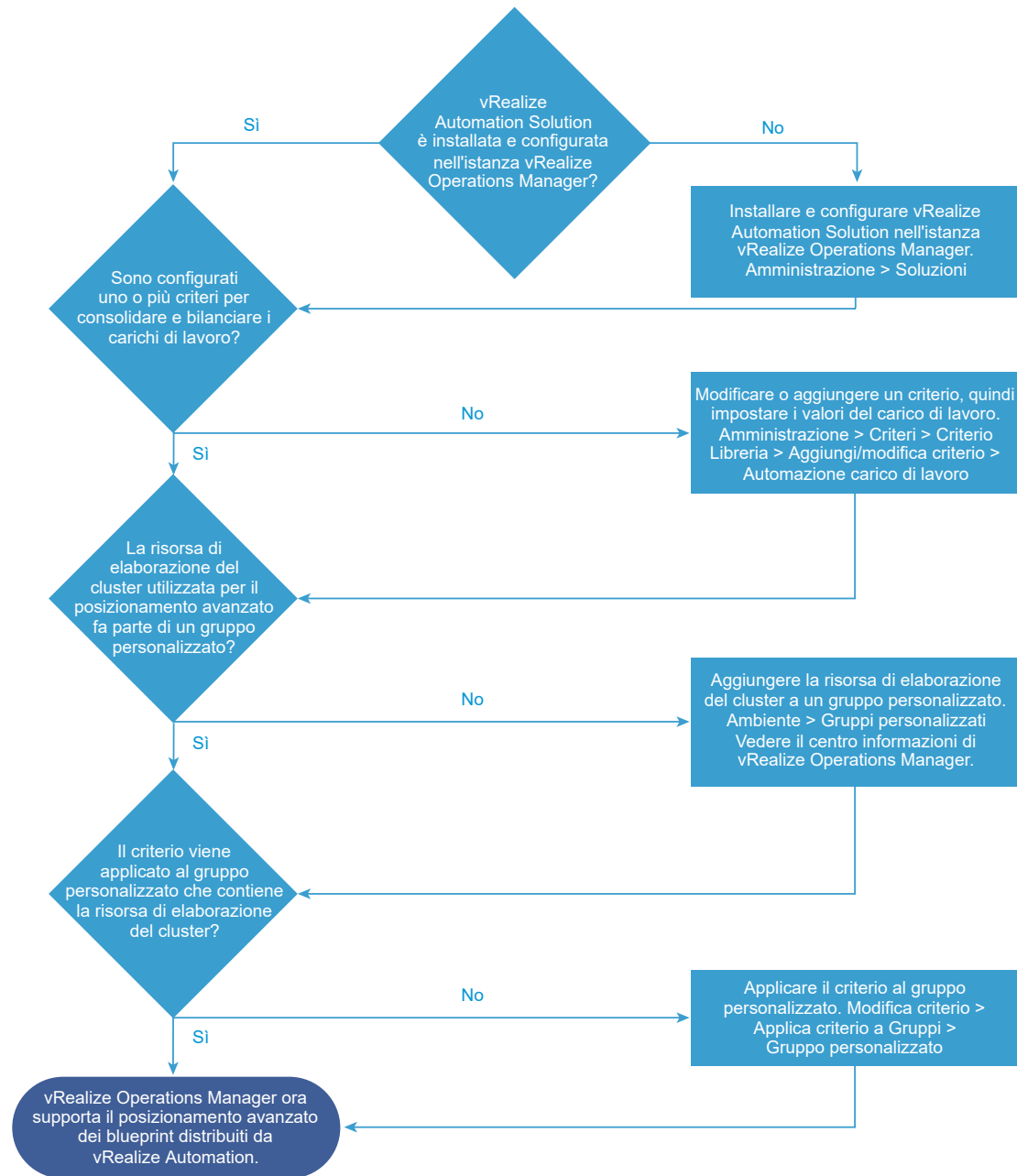
Attenzione È necessario installare la soluzione vRealize Automation, che comprende il Management Pack, solo su un'unica istanza di vRealize Operations Manager.

Per preparare l'istanza di vRealize Operations Manager in modo che fornisca le analisi a vRealize Automation, installare e configurare la soluzione vRealize Automation. È necessario configurare anche un criterio e applicarlo alle risorse di elaborazione del cluster.

Una volta configurata la soluzione vRealize Automation, non è possibile spostare o bilanciare di nuovo le macchine virtuali che vRealize Automation gestisce.

Se la soluzione vRealize Automation non è installata nell'istanza di vRealize Operations Manager, il posizionamento dei carichi di lavoro è ugualmente in grado di spostare o bilanciare di nuovo le macchine virtuali gestite da vRealize Automation.

Per consentire al posizionamento dei carichi di lavoro di spostare macchine virtuali, queste devono risiedere in un data center o in un data center personalizzato.



Prerequisiti

- Configurare vRealize Automation in modo da utilizzare le analisi relative al posizionamento dei carichi di lavoro. Vedere [Configurazione di vRealize Automation per il posizionamento dei carichi di lavoro](#).
- Verificare che la soluzione vRealize Automation sia installata e configurata nell'istanza di vRealize Operations Manager utilizzata per il posizionamento dei carichi di lavoro. Per ulteriori dettagli su questa soluzione, vedere [Management Pack for vRealize Automation su Solution Exchange](#). Per informazioni su come funziona il posizionamento dei carichi di lavoro in vRealize Operations Manager, vedere i [dettagli sull'automazione dei carichi di lavoro](#) e gli argomenti correlati nella documentazione di vRealize Operations Manager.

Procedura

- 1 Nell'istanza di vRealize Operations Manager che gestisce il posizionamento dei carichi di lavoro, installare e configurare la soluzione vRealize Automation.

La soluzione potrebbe già essere installata.

- a Per vedere le soluzioni installate in vRealize Operations Manager, fare clic su **Amministrazione > Soluzioni**.
- b Verificare se la soluzione vRealize Automation è già installata.
Se la soluzione vRealize Automation non viene visualizzata nell'elenco, scaricarla e installarla. Vedere [Management Pack for vRealize Automation su Solution Exchange](#).
- c Se viene visualizzata nell'elenco, selezionare la **soluzione VMWare vRealize Automation** e fare clic su **Configura**.
- d Configurare la soluzione vRealize Automation e salvare le impostazioni.
Per ulteriori informazioni sulla configurazione della soluzione, vedere le [soluzioni di vRealize Operations Manager](#) nel centro informazioni di vRealize Operations Manager.

- 2 Se non si utilizza il criterio predefinito di vRealize Operations Manager, è necessario creare un gruppo personalizzato. Aggiungere quindi le risorse di elaborazione dei cluster al gruppo personalizzato.

Per applicare ai cluster un criterio diverso da quello predefinito, aggiungere un gruppo personalizzato, quindi applicarvi il criterio. Se si utilizza un criterio predefinito, non è necessario creare un gruppo personalizzato perché il criterio predefinito si applica a tutti gli oggetti.

- a Fare clic su **Ambiente > Gruppi personalizzati**.
- b Se per i cluster non esiste un gruppo personalizzato, crearne uno.
Per ulteriori dettagli, vedere lo [scenario dell'utente relativo alla creazione di gruppi di oggetti personalizzati](#) nel centro informazioni di vRealize Operations Manager.
- c Aggiungere il cluster al gruppo personalizzato e salvare il gruppo.

- 3 Configurare un criterio per consolidare e bilanciare i carichi di lavoro nei cluster, quindi applicarlo al gruppo personalizzato.

I criteri di vRealize Operations Manager vengono configurati per stabilire le impostazioni di consolidamento, bilancio, compilazione, CPU, memoria e spazio su disco. Si supponga, ad esempio, di modificare l'impostazione relativa al consolidamento dei carichi di lavoro, in modo da determinare il migliore posizionamento dei nuovi carichi di lavoro gestiti in base allo stato e alla capacità del cluster. Si supponga inoltre di modificare l'impostazione di soglia per il bilanciamento dei carichi di lavoro, in modo da scegliere il livello di aggressività richiesto per posizionare i carichi di lavoro. È possibile configurare uno o più criteri e applicarli alle risorse di elaborazione del cluster.

- a Per individuare i criteri, fare clic su **Amministrazione > Criteri > Libreria di criteri**.
- b Per impostare i valori dei carichi di lavoro, fare clic su **Aggiungi/Modifica criterio**, quindi su **Automazione carico di lavoro**.

Le impostazioni relative ai carichi di lavoro consolidati e alla capacità aggiuntiva dei cluster si applicano al posizionamento iniziale delle macchine virtuali.

- Quando si impostano i carichi di lavoro consolidati su **nessuno**, il posizionamento dei carichi di lavoro bilancia il carico di lavoro su tutti i cluster a cui è applicato il criterio. Quando si impostano i carichi di lavoro consolidati su un valore diverso da nessuno, il posizionamento dei carichi di lavoro riempie prima il cluster più impegnato.
 - La capacità aggiuntiva del cluster corrisponde allo spazio riservato del buffer in un cluster, espresso come percentuale della capacità totale. Ad esempio, se si imposta la capacità aggiuntiva del cluster su 20%, quel buffer potrebbe impedire al posizionamento dei carichi di lavoro di posizionare macchine virtuali su quel cluster. Il motivo per cui il posizionamento è impedito è che il cluster ha il 20% in meno di capacità disponibile per la CPU, la memoria o lo spazio su disco.
- c Nell'area di lavoro dei criteri, fare clic su **Applica criterio ai gruppi**.
 - d Selezionare il gruppo personalizzato.
 - e Salvare il criterio.

Risultati

vRealize Operations Manager è stato configurato in modo che vRealize Automation utilizzi le analisi relative al posizionamento dei carichi di lavoro e suggerisca le destinazioni di posizionamento delle macchine quando gli utenti distribuiscono blueprint.

Operazioni successive

Attendere che vRealize Automation e vRealize Operations Manager raccolgano i dati dagli endpoint e dagli oggetti nell'ambiente. Quindi, quando si distribuiscono nuovi blueprint, vRealize Automation mostra i consigli relativi al posizionamento dei carichi di lavoro, i candidati di destinazione e il posizionamento selezionato per la conferma.

Risoluzione dei problemi relativi al posizionamento dei carichi di lavoro

Per risolvere problemi relativi al posizionamento dei carichi di lavoro, utilizzare le informazioni sulla risoluzione dei problemi.

Per garantire il corretto funzionamento del posizionamento del carico di lavoro, è necessaria la soluzione vRealize Automation

Il posizionamento dei carichi di lavoro è basato sulle singole macchine, e il posizionamento viene effettuato a livello di macchina. Quando si installano insieme vRealize Automation e vRealize Operations Manager, è necessario installare anche la soluzione vRealize Automation.

La soluzione, che include il pacchetto di gestione e l'adattatore, identifica i cluster in cui sono disattivate le azioni di ribilanciamento del contenitore e spostamento delle macchine virtuali. L'azione di ribilanciamento è disattivata nel data center personalizzato a cui il cluster appartiene.

- Per i cluster di vRealize Automation non gestiti che appartengono a un data center personalizzato che non include alcun cluster di vRealize Automation gestito, le azioni di spostamento delle macchine virtuali e ribilanciamento del contenitore sono abilitate. Per i cluster di vRealize Automation gestiti, queste azioni sono disattivate.
- In vRealize Operations Manager l'adattatore di vRealize Automation fa in modo che le macchine virtuali dei cluster mappati alle prenotazioni non siano disponibili per lo spostamento o il ribilanciamento.

Attenzione La soluzione vRealize Automation deve essere installata solo in un'istanza singola di vRealize Operations Manager.

La modalità ad alta disponibilità è attivata ma deve essere disattivata

Quando la modalità HA è attivata, se vRealize Operations Manager è inattivo, il timeout utilizzato per il posizionamento dei carichi di lavoro per la chiamata a vRealize Operations Manager potrebbe non riuscire.

vRealize Automation registra gli errori relativi al posizionamento del carico di lavoro nel file di registro `catalina.out`.

Gli endpoint vSphere in vRealize Automation non sono monitorati

vRealize Operations Manager non esegue il monitoraggio dell'istanza vCenter Server di vSphere che contiene i cluster di prenotazione.

Se vRealize Operations Manager non riconosce le prenotazioni candidato di vRealize Automation per un cluster, un datastore o un cluster di datastore quando prova a posizionarle, le ignora. Nella risposta al posizionamento, vRealize Operations Manager comunica a vRealize Automation che non le riconosce.

A questo punto, nei dettagli di posizionamento dell'esecuzione della richiesta, vRealize Automation visualizza un'icona di avviso sulla prenotazione candidato per indicare che non è stata riconosciuta.

In caso di mancata corrispondenza, viene visualizzato vRealize Automation in alto nell'elenco

vRealize Automation e vRealize Operations Manager gestiscono viste diverse dell'infrastruttura. Tuttavia devono entrambi gestire le identiche istanze di vCenter Server nella stessa infrastruttura.

Devono identificare disconnessioni e mancate corrispondenze e visualizzare i dettagli.

Cosa fare se l'adattatore di vRealize Automation è inattivo

Il posizionamento iniziale rispetta sempre l'elenco dei candidati di destinazione che riceve da vRealize Operations Manager, ad esempio quando un utente aggiunge un cluster immediatamente dopo l'installazione.

Se la soluzione vRealize Automation, che include il pacchetto di gestione e l'adattatore, non è disponibile in vRealize Operations Manager, le azioni di spostamento delle macchine virtuali e di ribilanciamento del contenitore non sono disponibili.

Ottimizzazione continua con vRealize Operations Manager

L'ottimizzazione continua offre la gestione continua e autonoma dei carichi di lavoro di vRealize Automation da vRealize Operations Manager.

Con l'ottimizzazione continua si sfruttano i vantaggi del ribilanciamento e riposizionamento dei carichi di lavoro e si utilizza vRealize Automation con vRealize Operations Manager oltre il posizionamento dei carichi di lavoro iniziale. Quando le risorse di virtualizzazione vengono spostate o ricevono carichi più pesanti o più leggeri, è possibile spostare i carichi di lavoro di vRealize Automation forniti in provisioning in base alle esigenze.

- L'ottimizzazione continua crea automaticamente un nuovo data center vRealize Operations Manager.

Viene creato un nuovo data center per ogni endpoint vCenter vRealize Automation.

- Il data center appena creato contiene ogni cluster gestito di vRealize Automation associato all'endpoint.

Nota Non creare manualmente un data center misto di cluster di vRealize Automation e non di vRealize Automation.

- È possibile eseguire l'ottimizzazione continua solo dal data center basato su vRealize Automation appena creato.
- L'ottimizzazione non supporta requisiti di prenotazione diversi tra i cluster in vCenter, che potrebbero verificarsi quando sono presenti gruppi di business diversi.

L'ottimizzazione si trova a livello di data center basato su vRealize Automation e requisiti di prenotazione diversi attraverso i cluster possono impedire il buon fine. Quando ciò si verifica, viene visualizzato un errore indicante che alcuni dei cluster di destinazione o di storage non soddisfacevano i requisiti, impedendo alcune azioni di ottimizzazione.

- L'ottimizzazione non crea mai una nuova violazione dei criteri di vRealize Automation o vRealize Operations Manager.
 - Se sono già presenti violazioni dei criteri, l'ottimizzazione può risolvere problemi dello scopo operativo di vRealize Operations Manager.
 - Se sono già presenti violazioni dei criteri, l'ottimizzazione non può risolvere problemi dello scopo di business di vRealize Operations Manager.

Ad esempio, se una macchina virtuale è stata spostata manualmente in un cluster che non fa parte del suo criterio di prenotazione, vRealize Operations Manager non rileva una violazione né tenta di risolvere il problema. Per risolvere i problemi relativi allo scopo di business, è necessario utilizzare vRealize Automation per spostare il carico di lavoro.

- Questa release rispetta lo scopo operativo a livello di data center. Tutti i cluster di vRealize Automation membro sono ottimizzati con le stesse impostazioni.

Per impostare uno scopo operativo differenti per i cluster, è necessario configurarli in data center di vRealize Automation separati, associati agli endpoint vCenter separati. Un esempio di situazione può essere differenti cluster di verifica e di produzione.

- vRealize Operations Manager invia una query a vRealize Automation per il posizionamento consentito in base alle prenotazioni e ai criteri di vRealize Automation.
- I tag di posizionamento di vRealize Operations Manager non possono essere applicati ai carichi di lavoro a cui vRealize Automation esegue il provisioning.

Inoltre, è supportata l'ottimizzazione pianificata con più macchine. Le ottimizzazioni regolarmente pianificate non sono processi radicali. Se le condizioni interrompono il movimento della macchina, le macchine correttamente trasferite rimangono trasferite e il ciclo vRealize Operations Manager successivo tenta di trasferire il resto come di consueto per vRealize Operations Manager. Tale ottimizzazione parzialmente completata non causa alcun impatto negativo in vRealize Automation.

Individuazione dei carichi di lavoro non bilanciati in vRealize Automation

vRealize Automation consente di rilevare quando i carichi di lavoro sono fortemente sottoposti a provisioning allo stesso cluster.

Procedura

- 1 Per visualizzare dove viene eseguito il provisioning dei carichi di lavoro, fare clic su **Infrastruttura > Elabora risorse > Elabora risorse**.

Prendere nota di un eventuale posizionamento sbilanciato delle macchine.

- 2 Le prenotazioni possono causare un provisioning elevato allo stesso cluster. Per rivedere le prenotazioni, fare clic su **Infrastruttura > Prenotazioni > Prenotazioni**.

Tenere presente la priorità e la sua influenza sul posizionamento di una macchina.

Abilitazione dell'ottimizzazione continua

Quando si aggiunge l'adattatore vRealize Automation in vRealize Operations Manager, vRealize Operations Manager crea automaticamente un nuovo data center dedicato per i carichi di lavoro basati su vRealize Automation.

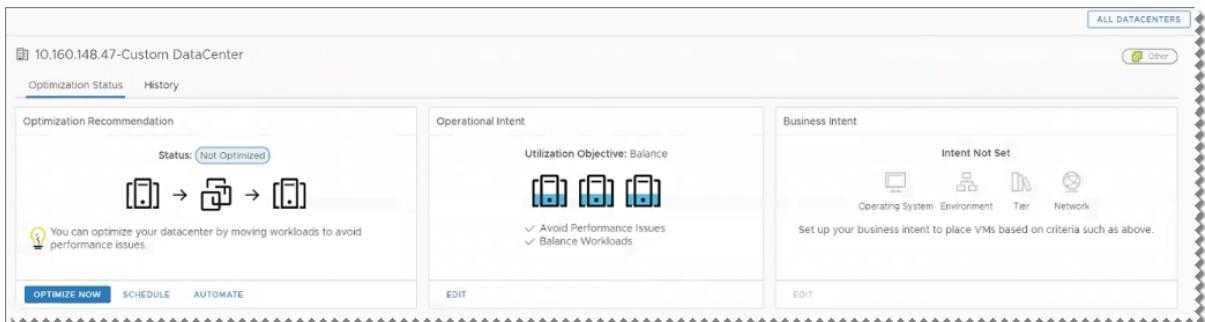
Oltre ad aggiungere l'adattatore, non esistono passaggi di installazione separati per l'ottimizzazione continua. È possibile iniziare a configurare e utilizzare vRealize Operations Manager per il trasferimento dei carichi di lavoro nel nuovo data center. Vedere [Esempio di ottimizzazione continua](#).

Esempio di ottimizzazione continua

L'esempio seguente mostra un flusso di lavoro di ribilanciamento per l'ottimizzazione continua di vRealize Automation con vRealize Operations Manager.

- 1 Nella pagina iniziale di vRealize Operations Manager, fare clic su **Ottimizzazione carico di lavoro**.
- 2 Selezionare il data center vRealize Automation creato automaticamente.
- 3 In **Scopo operativo**, fare clic su **Modifica** e selezionare **Bilancia**.

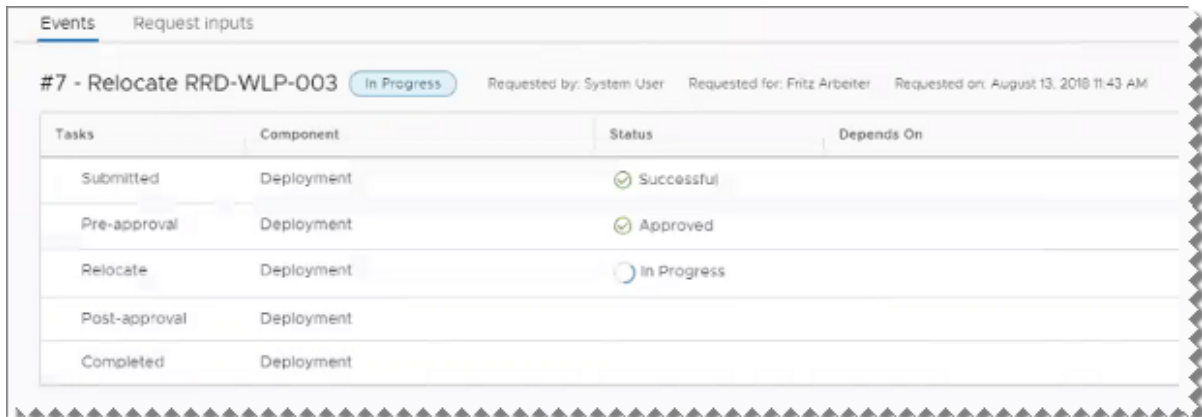
È possibile selezionare o modificare lo scopo di business, disattivate quando il data center è dedicato all'ottimizzazione di vRealize Automation.



- 4 In **Raccomandazione ottimizzazione**, fare clic su **Ottimizza ora**.

vRealize Operations Manager mostra un diagramma sulla situazione precedente e successiva all'operazione proposta.

- 5 Fare clic su **Avanti**.
- 6 Fare clic su **Inizia azione**.
- 7 In vRealize Automation, monitorare l'operazione in corso facendo clic su **Distribuzioni** e osservando lo stato dell'evento.

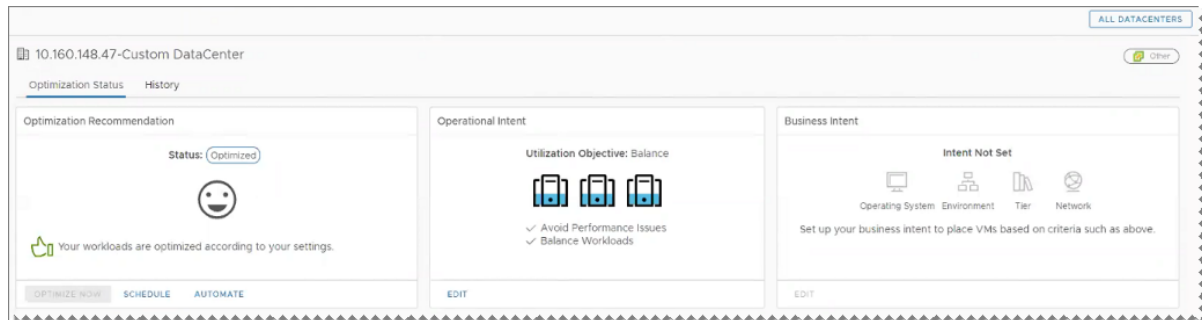


The screenshot shows the 'Events' tab in vRealize Automation. It displays a task titled '#7 - Relocate RRD-WLP-003' with a status of 'In Progress'. The task was requested by 'System User' for 'Fritz Arbeiter' on 'August 13, 2018 11:43 AM'. Below the header is a table with the following data:

Tasks	Component	Status	Depends On
Submitted	Deployment	Successful	
Pre-approval	Deployment	Approved	
Relocate	Deployment	In Progress	
Post-approval	Deployment		
Completed	Deployment		

Quando il ribilanciamento termina, vRealize Automation viene aggiornato. La pagina **Elabora risorse** mostra che le macchine sono state trasferite.

In vRealize Operations Manager, la raccolta dati successiva aggiorna la visualizzazione per mostrare che l'ottimizzazione è completa.



In vRealize Operations Manager è possibile rivedere l'operazione facendo clic su

Amministrazione > Cronologia > Attività recenti.

Individuazione dei data center di vRealize Automation in vRealize Operations Manager

È possibile utilizzare vRealize Operations Manager per visualizzare solo i data center gestiti da vRealize Automation.

Procedura

- 1 Nella pagina iniziale di vRealize Operations Manager, fare clic su **Ottimizzazione carico di lavoro**.
- 2 In alto a destra, fare clic sul menu a discesa **Visualizza**.

3 Selezionare solo i data center gestiti da vRealize Automation.



Gestione delle coppie di chiavi

Le coppie di chiavi sono utilizzate per eseguire il provisioning e connettersi a un'istanza cloud. Una coppia di chiavi è utilizzata per decrittografare le password di Windows o accedere a una macchina Linux.

Coppie di chiavi sono necessarie per il provisioning con Amazon Web Services. Per Red Hat OpenStack, l'uso di coppie di chiavi è facoltativo.

Le coppie di chiavi esistenti vengono importate come parte della raccolta dati quando si aggiunge un endpoint cloud. Un amministratore di struttura può anche creare e gestire coppie di chiavi utilizzando la console di vRealize Automation. Se si elimina una coppia di chiavi dalla console di vRealize Automation, essa viene eliminata anche dall'account del servizio cloud.

Oltre a gestire manualmente le coppie di chiavi, è possibile configurare vRealize Automation per generare coppie di chiavi automaticamente per macchina o per gruppo di business.

- Un amministratore di struttura può configurare la generazione automatica di coppie di chiavi a livello di prenotazione.
- Se la coppia di chiavi dovrà essere controllata a livello di blueprint, l'amministratore di struttura deve selezionare **Non specificato** nella prenotazione.
- Un amministratore tenant o un manager del gruppo di business può configurare la generazione automatica di coppie di chiavi a livello di un blueprint.
- Se la generazione delle coppie di chiavi è configurata sia al livello di prenotazione che al livello di blueprint, l'impostazione della prenotazione ha priorità su quella del blueprint.

Creazione di una coppia di chiavi

È possibile creare coppie di chiavi da impiegare con gli endpoint utilizzando vRealize Automation.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Creare un endpoint cloud e aggiungere le risorse di elaborazione cloud a un gruppo di strutture. Vedere [Scelta dello scenario per un endpoint](#) e [Creazione di un gruppo di strutture](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Coppie di chiavi**.

- 2 Fare clic su **Nuovo**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare una regione cloud dal menu a discesa **Risorsa di elaborazione**.
- 5 Fare clic su **OK**.

Risultati

La coppia di chiavi è pronta all'uso quando la colonna Chiave privata presenta il valore
*****.



Caricamento della chiave privata per una coppia di chiavi

È possibile caricare la chiave privata per una coppia di chiavi in formato PEM.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- È necessario disporre già di una coppia di chiavi. Vedere [Creazione di una coppia di chiavi](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Coppie di chiavi**.
- 2 Individuare la coppia di chiavi per cui caricare una chiave privata.
- 3 Fare clic sull'icona **Modifica** (.
- 4 Il caricamento della chiave può essere eseguito nei modi seguenti.
 - Portarsi nella cartella del file codificato in PEM e fare clic su **Carica**.
 - Incollare il testo della chiave privata che inizia con -----BEGIN RSA PRIVATE KEY----- e termina con -----END RSA PRIVATE KEY-----.
- 5 Fare clic sull'icona **Salva** (.

Esportazione della chiave privata da una coppia di chiavi

È possibile esportare la chiave privata da una coppia di chiavi in un file con codifica PEM.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Deve esistere una coppia di chiavi con una chiave privata. Vedere [Caricamento della chiave privata per una coppia di chiavi](#).

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Coppie di chiavi**.
- 2 Individuare la coppia di chiavi da cui esportare la chiave privata.

- 3 Fare clic sull'icona **Esporta** (📄🔗).
- 4 Selezionare la posizione in cui salvare il file e fare clic su **Salva**.

Scenario: applicazione di una posizione a una risorsa di elaborazione per distribuzioni tra più regioni

Nelle distribuzioni tra più regioni, l'amministratore della struttura può avere l'esigenza di indicare se le risorse di elaborazione appartengono, ad esempio, al data center di Boston o di Londra. Se gli architetti dei blueprint attivano la funzionalità delle posizioni, gli utenti possono scegliere se eseguire il provisioning di macchine nel data center di Boston o di Londra.



Se si dispone di un data center a Londra e uno a Boston, è importante evitare che gli utenti di Boston eseguano il provisioning di macchine sull'infrastruttura di Londra e viceversa. Affinché gli utenti di Boston e Londra possano eseguire il provisioning solo nella propria infrastruttura, è necessario consentire loro di selezionare la posizione appropriata per il provisioning al momento della richiesta delle macchine.

Prerequisiti

- Accedere a vRealize Automation come **amministratore di struttura**.
- Un amministratore di sistema può definire le posizioni dei data center. Vedere [Scenario: aggiunta di posizioni di data center per distribuzioni tra più regioni](#).

Procedura

- 1 Selezionare **Infrastruttura > Risorse di elaborazione > Risorse di elaborazione**.
- 2 Individuare la risorsa di elaborazione che si trova nel data center di Boston e fare clic su **Modifica**.
- 3 Selezionare Boston dal menu a discesa **Posizioni**.
- 4 Fare clic su **OK**.
- 5 Ripetere questa procedura per associare ulteriori risorse di elaborazione a Boston e a Londra.

Risultati

Gli architetti IaaS possono attivare la funzionalità delle posizioni per consentire agli utenti di scegliere se eseguire il provisioning delle macchine a Boston o Londra, durante la compilazione dei moduli di richiesta per gli elementi del catalogo. Vedere [Abilitazione degli utenti a selezionare posizioni di datacenter per distribuzioni tra più regioni](#).

Provisioning di una distribuzione di vRealize Automation mediante un provider IPAM di terze parti

È possibile ottenere indirizzi e intervalli IP che possano essere utilizzati in un profilo di rete vRealize Automation da un provider di soluzioni IPAM di terze parti supportato, ad esempio Infoblox.

Gli intervalli degli indirizzi IP nel profilo di rete vengono usati in una prenotazione associata, specificata in un blueprint. Quando un utente autorizzato richiede il provisioning della macchina utilizzando un elemento del catalogo del blueprint, si ottiene un indirizzo IP dall'intervallo di indirizzi IP specificato dall'IPAM di terze parti. Dopo la distribuzione della macchina, è possibile scoprire l'indirizzo IP utilizzato interrogando la relativa pagina dei dettagli degli elementi di vRealize Automation.

Tabella 2-19. Preparazione per il provisioning di una distribuzione di vRealize Automation mediante elenco di controllo dell'IPAM Infoblox

Attività	Descrizione	Dettagli
Ottenere, importare e configurare il plug-in o il pacchetto del provider di soluzioni IPAM di terze parti.	Ottenere e importare il plug-in di vRealize Orchestrator, eseguire i workflow di configurazione di vRealize Orchestrator e registrare il tipo di endpoint del provider IPAM in vRealize Orchestrator. Se VMware Solution Exchange all'indirizzo https://marketplace.vmware.com/vsx non contiene il pacchetto del provider IPAM necessario, è possibile crearne uno utilizzando l'SDK di un provider di soluzioni IPAM e la documentazione di supporto. Vedere la pagina Esempio di pacchetto IPAM di terze parti di vRealize Automation in code.vmware.com/web/sdk .	Vedere Elenco di controllo per fornire il supporto del provider IPAM di terze parti .
Creare un endpoint del provider di soluzioni IPAM di terze parti.	Creare un nuovo endpoint IPAM in vRealize Automation.	Vedere Creazione di un endpoint di un provider IPAM di terze parti .
Specificare le impostazioni dell'endpoint del provider di soluzioni IPAM di terze parti in un profilo di rete esterno.	Creare un profilo di rete esterna e specificare l'endpoint IPAM definito in vRealize Automation.	Vedere Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti .

Tabella 2-19. Preparazione per il provisioning di una distribuzione di vRealize Automation mediante elenco di controllo dell'IPAM Infoblox (continua)

Attività	Descrizione	Dettagli
Facoltativamente, è possibile specificare le impostazioni dell'endpoint del provider di soluzioni IPAM di terze parti in un profilo di rete instradata.	Creare un profilo di rete su richiesta e specificare l'endpoint IPAM definito in vRealize Automation.	Vedere Creazione di un profilo di rete instradata mediante un endpoint IPAM di terze parti o Creazione di un profilo di rete NAT mediante un endpoint IPAM di terze parti in vRealize Automation .
Definire una prenotazione per utilizzare il profilo di rete.	Creare una prenotazione che chiami il profilo di rete in vRealize Automation.	Vedere Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer .
Definire un blueprint che utilizzi il profilo di rete.	Creare un blueprint che utilizzi la prenotazione in vRealize Automation.	Vedere Capitolo 3 Fornire blueprint di servizio agli utenti .
Pubblicare il blueprint nel catalogo per renderlo disponibile all'uso.	Pubblicare il blueprint nel catalogo in vRealize Automation. Aggiungere tutti i permessi necessari.	Vedere Pubblicazione di un blueprint .
Richiedere il provisioning della macchina utilizzando l'elemento blueprint del catalogo.	Utilizzare l'elemento del catalogo di blueprint per richiedere il provisioning della macchina in vRealize Automation	Vedere Gestione del catalogo dei servizi .

Configurazione delle risorse XaaS

La configurazione degli endpoint XaaS consente di connettere vRealize Automation al proprio ambiente. Per configurare i plug-in di vRealize Orchestrator come endpoint, si utilizza l'interfaccia utente di vRealize Automation e non l'interfaccia di configurazione di vRealize Orchestrator.

Per utilizzare le capacità di vRealize Orchestrator e i plug-in di vRealize Orchestrator per esporre VMware e tecnologie di terze parti a vRealize Automation, è possibile configurare i plug-in di vRealize Orchestrator aggiungendoli come endpoint. Così facendo vengono create delle connessioni a diversi host e server, come ad esempio istanze di vCenter Server, un host Microsoft Active Directory e così via.

Quando si aggiunge un plug-in di vRealize Orchestrator come endpoint tramite l'interfaccia utente di vRealize Automation, si esegue un workflow di configurazione nel server vRealize Orchestrator predefinito. I workflow di configurazione si trovano nella cartella dei workflow **vRealize Automation > XaaS > Configurazione endpoint**.

Importante la configurazione di un singolo plug-in in vRealize Orchestrator e nella console di vRealize Automation non è supportata e genera errori.

Configurazione del plug-in di Active Directory come endpoint

Aggiungere un endpoint e configurare il plug-in di Active Directory per connettersi a un'istanza di Active Directory in esecuzione e gestire utenti e gruppi di utenti, computer di Active Directory, unità organizzative e così via.

Una volta aggiunto un endpoint Active Directory, è possibile aggiornarlo in qualsiasi momento.

Prerequisiti

- Assicurarsi di avere accesso a un'istanza di Microsoft Active Directory. Vedere la documentazione Microsoft Active Directory.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Nel menu a discesa **Plug-in**, selezionare **Active Directory**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.
- 7 Configurare i dettagli relativi al server di Active Directory.
 - a Nella casella di testo **IP/URL host Active Directory**, specificare l'indirizzo IP o il nome DNS dell'host su cui è eseguito Active Directory.
 - b Immettere la porta di ricerca del server di Active Directory nella casella di testo **Porta**.

vRealize Orchestrator supporta la struttura gerarchica dei domini di Active Directory. Se il controller di dominio è configurato per utilizzare il catalogo globale, è necessario utilizzare la porta 3268. Non è possibile utilizzare la porta predefinita 389 per connettersi al server del catalogo globale. Oltre alle porte 389 e 3268, è possibile utilizzare 636 per LDAPS.
 - c Immettere l'elemento radice del servizio Active Directory nella casella di testo **Radice**.

Ad esempio, se il nome del dominio è *mycompany.com*, la radice di Active Directory è **dc=mycompany,dc=com**.

Questo nodo è utilizzato per esplorare la directory del servizio dopo aver immesso credenziali appropriate. Quando le directory del servizio sono di grandi dimensioni, la definizione di un nodo nella struttura restringe la ricerca e migliora le prestazioni. Ad esempio, invece di cercare nell'intera directory, è possibile specificare **ou=employees,dc=mycompany,dc=com**. Questo elemento radice visualizza tutti gli utenti nel gruppo Employees.
 - d (Facoltativo) Per attivare la certificazione codificata per la connessione tra vRealize Orchestrator e Active Directory, selezionare **Sì** dal menu a discesa **Usa SSL**.

Il certificato SSL viene automaticamente importato senza richiedere conferma, anche se il certificato è autofirmato.
 - e (Facoltativo) Immettere il dominio nella casella di testo **Dominio predefinito**.

Ad esempio, se il nome del dominio è *mycompany.com*, immettere **@mycompany.com**.

8 Configurare le impostazioni della sessione condivisa.

Le credenziali vengono utilizzate da vRealize Orchestrator per eseguire tutti i workflow e le azioni di Active Directory.

- a Immettere il nome utente per la sessione condivisa nella casella di testo **Nome utente per la sessione condivisa**.
- a Immettere la password per la sessione condivisa nella casella di testo **Password per la sessione condivisa**.

9 Fare clic su **Fine**.

Risultati

L'istanza di Active Directory come endpoint è stata aggiunta. Gli architetti di XaaS possono utilizzare XaaS per pubblicare workflow del plug-in di Active Directory come elementi di catalogo e azioni risorsa.

Operazioni successive

- Per utilizzare i blueprint di vRealize Automation per gestire gli utenti di Active Directory nel proprio ambiente, creare un blueprint di XaaS basato su Active Directory. Per un esempio, vedere [Creazione di un blueprint di XaaS e di un'azione per la creazione e la modifica di un utente](#).
- Per utilizzare vRealize Automation per creare i record di Active Directory quando si distribuisce una macchina, è possibile creare diversi criteri di Active Directory e applicarli a diversi gruppi di business e blueprint. Vedere [Creazione e applicazione di criteri di Active Directory](#).

Configurazione del plug-in HTTP-REST come endpoint

È possibile aggiungere un endpoint e configurare il plug-in HTTP-REST per la connessione a un host REST.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.
- Assicurarsi di poter accedere a un host REST.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Selezionare **HTTP-REST** dal menu a discesa **Plug-in**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.

7 Fornire i dati dell'host REST.

- a Immettere il nome dell'host nella casella di testo **Nome**.
- b Immettere l'indirizzo dell'host nella casella di testo **URL**.

Nota se si utilizza l'autenticazione degli accessi Kerberos, è necessario fornire l'indirizzo host in formato FQDN.

- c (Facoltativo) Nella casella di testo **Timeout connessione (secondi)** specificare quanti secondi devono trascorrere prima che si verifichi il timeout di una connessione.

Il valore predefinito è 30 secondi.

- d (Facoltativo) Nella casella di testo **Timeout operazione (secondi)** specificare quanti secondi devono trascorrere prima che si verifichi il timeout di un'operazione.

Il valore predefinito è 60 secondi.

8 (Facoltativo) Configurare le impostazioni del proxy.

- a Selezionare **Sì** per usare un proxy dal menu a discesa **Utilizza proxy**.
- b Immettere l'indirizzo IP del server proxy nella casella di testo **Indirizzo proxy**.
- c Nella casella di testo **Porta** specificare il numero della porta da utilizzare per comunicare con il server proxy.

9 Fare clic su **Avanti**.**10** Selezionare il tipo di autenticazione.

Opzione	Azione
Nessuno	Non è richiesta alcuna autenticazione.
OAuth 1.0	<p>Utilizza il protocollo OAuth 1.0. Fornire i parametri di autenticazione richiesti da OAuth 1.0.</p> <ul style="list-style-type: none"> a Nella casella di testo Chiave utente immettere la chiave utilizzata per identificare l'utente come provider di servizi. b Nella casella di testo Segreto utente immettere il segreto per confermare l'effettiva proprietà della chiave utente. c (Facoltativo) Nella casella di testo Token di accesso immettere il token di accesso utilizzato dall'utente per accedere alle risorse protette. d (Facoltativo) Nella casella di testo Segreto token di accesso immettere il segreto per confermare l'effettiva proprietà del token.
OAuth 2.0	<p>Utilizza il protocollo OAuth 2.0.</p> <p>Immettere il token di autenticazione nella casella di testo Token.</p>
Di base	<p>Offre un metodo di autenticazione degli accessi di base. La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ul style="list-style-type: none"> a Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente autenticazione. b Immettere la password per la sessione condivisa nella casella di testo Password di autenticazione.

Opzione	Azione
Digest	<p>Offre l'autenticazione degli accessi di tipo digest con codifica. La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ol style="list-style-type: none"> Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente autenticazione. Immettere la password per la sessione condivisa nella casella di testo Password di autenticazione.
NTLM	<p>Offre l'autenticazione degli accessi NT LAN Manager (NTLM) nell'ambito del framework Window Security Support Provider (SSP). La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ol style="list-style-type: none"> Fornire le credenziali utente per la sessione condivisa. <ul style="list-style-type: none"> Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente autenticazione. Immettere la password per la sessione condivisa nella casella di testo Password di autenticazione. Configurazione dei dettagli NTLM <ul style="list-style-type: none"> (Facoltativo) Immettere il nome della workstation nella casella di testo Workstation per autenticazione NTLM. Immettere il nome di dominio nella casella di testo Dominio per autenticazione NTLM.
Kerberos	<p>Offre l'autenticazione degli accessi Kerberos. La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ol style="list-style-type: none"> Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente autenticazione. Immettere la password per la sessione condivisa nella casella di testo Password di autenticazione.

11 Fare clic su **Fine**.

Risultati

È stato configurato un endpoint ed è stato aggiunto un host REST. Gli architetti XaaS possono usare XaaS per pubblicare i workflow del plug-in HTTP-REST come elementi di catalogo e azioni per risorse.

Configurazione del plug-in PowerShell come endpoint

È possibile aggiungere un endpoint e configurare il plug-in PowerShell per la connessione a un host PowerShell in esecuzione, affinché sia possibile effettuare chiamate a script e cmdlet PowerShell dalle azioni e dai workflow di vRealize Orchestrator.

Prerequisiti

- Assicurarsi di avere accesso a un host Windows PowerShell. Per ulteriori informazioni su Microsoft Windows PowerShell, vedere la documentazione di Windows PowerShell.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- Selezionare **Amministrazione > Configurazione vRO > Endpoint**.

- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Selezionare **PowerShell** dal menu a discesa **Plug-in**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome per l'endpoint PowerShell.
- 6 (Facoltativo) Immettere una descrizione per l'endpoint PowerShell.
- 7 Fare clic su **Avanti**.
- 8 Specificare i dati dell'host PowerShell.
 - a Immettere il nome dell'host nella casella di testo **Nome**.
 - b Immettere l'indirizzo IP o FQDN dell'host nella casella di testo **Host/IP**.
- 9 Configurare le impostazioni di WinRM per l'host di PowerShell.
 - a Nella casella di testo **Porta**, nella sezione dei dettagli dell'host PowerShell, immettere il numero della porta da usare per la comunicazione con l'host.
 - b Selezionare un protocollo di trasporto dal menu a discesa **Protocollo di trasporto**.

Nota Se si utilizza il protocollo di trasporto HTTPS, il certificato dell'host PowerShell remoto viene importato nel keystore di vRealize Orchestrator.

 - c Selezionare il tipo di autenticazione dal menu a discesa **Autenticazione**.

Nota Per utilizzare l'autenticazione Kerberos, attivarla nel servizio WinRM. Per informazioni sulla configurazione dell'autenticazione Kerberos, vedere *Utilizzo del plug-in PowerShell*.

- 10 Immettere le credenziali per la comunicazione mediante una sessione condivisa con l'host PowerShell nelle caselle di testo **Nome utente** e **Password**.
- 11 Fare clic su **Fine**.

Risultati

È stato aggiunto un host Windows PowerShell come endpoint. Gli architetti XaaS possono usare XaaS per pubblicare i workflow del plug-in PowerShell come elementi di catalogo e azioni per risorse.

Configurazione del plug-in SOAP come endpoint

È possibile aggiungere un endpoint e configurare il plug-in SOAP per definire un servizio SOAP come oggetto di inventario, ed eseguire quindi operazioni SOAP sugli oggetti definiti.

Prerequisiti

- Assicurarsi di poter accedere a un host SOAP. Il plug-in supporta SOAP versione 1.1 e 1.2, nonché WSDL 1.1 e 2.0.

- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Selezionare **SOAP** dal menu a discesa **Plug-in**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.
- 7 Fornire i dettagli dell'host SOAP.
 - a Immettere il nome dell'host nella casella di testo **Nome**.
 - b Nel menu a discesa **Fornisci contenuto WSDL (Provide WSDL content)**, specificare se il contenuto WSDL deve essere fornito come testo.

Opzione	Azione
Sì	Immettere il testo WSDL nella casella di testo Contenuto WSDL (WSDL content) .
No	Immettere il percorso corretto nella casella di testo URL WSDL (WSDL URL) .

- c (Facoltativo) Nella casella di testo **Timeout connessione in secondi (Connection timeout (in seconds))** specificare quanti secondi devono trascorrere prima che si verifichi il timeout di una connessione.
Il valore predefinito è 30 secondi.
 - d (Facoltativo) Nella casella di testo **Richiesta timeout in secondi (Request timeout (in seconds))** specificare quanti secondi devono trascorrere prima che si verifichi il timeout di un'operazione.
Il valore predefinito è 60 secondi.
- 8 (Facoltativo) Specificare le impostazioni del proxy.
 - a Per utilizzare un proxy, selezionare **Sì** nel menu a discesa **Proxy**.
 - b Immettere l'indirizzo IP del server proxy nella casella di testo **Indirizzo**.
 - c Nella casella di testo **Porta** specificare il numero della porta da utilizzare per comunicare con il server proxy.
 - 9 Fare clic su **Avanti**.

10 Selezionare il tipo di autenticazione.

Opzione	Azione
Nessuno	Non è richiesta alcuna autenticazione.
Di base	<p>Offre un metodo di autenticazione degli accessi di base. La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ul style="list-style-type: none"> a Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente. b Immettere la password per la sessione condivisa nella casella di testo Password.
Digest	<p>Offre l'autenticazione degli accessi di tipo digest con codifica. La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ul style="list-style-type: none"> a Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente. b Immettere la password per la sessione condivisa nella casella di testo Password.
NTLM	<p>Offre l'autenticazione degli accessi NT LAN Manager (NTLM) nell'ambito del framework Window Security Support Provider (SSP). La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ul style="list-style-type: none"> a Fornire le credenziali dell'utente. <ul style="list-style-type: none"> ■ Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente. ■ Immettere la password per la sessione condivisa nella casella di testo Password. b Fornire le impostazioni NTLM. <ul style="list-style-type: none"> ■ Immettere il nome di dominio nella casella di testo Dominio NTLM (NTLM domain). ■ (Facoltativo) Immettere il nome della workstation nella casella di testo Workstation NTLM (NTLM workstation).
Negoziazione	<p>Offre l'autenticazione degli accessi Kerberos. La comunicazione con l'host avviene in modalità di sessione condivisa.</p> <ul style="list-style-type: none"> a Fornire le credenziali dell'utente. <ul style="list-style-type: none"> 1 Immettere il nome utente per la sessione condivisa nella casella di testo Nome utente. 2 Immettere la password per la sessione condivisa nella casella di testo Password. b Immettere il nome SPN del servizio Kerberos nella casella di testo SPN servizio Kerberos (Kerberos service SPN).

11 Fare clic su **Fine**.**Risultati**

È stato aggiunto un servizio SOAP. Gli architetti XaaS possono usare XaaS per pubblicare i workflow del plug-in SOAP come elementi di catalogo e azioni per risorse.

Configurazione del plug-in di vCenter Server come endpoint

È possibile aggiungere un endpoint e configurare il plug-in di vCenter Server per connettersi a un'istanza vCenter Server in esecuzione e creare XaaS blueprint per la gestione di oggetti di inventario di vSphere.

Prerequisiti

- Installare e configurare vCenter Server. Vedere *Installazione e configurazione di vSphere*.
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Selezionare **vCenter Server** dal menu a discesa **Plug-in**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.
- 7 Fornire le informazioni relative all'istanza di vCenter Server.
 - a Specificare l'indirizzo IP o il nome DNS della macchina nella casella di testo **IP o nome host dell'istanza vCenter Server da aggiungere**.

Questo è l'indirizzo IP o il nome DNS della macchina su cui installare l'istanza di vCenter Server da aggiungere.
 - b Specificare la porta da utilizzare per la comunicazione con l'istanza di vCenter Server nella casella di testo **Porta dell'istanza di vCenter Server**.

La porta predefinita è 443.
 - c Specificare la posizione dell'SDK da utilizzare per la connessione all'istanza di vCenter Server nella casella di testo **Posizione dell'SDK da utilizzare per connettersi all'istanza di vCenter Server**.

Ad esempio `/sdk`.
- 8 Fare clic su **Avanti**.

9 Definire i parametri della connessione.

- a Specificare la porta HTTP dell'istanza di vCenter Server nella casella di testo **Porta HTTP dell'istanza di vCenter Server - applicabile per il plug-in di VC versione 5.5.2 o precedente.**
- b Immettere le credenziali utilizzate da vRealize Orchestrator per stabilire la connessione all'istanza di vCenter Server nelle caselle di testo **Nome dell'utente utilizzato da Orchestrator per connettersi all'istanza di vCenter Server** e **Password dell'utente utilizzato da Orchestrator per connettersi all'istanza di vCenter Server.**

L'utente selezionato deve essere valido nel sistema ed essere dotato di privilegi che consentano di gestire estensioni di vCenter Server e un set di privilegi definiti personalizzati.

10 Fare clic su **Fine**.

Risultati

L'istanza di vCenter Server come endpoint è stata aggiunta. Gli architetti di XaaS possono utilizzare XaaS per pubblicare workflow del plug-in di vCenter Server come elementi di catalogo e azioni risorsa.

Creazione di un endpoint Microsoft Azure

È possibile creare un endpoint Microsoft Azure per facilitare una connessione con credenziali tra vRealize Automation e una distribuzione di Azure.

Un endpoint stabilisce una connessione a una risorsa, in questo caso un'istanza di Azure, che è possibile usare per creare blueprint di macchine virtuali. È necessario disporre di un endpoint Azure da utilizzare come base dei blueprint per eseguire il provisioning delle macchine virtuali Azure. Se si utilizzano più sottoscrizioni per Azure, è necessario creare un endpoint per ciascun ID sottoscrizione.

In alternativa, è possibile creare una connessione Azure direttamente da vRealize Orchestrator usando il comando **Aggiungi una connessione Azure** disponibile nell'albero del workflow **Libreria > Azure > Configurazione** di vRealize Orchestrator. Per la maggior parte degli scenari, la creazione di una connessione tramite la configurazione dell'endpoint, come descritto qui, è l'opzione preferita.

Gli endpoint Azure sono supportati da vRealize Orchestrator e dalla funzionalità XaaS. È possibile creare, eliminare o modificare endpoint Azure. Se si modifica un endpoint esistente e sono stati eseguiti aggiornamenti sul portale Azure tramite la connessione aggiornata per diverse ore, possono verificarsi problemi. È necessario riavviare il servizio vRealize Orchestrator utilizzando il comando `service vco-service restart`. Se il servizio non viene riavviato potrebbero verificarsi degli errori.

Prerequisiti

- Configurare un'istanza di Microsoft Azure e ottenere una sottoscrizione valida per Microsoft Azure dalla quale sia possibile utilizzare l'ID di sottoscrizione. Per ulteriori informazioni, sulla configurazione di Azure e su come ottenere un ID di sottoscrizione, vedere [Configurazione di endpoint di Microsoft Azure](#).
- Verificare che la distribuzione di vRealize Automation disponga di almeno un tenant e un gruppo di business.
- Creare un'applicazione Active Directory come indicato in <https://azure.microsoft.com/it-it/documentation/articles/resource-group-create-service-principal-portal>
- Prendere nota delle seguenti informazioni relative ad Azure, che saranno necessarie nel corso della configurazione dell'endpoint e del blueprint.
 - ID sottoscrizione
 - ID tenant
 - nome account storage
 - nome gruppo di risorse
 - posizione
 - nome rete virtuale
 - ID applicazione client
 - chiave privata applicazione client
 - URN immagine macchina virtuale
- L'implementazione di Azure di vRealize Automation supporta un sottoinsieme delle aree geografiche supportate da Microsoft Azure. Vedere [Aree geografiche supportate da Azure](#).
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Configurazione vRO > Endpoint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Nella scheda Plug-in, fare clic sul menu a discesa **Plug-in** e selezionare **Azure**.
- 4 Fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.

7 Compilare le caselle di testo nella scheda Dettagli come opportuno per l'endpoint.

Parametro	Descrizione
Impostazioni di connessione	
Nome connessione	Nome univoco per la nuova connessione dell'endpoint. Questo nome viene visualizzato nell'interfaccia di vRealize Orchestrator per semplificare l'identificazione di una connessione particolare.
ID sottoscrizione Azure	L'identificatore per la sottoscrizione di Azure. L'ID definisce gli account di storage, le macchine virtuali e altre risorse Azure alle quali l'utente ha accesso.
Ambiente di Azure	La località geografica per la risorsa Azure distribuita. vRealize Automation supporta tutte le regioni di Azure correnti in base all'ID di sottoscrizione.
Impostazioni di Gestione risorse	
URI servizio Azure	L'URI attraverso il quale si ottiene l'accesso alla propria istanza di Azure. Il valore predefinito <code>https://management.azure.com/</code> è appropriato per molte implementazioni tipiche. Questa casella viene popolata quando si seleziona un ambiente.
ID tenant	L'ID tenant di Azure che si desidera utilizzare per l'endpoint.
ID client	L'identificatore del client di Azure che si desidera utilizzare per l'endpoint. L'identificatore viene assegnato quando si crea un'applicazione Active Directory.
Segreto client	La chiave utilizzata con un ID client di Azure. La chiave viene assegnata quando si crea un'applicazione Active Directory.
URI storage Azure	L'URI che consente di accedere alla propria istanza dello storage di Azure. Questa casella viene popolata quando si seleziona un ambiente.
Impostazioni proxy	
Host proxy	Se l'azienda utilizza un server Web proxy, immettere il nome host del server.
Porta proxy	Se l'azienda utilizza un server Web proxy, immettere il numero della porta del server.

8 (Facoltativo) Fare clic su Proprietà e aggiungere le proprietà personalizzate fornite, i gruppi di proprietà o le definizioni di proprietà personalizzate.

9 Fare clic su **Fine**.

Operazioni successive

Creare gruppi di risorse, account di storage e gruppi di sicurezza di rete in Azure. È inoltre consigliabile creare servizi di bilanciamento del carico, se appropriato per l'implementazione.

Azione	Opzioni
Creare un gruppo di risorse Azure	<ul style="list-style-type: none"> ■ Creare il gruppo di risorse utilizzando il portale Azure. Vedere la documentazione Azure per le istruzioni specifiche. ■ Utilizzare il workflow vRealize Orchestrator appropriato nel gruppo di risorse Library/Azure/Resource/Create. ■ In vRealize Automation, creare e pubblicare un blueprint XaaS che contenga il workflow di vRealize Orchestrator. È possibile richiedere il gruppo di risorse dopo averlo allegato al servizio e ai permessi. <p>Nota Il tipo di risorsa Gruppo di risorse non è supportato né gestito da vRealize Automation.</p>
Creare un account di storage Azure	<ul style="list-style-type: none"> ■ Usare Azure per creare un account di storage. Vedere la documentazione Azure per le istruzioni specifiche. ■ Utilizzare il workflow vRealize Orchestrator appropriato nell'account di storage Library/Azure/Storage/Create. ■ In vRealize Automation, creare e pubblicare un blueprint XaaS che contenga il workflow di vRealize Orchestrator. È possibile richiedere l'account di storage dopo averlo allegato al servizio e ai permessi.
Creare un gruppo di sicurezza di rete Azure	<ul style="list-style-type: none"> ■ Utilizzare Azure per creare un gruppo di sicurezza. Vedere la documentazione Azure per le istruzioni specifiche. ■ Utilizzare il workflow vRealize Orchestrator appropriato nel gruppo di sicurezza di rete Library/Azure/Network/Create . ■ In vRealize Automation, creare e pubblicare un blueprint XaaS che contenga il workflow di vRealize Orchestrator. È possibile richiedere il gruppo di sicurezza dopo averlo allegato al servizio e ai permessi.

Aree geografiche supportate da Azure

L'implementazione di Azure di vRealize Automation supporta un sottoinsieme delle aree geografiche supportate da Microsoft Azure.

L'implementazione di Azure all'interno di vRealize Automation supporta le seguenti aree geografiche di Azure.

■ Asia orientale	■ Australia orientale
■ Asia sud-orientale	■ Australia sud-orientale
■ Stati Uniti centrali	■ India meridionale
■ Stati Uniti orientali	■ India centrale
■ Stati Uniti orientali 2	■ India occidentale
■ Stati Uniti occidentali	■ Canada centrale
■ Stati Uniti occidentali 2	■ Canada orientale
■ Stati Uniti centro-settentrionali	■ Stati Uniti centro-occidentali
■ Stati Uniti centro-meridionali	■ Corea centrale
■ Europa settentrionale	■ Corea meridionale
■ Europa occidentale	■ Regno Unito occidentale
■ Giappone occidentale	■ Regno Unito meridionale
■ Giappone orientale	■ Cina orientale
■ Brasile meridionale	■ Cina settentrionale

Creazione e configurazione di contenitori

È possibile utilizzare la scheda Contenitori in vRealize Automation per aprire l'applicazione integrata Contenitori per vRealize Automation che consente di creare e configurare i contenitori e le impostazioni della rete di contenitori da rendere disponibili agli architetti di blueprint di vRealize Automation.

I contenitori possono essere definiti nell'applicazione integrata Contenitori utilizzando immagini e modelli e nuovi o esistenti. È quindi possibile aggiungere ai blueprint di vRealize Automation i componenti dei contenitori e le impostazioni di rete associate.

Gestione di host contenitori e cluster

È possibile visualizzare e gestire gli host aggiunti dalla pagina Cluster. Nel contesto della funzionalità Contenitori, l'host è un'infrastruttura o una macchina virtuale che consente di eseguire i contenitori.

La pagina Cluster, nella scheda Infrastruttura, contiene i controlli per l'aggiunta di nuovi cluster e host. Per aggiungere un host nell'ambiente Contenitori, è necessario aggiungerlo a un cluster. È possibile monitorare lo stato delle richieste di provisioning degli host esistenti e visualizzare i registri eventi per i contenitori da qualsiasi pagina nelle schede Libreria e Distribuzioni. I pannelli Richieste e Registro eventi si trovano sul lato destro delle pagine.

Creare un cluster di host contenitore

È necessario aggiungere un host a un cluster per distribuire i contenitori.

Prerequisiti

Selezionare un gruppo di business nel lato superiore sinistro della scheda Contenitori.

Procedura

- 1 Accedere alla console di vRealize Automation come **amministratore dei contenitori**.
- 2 Fare clic sulla scheda **Contenitori**.

- 3 Fare clic su **infrastruttura > Cluster di host contenitore**.
- 4 Fare clic su **Cluster**.
- 5 Immettere un nome e una descrizione per il cluster.
- 6 Selezionare l'host del contenitore virtuale Docker (VCH) nel menu a discesa **Tipo**.
- 7 Immettere il nome o l'indirizzo IP dell'host utilizzando il formato URL **http(s)://<nomehost>:<porta>**.
- 8 Selezionare le credenziali di accesso dall'elenco.

La funzionalità Contenitori supporta l'autenticazione tramite credenziali e tramite chiave pubblica-privata. È possibile aggiungere le proprie credenziali dalla pagina **Gestione identità**.

- 9 Fare clic su **Salva**.

Risultati

È stato creato un cluster di host contenitore.

Utilizzo dei criteri di distribuzione dei contenitori

È possibile collegare i criteri di distribuzione a host e definizioni di contenitori. È possibile utilizzare i criteri di distribuzione in Contenitori per vRealize Automation per impostare una preferenza per l'host e le quote specifici quando si distribuisce un contenitore.

I criteri di distribuzione applicati a un contenitore hanno una priorità più alta dei posizionamenti applicati agli host di contenitori.

Nota I criteri di distribuzione sono obsoleti e verranno rimossi in una versione futura di vRealize Automation.

Impostazione di un criterio di distribuzione su un host

Imposta una preferenza per l'host e le quote specifici quando si distribuisce un contenitore.

Nota I criteri di distribuzione sono obsoleti e verranno rimossi in una versione futura di vRealize Automation.

Prerequisiti

Aggiungere un host a un cluster.

Procedura

- 1 Accedere alla console di vRealize Automation come **amministratore dei contenitori**.
- 2 Fare clic sulla scheda **Contenitori**.
- 3 Selezionare **infrastruttura > Cluster di host contenitore**.
- 4 Fare clic sul cluster che contiene l'host che si desidera modificare.
- 5 Fare clic su **Risorse**.

- 6 Fare clic sull'icona delle opzioni nell'host che si desidera configurare e fare clic su **Modifica**.
- 7 Selezionare il criterio di distribuzione e fare clic su **Aggiorna**.

Impostazione di un criterio di distribuzione per la definizione di un contenitore

Impostare un criterio di distribuzione per la definizione di un contenitore.

Nota I criteri di distribuzione sono obsoleti e verranno rimossi in una versione futura di vRealize Automation.

Procedura

- 1 Fare clic sulla scheda **Contenitori**.
- 2 Fare clic su **Hot cluster del container** per avviare il provisioning del container.
- 3 Selezionare un container esistente dall'elenco.
- 4 Nelle opzioni di provisioning, fare clic su **Criterio**.
- 5 Dall'elenco a discesa **Criterio di distribuzione**, selezionare un criterio esistente.
- 6 Eseguire il provisioning del contenitore o salvarlo come modello.

Configurazione delle impostazioni del contenitore

È possibile definire un'applicazione con uno o più contenitori utilizzando le impostazioni e le proprietà di una configurazione di contenitori nuova o esistente.

Oltre alle impostazioni di base di Contenitori per vRealize Automation, sono disponibili anche le seguenti impostazioni di vRealize Automation per le distribuzioni che utilizzano componenti contenitore:

- Configurazione dei controlli di stato
- Collegamenti
- Servizi esposti
- Parametri per dimensioni dei cluster e scalabilità orizzontale e verticale

Configurazione dei controlli di stato in Contenitori

È possibile configurare il metodo dei controlli di stato per aggiornare lo stato di un contenitore in base a dei criteri specifici.

Quando si esegue un comando sul contenitore, è possibile utilizzare il protocollo HTTP o TCP. È inoltre possibile specificare il metodo per il controllo di stato.

Prerequisiti

- Verificare che l'opzione Contenitori per vRealize Automation sia abilitata nella distribuzione di vRealize Automation supportata.
- Verificare di disporre dei privilegi per i ruoli di **amministratore dei contenitori** o **architetto dei contenitori**.

Procedura

- 1 Accedere a vRealize Automation.
- 2 Fare clic sulla scheda **Contenitori**.
- 3 Selezionare **Libreria > Modelli** nel riquadro a sinistra.
- 4 Modificare il modello o l'immagine.

Opzione	Descrizione
Per modificare un modello	<ol style="list-style-type: none"> a Fare clic su Modifica nella sezione in alto a destra del modello che si desidera aprire. b Fare clic su Modifica nella sezione in alto a destra del contenitore che si desidera aprire.
Per modificare un'immagine.	Fare clic sulla freccia accanto al pulsante Provisioning relativo all'immagine, quindi su Immettere altre informazioni .

- 5 Fare clic sulla scheda relativa alla **configurazione dei controlli**.
- 6 Selezionare una modalità di controllo.

Tabella 2-20. Modalità di configurazione dei controlli di stato

Modalità	Descrizione
Nessuno	Valore predefinito. Non sono stati configurati controlli di stato.
HTTP	<p>Se si seleziona HTTP, è necessario specificare un'API a cui accedere nonché un metodo e una versione HTTP da utilizzare. L'API è relativa. Non è necessario inserire l'indirizzo del contenitore. È inoltre possibile specificare un periodo di timeout per il funzionamento e impostare una soglia di integrità.</p> <p>Ad esempio, una soglia di integrità pari a 2 indica che, affinché il contenitore venga considerato integro, devono essere portate a termine correttamente due chiamate consecutive con stato RUNNING. Ad esempio, una soglia di non integrità pari a 2 indica che, affinché il contenitore venga considerato non integro, non devono andare a buon fine due chiamate, che devono presentare lo stato ERROR. Per gli stati intermedi fra la soglia di integrità e di non integrità, lo stato del contenitore è DEGRADED.</p>
Connessione TCP	Se si seleziona Connessione TCP , sarà necessario inserire solo una porta per il contenitore. Il controllo dello stato tenta di stabilire una connessione TCP con il contenitore mediante la porta specificata. È inoltre possibile specificare un valore di timeout per il funzionamento e impostare una soglia di integrità o di non integrità con HTTP.

Tabella 2-20. Modalità di configurazione dei controlli di stato (continua)

Modalità	Descrizione
Comando	Se si seleziona Comando , è necessario inserire un comando da eseguire sul contenitore. L'esito del controllo di stato è determinato dall'esito del comando.
Ignora controllo di integrità durante il provisioning	Deselezionare questa opzione per forzare il controllo dell'integrità durante il provisioning. Quando si forza il controllo dell'integrità, il provisioning del contenitore non viene considerato completato finché non viene eseguito un controllo dell'integrità con esito positivo.
Distribuisci automaticamente	Ridistribuzione automatica di contenitori quando si trovano nello stato ERRORE.

7 Fare clic su **Salva**.

Configurazione di collegamenti in Contenitori

I collegamenti e i servizi esposti gestiscono la comunicazione fra i servizi contenitore e il bilanciamento del carico fra gli host. In Contenitori, è possibile definire le impostazioni dei collegamenti per i contenitori.

I collegamenti consentono di comunicare tra i vari servizi dell'applicazione. I collegamenti in Contenitori sono simili ai collegamenti di Docker, ma servono per collegare i contenitori agli host. Un collegamento è composto da due parti: un nome di servizio e un alias. Il nome di servizio è il nome del servizio o del modello da richiamare. L'alias è il nome host da utilizzare per comunicare con il servizio.

Ad esempio, se un'applicazione contiene un servizio di database e Web e in quest'ultimo si definisce un collegamento al servizio di database usando un alias di **my-db**, l'applicazione del servizio Web avvia una connessione TCP a **my-db: {PORT_OF_DB}**. **PORT_OF_DB** è la porta alla quale il database fa riferimento, indipendentemente dalla porta pubblica assegnata all'host nelle impostazioni del contenitore. Se MySQL verifica la presenza di aggiornamenti nella porta predefinita 3306 e la porta per l'host del contenitore pubblicata è la 32799, l'applicazione Web accede al database in **my-db:3306**.

Nota Si consiglia di utilizzare reti al posto di collegamenti. Ora i collegamenti sono una funzione legacy di Docker. Presentano tuttavia significative limitazioni per quanto riguarda il collegamento di cluster di contenitori, fra cui quelle elencate di seguito:

- Il Docker non supporta più collegamenti con lo stesso alias. Si consiglia di consentire a Contenitori per vRealize Automation di generare alias per i collegamenti al posto dell'utente.
- Non è possibile aggiornare i collegamenti di un contenitore in runtime. Quando si scala un cluster con collegamenti in orizzontale o in verticale, i collegamenti al contenitore dipendenti non verranno aggiornati.

Prerequisiti

- Verificare che l'opzione Contenitori per vRealize Automation sia abilitata nella distribuzione di vRealize Automation supportata.
- Verificare di disporre dei privilegi per i ruoli di **amministratore dei contenitori** o **architetto dei contenitori**.
- Verificare che sia presente una rete con bridging per il collegamento dei servizi.
- Verificare che la porta interna del servizio di destinazione sia stata pubblicata. In caso di comunicazioni incrociate, il servizio può essere mappato a un'altra porta, ma dovrà essere accessibile dall'esterno dell'host.
- Verificare che gli host del servizio possano accedere reciprocamente l'uno all'altro.

Procedura

- 1 Accedere a vRealize Automation.
- 2 Fare clic sulla scheda Contenitori.
- 3 Selezionare **Libreria > Modelli** nel riquadro a sinistra.
- 4 Modificare il modello o l'immagine.

Opzione	Descrizione
Per modificare un modello	<ol style="list-style-type: none"> a Fare clic su Modifica nella sezione in alto a destra del modello che si desidera aprire. b Fare clic su Modifica nella sezione in alto a destra del contenitore che si desidera aprire.
Per modificare un'immagine.	Fare clic sulla freccia accanto al pulsante Provisioning relativo all'immagine, quindi su Immettere altre informazioni .

- 5 Fare clic sulla scheda **Di base**.
- 6 Nella casella di testo **Servizi** inserire l'elenco di servizi (separati da una virgola) da cui dipende il contenitore.
- 7 Nella casella di testo **Alias** specificare un nome descrittivo del servizio o un elenco di servizi separati da virgola.
- 8 Fare clic su **Salva**.

Configurazione dei servizi esposti in Contenitori

Per usare un nome host univoco per un bilanciamento del carico, è necessario specificare un indirizzo e un segnaposto nelle impostazioni del contenitore.

Il segnaposto stabilisce la posizione di una parte dell'URL generata automaticamente. Questo valore è univoco per ciascun nome host. L'indirizzo supporta l'inserimento del carattere %s all'interno del formato, che indica la posizione del segnaposto.

Nota Se non viene usato un segnaposto, a seconda della configurazione del sistema, verrà inserito un prefisso o un suffisso al nome host.

Se viene creata un'applicazione che include un servizio da esporre in pubblico e scalabile orizzontalmente o verticalmente, si consiglia di usare un bilanciamento del carico in grado di inviare le richieste a ogni nodo. Dopo aver eseguito il provisioning dell'applicazione, la configurazione del bilanciamento del carico viene aggiornata automaticamente ogni volta che il servizio viene scalato orizzontalmente o verticalmente da vRealize Automation.

Prerequisiti

- Verificare che l'opzione Contenitori per vRealize Automation sia abilitata nella distribuzione di vRealize Automation supportata.
- Verificare di disporre dei privilegi per i ruoli di **amministratore dei contenitori** o **architetto dei contenitori**.

Procedura

- 1 Accedere a vRealize Automation.
- 2 Fare clic sulla scheda **Contenitori**.
- 3 Selezionare **Libreria > Modelli** nel riquadro a sinistra.
- 4 Modificare il modello o l'immagine.

Opzione	Descrizione
Per modificare un modello	<ol style="list-style-type: none"> a Fare clic su Modifica nella sezione in alto a destra del modello che si desidera aprire. b Fare clic su Modifica nella sezione in alto a destra del contenitore che si desidera aprire.
Per modificare un'immagine.	Fare clic sulla freccia accanto al pulsante Provisioning relativo all'immagine, quindi su Immettere altre informazioni .

- 5 Fare clic sulla scheda **Rete**.
- 6 Inserire percorso e segnaposto nella casella di testo **Indirizzo**.

La componente host dell'indirizzo fungerà da host virtuale. Per accedere alla componente host dell'indirizzo è possibile aggiungere informazioni sulla mappatura nel file etc/hosts o usare un DNS per mappare l'indirizzo del contenitore al nome host.

- 7** Nella casella di testo relativa alla **porta del contenitore**, inserire il numero di porta utilizzato per l'esposizione del servizio.

Usare il formato di esempio fornito nel modulo. Se nell'applicazione del contenitore sono esposte più porte, specificare quali porte interne possono esporre il servizio.

- 8** Fare clic su **Salva**.

Configurazione delle dimensioni dei cluster e della scalabilità verticale Contenitori

È possibile creare cluster di contenitori usando le impostazioni di posizionamento di Contenitori per specificare le dimensioni dei cluster.

Quando si configura un cluster, Contenitori esegue il provisioning del numero di contenitori specificato. Il carico delle richieste viene bilanciato fra tutti i contenitori del cluster.

È possibile modificare le dimensioni dei cluster di un contenitore o di un'applicazione sottoposti a provisioning per aumentare o diminuire le dimensioni del cluster di uno. Se si modificano le dimensioni del cluster in runtime, verranno considerati tutti i filtri di affinità e le regole di posizionamento.

Prerequisiti

- Verificare che l'opzione Contenitori per vRealize Automation sia abilitata nella distribuzione di vRealize Automation supportata.
- Verificare di disporre dei privilegi per i ruoli di **amministratore dei contenitori** o **architetto dei contenitori**.

Procedura

- 1** Accedere a vRealize Automation.
- 2** Fare clic sulla scheda **Contenitori**.
- 3** Selezionare **Libreria > Modelli** nel riquadro a sinistra.
- 4** Modificare il modello o l'immagine.

Opzione	Descrizione
Per modificare un modello	<ol style="list-style-type: none"> a Fare clic su Modifica nella sezione in alto a destra del modello che si desidera aprire. b Fare clic su Modifica nella sezione in alto a destra del contenitore che si desidera aprire.
Per modificare un'immagine.	Fare clic sulla freccia accanto al pulsante Provisioning relativo all'immagine, quindi su Immettere altre informazioni .

- 5** Fare clic sulla scheda **Criterio**.
- 6** Specificare le dimensioni del cluster di contenitori.
- 7** Fare clic su **Salva**.

Configurazione e utilizzo di modelli e immagini in Contenitori

Contenitori utilizza modelli per eseguire il provisioning dei contenitori.

Un modello è una configurazione riutilizzabile per il provisioning di un contenitore o una serie di contenitori. In un modello, è possibile definire un'applicazione multi-tier composta da servizi collegati.

Un servizio è definito come uno o più contenitori dello stesso tipo o immagine.

È possibile creare un modello di contenitore personalizzato basato su un modello esistente nella pagina **Modelli** o importare un file YAML correttamente formattato. È inoltre possibile eseguire il provisioning di un modello o immagine di contenitore.

Creazione di un modello di contenitore personalizzato

È possibile creare modelli personalizzati da utilizzare per la definizione di contenitori

Un modello è una configurazione riutilizzabile che è possibile usare per il provisioning di un contenitore o di una suite di contenitori.

Nella pagina Modelli sono visualizzate immagini di modelli disponibili in base a registri definiti dall'utente. È possibile creare un modello personalizzato basato sull'immagine di un modello esistente oppure importare un modello o un file di Docker Compose. Vedere [Importazione di un modello Docker Container o un file Docker Compose](#).

È possibile creare modelli personalizzati o immagini anche utilizzando l'opzione **Provisioning > Immettere altre informazioni** descritta in [Provisioning di un contenitore da un modello o un'immagine](#).

Prerequisiti

- Verificare di disporre dei privilegi per i ruoli di **amministratore dei contenitori**.

Procedura

- 1 Accedere alla console di vRealize Automation come **amministratore dei contenitori**.
- 2 Fare clic sulla scheda **Contenitori**.
- 3 Selezionare **Libreria > Modelli** nel riquadro a sinistra.

Viene visualizzato l'elenco dei modelli e delle immagini disponibili per il provisioning.

- Modelli configurati nella visualizzazione Immagini.
- Modelli personalizzati o esistenti nella visualizzazione **Modelli**.
- Tutti i modelli e le immagini disponibili basati sui registri specificati nella visualizzazione **Tutto**.

Le opzioni di **importazione** ed **esportazione** consentono di importare anche modelli e immagini.

- 4 Fare clic sulla freccia accanto al pulsante **Provisioning** di un'immagine che si desidera includere nel modello.

5 Fare clic su **Immettere ulteriori informazioni**

- 6 Fare clic su **Salva come modello** per salvare le modifiche come nuovo modello di contenitore in Contenitori per vRealize Automation.

Operazioni successive

È possibile modificare un modello da utilizzare in futuro per il provisioning. Le applicazioni esistenti di cui è stato eseguito il provisioning a partire dal modello non verranno interessate dalle modifiche apportate dopo il provisioning.

Importazione di un modello Docker Container o un file Docker Compose

È possibile utilizzare un modello Docker Container importato o un file YAML Docker Compose come modello personalizzato in Contenitori per vRealize Automation

Se si utilizza un file YAML, inserire il contenuto di tale file come testo oppure selezionare e caricare il file YAML. Il file YAML rappresenta il modello, la configurazione dei diversi contenitori e le relative connessioni. I tipi di formati supportati sono YAML Docker Compose e YAML di Contenitori per vRealize Automation

Il formato YAML di Contenitori per vRealize Automation è simile a Docker Compose, tuttavia utilizza il formato YAML del blueprint di vRealize Automation visibile nell'API REST di vRealize Automation o in vRealize CloudClient. Il formato YAML di Contenitori per vRealize Automation consente di importare le applicazioni Docker Compose esistenti e modificarle, eseguirne il provisioning e gestirle tramite Contenitori.

Prerequisiti

- Verificare che l'opzione Contenitori per vRealize Automation sia abilitata nella distribuzione di vRealize Automation supportata.
- Accedere a vRealize Automation come **amministratore dei contenitori**.

Per maggiori informazioni sul formato YAML utilizzato dalle REST API del servizio vRealize Automation, vedere *Riferimento API di vRealize Automation*.

Procedura

- 1 Fare clic sulla scheda **Contenitori**.
- 2 Selezionare **Libreria > Modelli** nel riquadro a sinistra.

Viene visualizzato l'elenco dei modelli e delle immagini disponibili per il provisioning.

- Modelli configurati nella visualizzazione Immagini.
- Modelli personalizzati o esistenti nella visualizzazione **Modelli**.
- Tutti i modelli e le immagini disponibili basati sui registri specificati nella visualizzazione **Tutto**.

Le opzioni di **importazione** ed **esportazione** consentono di importare anche modelli e immagini.

3 Fare clic sull'icona per l'**importazione del modello o relativa a Compose di Docker**.

Viene visualizzata la pagina relativa all'importazione del modello.

4 Specificare il contenuto del file YAML.

Opzione	Descrizione
Carica da file	Fare clic su Carica da file per cercare e selezionare il file YAML da una directory.
Inserire il modello o Docker Compose	Incollare il contenuto di un file YAML correttamente formattato nella casella di testo Inserire il modello o Docker Compose .

5 Fare clic su **Importa**.

Il nuovo modello comparirà nella visualizzazione **Modelli**.

Provisioning di un contenitore da un modello o un'immagine

È possibile eseguire il provisioning di un contenitore da un modello o un'immagine nella vista **Modelli**.

Il processo di provisioning crea un contenitore in base alle impostazioni di configurazione presenti nel modello o nell'immagine da cui si esegue il provisioning.

È possibile eseguire il provisioning di un contenitore da un modello o un'immagine utilizzando le impostazioni di configurazione esistenti o modificando le impostazioni di configurazione e quindi eseguendo il provisioning.

È inoltre possibile modificare e salvare le impostazioni di configurazione per creare il modello o l'immagine di un nuovo contenitore personalizzato.

Prerequisiti

- Verificare che l'opzione Contenitori per vRealize Automation sia abilitata nella distribuzione di vRealize Automation supportata.
- Accedere a vRealize Automation come **amministratore dei contenitori**.

Procedura

1 Fare clic sulla scheda **Contenitori**.

2 Selezionare **Libreria > Modelli** nel riquadro a sinistra.

Viene visualizzato l'elenco dei modelli e delle immagini disponibili per il provisioning.

- Modelli configurati nella visualizzazione Immagini.
- Modelli personalizzati o esistenti nella visualizzazione **Modelli**.
- Tutti i modelli e le immagini disponibili basati sui registri specificati nella visualizzazione **Tutto**.

Le opzioni di **importazione** ed **esportazione** consentono di importare anche modelli e immagini.

- 3 Utilizzare le opzioni della vista **Tutto, Immagini o Modelli** per visualizzare l'immagine o il modello di cui eseguire il provisioning.
- 4 Provisioning del modello o dell'immagine

Opzione	Descrizione
Eseguire il provisioning utilizzando le impostazioni esistenti.	<p>a Fare clic su Provisioning.</p> <p>La vista Richieste di provisioning mostra le informazioni sulla buona riuscita del processo di provisioning.</p>
Eseguire il provisioning modificando le impostazioni.	<p>a Fare clic sulla freccia accanto al pulsante Provisioning.</p> <p>b Fare clic su Immettere ulteriori informazioni</p> <p>c Immettere le informazioni aggiuntive per il contenitore in Provisioning del modulo di un contenitore.</p> <p>d Una volta completati gli aggiornamenti del modulo, fare clic su Provisioning per eseguire il provisioning utilizzando le impostazioni modificate.</p> <p>e Fare clic su Salva come modello per salvare le modifiche come nuovo modello di contenitore in Contenitori per vRealize Automation.</p> <p>La vista Richieste di provisioning mostra le informazioni sulla buona riuscita del processo di provisioning.</p>

Esportazione di un modello di contenitore o di un file di Docker Compose

È possibile esportare un modello di contenitore in un file YAML di Docker Compose oppure in un file YAML di Contenitori per vRealize Automation.

Un modello può essere esportato, modificato mediante un programma utilizzando l'API REST di vRealize Automation o vRealize CloudClient, oppure mediante interfaccia grafica in Contenitori. Una volta modificato, il file può essere esportato. Ad esempio, è possibile eseguire l'importazione in formato di Docker Compose e l'esportazione nel formato YAML dei blueprint utilizzato nell'API composition-service di vRealize Automation. Tuttavia, alcune configurazioni specifiche di Contenitori, ad esempio la configurazione dell'integrità e i vincoli dell'affinità, non vengono inclusi nell'esportazione se si utilizza il formato di Docker Compose.

Prerequisiti

- Verificare che l'opzione Contenitori per vRealize Automation sia abilitata nella distribuzione di vRealize Automation supportata.
- Accedere a vRealize Automation come **amministratore dei contenitori**.

Per maggiori informazioni sul formato YAML utilizzato dalle REST API del servizio vRealize Automation, vedere *Riferimento API di vRealize Automation*.

Procedura

- 1 Fare clic sulla scheda **Contenitori**.

2 Selezionare **Libreria > Modelli** nel riquadro a sinistra.

Viene visualizzato l'elenco dei modelli e delle immagini disponibili per il provisioning.

- Modelli configurati nella visualizzazione Immagini.
- Modelli personalizzati o esistenti nella visualizzazione **Modelli**.
- Tutti i modelli e le immagini disponibili basati sui registri specificati nella visualizzazione **Tutto**.

Le opzioni di **importazione** ed **esportazione** consentono di importare anche modelli e immagini.

3 Posizionare il mouse su un modello e fare clic sull'icona **Esporta** ad esso associata.

4 Quando viene richiesto, selezionare un tipo di formato di output:

■ **Blueprint YAML**

Questo formato è conforme al formato YAML dei blueprint utilizzato nella composition-service API di vRealize Automation.

■ **Docker Compose**

Questo formato è conforme al formato YAML utilizzato nell'applicazione Docker Compose.

5 Fare clic su **Esporta**.

6 Quando viene richiesto, salvare il file o aprirlo con l'applicazione appropriata.

Utilizzo dei registri di contenitori

Un registro Docker è un'applicazione lato server senza stato. È possibile utilizzare i registri in Contenitori per vRealize Automation per archiviare e distribuire immagini Docker.

Per configurare un registro, è necessario fornire il relativo registro, un nome di registro personalizzato e, facoltativamente, le credenziali. L'indirizzo deve iniziare con HTTP o HTTPS per designare se il registro è protetto o non protetto. Se non si specifica il tipo di connessione, viene utilizzato il protocollo HTTPS per impostazione predefinita.

Nota Per HTTP, è necessario dichiarare la porta 80; per HTTPS, è necessario dichiarare la porta 443. Se la porta non viene specificata, il motore Docker prevede la porta 5000, che può causare l'interruzione delle connessioni.

Nota Si consiglia di non utilizzare registri HTTP, poiché il protocollo HTTP è considerato non sicuro. Se si desidera utilizzare il protocollo HTTP, è necessario modificare la proprietà DOCKER_OPTS in ogni host nel modo seguente:

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000".
```

Per ulteriori informazioni, consultare la documentazione di Docker all'indirizzo <https://docs.docker.com/registry/insecure/>.

Contenitori può interagire sia con Docker Registry HTTP API V1 che V2 nel seguente modo:

V1 su HTTP (non protetto, registro HTTP semplice)

È possibile cercare liberamente questo tipo di registro, tuttavia è necessario configurare manualmente ciascun host di Docker con il contrassegno `--insecure-registry` per eseguire il provisioning dei contenitori in base a immagini provenienti da registri non sicuri. Dopo aver impostato la proprietà, è necessario riavviare il daemon Docker.

V1 su HTTPS

Utilizzare dietro un proxy inverso, ad esempio NGINX. L'implementazione standard è disponibile in formato open source all'indirizzo <https://github.com/docker/docker-registry>.

V2 su HTTPS

L'implementazione standard è disponibile in formato open source all'indirizzo <https://github.com/docker/distribution>.

V2 su HTTPS con autenticazione di base

L'implementazione standard è disponibile in formato open source all'indirizzo <https://github.com/docker/distribution>.

V2 su HTTPS con autenticazione tramite un servizio centrale

È possibile eseguire un registro Docker in modalità autonoma, che non prevede controlli di autorizzazione. I registri di terzi supportati sono JFrog Artifactory e Harbor. Docker Hub viene abilitato per impostazione predefinita per tutti i tenant e non è presente nell'elenco di registri, tuttavia può essere disattivato con una proprietà di sistema.

Nota In genere, Docker non interagisce con registri sicuri configurati con certificati firmati da autorità sconosciute. Il servizio di contenitori gestisce questo caso caricando automaticamente i certificati non attendibili in tutti gli host Docker e consentendo agli host di collegarsi a tali registri. Se non è possibile caricare un certificato in un determinato host, l'host viene disattivato automaticamente.

Creazione e gestione di registri dei contenitori

È possibile configurare più registri per ottenere l'accesso a immagini pubbliche che private.

I registri sono archivi pubblici o privati in cui è possibile caricare o scaricare immagini. I registri creati possono essere disattivati, modificati o eliminati. Le immagini visualizzate nella scheda **Modelli** dipendono dai registri definiti dall'utente.

Durante la creazione o la gestione di registri, è possibile fare clic sul pulsante **Credenziali** o sul pulsante **Certificato** per aggiungere o gestire credenziali e certificati.

Prerequisiti

- Accedere a vRealize Automation come **amministratore dei contenitori**.

- Verificare che risulti configurato e disponibile almeno un host per la configurazione di rete dei contenitori.

Procedura

- 1 Fare clic sulla scheda **Contenitori**.
- 2 Selezionare **Libreria > Registri globali**.
- 3 Fare clic su **Registro** per creare un nuovo registro.
- 4 Immettere l'indirizzo del registro.
- 5 Immettere il nome del registro.
- 6 Selezionare le proprie credenziali di accesso dall'elenco a discesa.
- 7 (Facoltativo) Fare clic su **Verifica** per verificare la validità dei parametri configurati.
- 8 Fare clic su **Salva** per aggiungere il registro.

Aggiunta di un'immagine ai Preferiti

È possibile accedere rapidamente alle immagini preferite o utilizzate con maggiore frequenza aggiungendole ai Preferiti.

Quando viene aggiunta ai Preferiti, un'immagine viene visualizzata nella pagina Repository senza alcuna ricerca. Solo gli amministratori dei contenitori possono aggiungere e rimuovere immagini nei Preferiti, mentre tutti gli utenti possono visualizzare le immagini preferite in base al repository. Accanto al nome delle immagini contrassegnate come preferite viene visualizzata una stella.

Procedura

- 1 Dalla pagina Repository selezionare il registro nel menu a discesa e cercare l'immagine desiderata.
- 2 Fare clic sulla freccia accanto a **Provisioning** e selezionare **Aggiungi immagine ai Preferiti**.
Viene visualizzata una notifica che indica che l'immagine è stata aggiunta ai Preferiti e accanto al nome dell'immagine viene aggiunta una stella.

Risultati

L'immagine viene visualizzata nella pagina Repository senza alcuna ricerca. Per rimuovere l'immagine dai Preferiti, nella pagina Repository fare clic sulla freccia accanto a **Provisioning** e selezionare **Rimuovi immagine dai Preferiti**.

Configurazione delle risorse di rete per i contenitori

È possibile creare, modificare e collegare configurazioni di rete a contenitori e modelli di contenitori nell'applicazione Contenitori per vRealize Automation.

Quando si esegue il provisioning di un contenitore, la configurazione di rete è incorporata e disponibile. È possibile personalizzare le impostazioni di rete dei componenti del contenitore aggiunti a un blueprint di vRealize Automation.

Creazione di una nuova rete per Containers

Se non è disponibile una configurazione di rete adatta, è possibile crearne una nuova in vRealize Automation.

Prerequisiti

- Verificare di disporre dei ruoli di **amministratore dei contenitori**, **architetto dei contenitori** o **amministratore IaaS**.
- Verificare che risulti configurato e disponibile almeno un host per la configurazione di rete dei contenitori.

Procedura

- 1 Accedere a vRealize Automation.
- 2 Fare clic sulla scheda **Contenitori**.
- 3 Selezionare **Distribuzioni > Reti** nel riquadro a sinistra.

Nel pannello principale sono visualizzate le configurazioni di rete esistenti per le quali è possibile eseguire il provisioning nell'ambito della distribuzione dei contenitori. Le configurazioni di rete includono sia quelle raccolte dagli host Docker aggiunti sia quelle create in vRealize Automation. Le icone che rappresentano le configurazioni di rete visualizzano i driver di rete e IPAM, le informazioni su subnet, gateway e intervallo IP, nonché il numero di contenitori che utilizzano la configurazione di rete e il numero di host.

- 4 Fare clic su **+Rete**.
- 5 Immettere il nome per la rete.

Una volta completata la creazione della nuova configurazione, un identificatore univoco verrà aggiunto al valore del nome.

- 6 (Facoltativo) Per aggiungere impostazioni di configurazione più dettagliate, selezionare la casella di controllo **Avanzate**.

Nel pannello Aggiungi rete vengono visualizzate ulteriori impostazioni di configurazione della rete.

7 Configurare le impostazioni avanzate di configurazione della rete.

Opzione	Descrizione
Configurazione IPAM	<p>Subnet</p> <p>Specificare indirizzi di subnet e gateway che siano univoci all'interno di questa configurazione di rete e che non si sovrappongano a quelli di altre reti nello stesso host del contenitore.</p>
Proprietà personalizzate	<p>Se si desidera, è possibile specificare proprietà personalizzate per la nuova configurazione di rete.</p> <p>containers.ipam.driver</p> <p>Riservata all'utilizzo esclusivo con i contenitori. Specifica il driver IPAM da utilizzare quando si aggiunge un componente di rete di Contenitori a un blueprint. I valori supportati dipendono dai driver installati nell'ambiente host del contenitore in cui vengono utilizzati. Ad esempio, un valore supportato potrebbe essere <code>infoblox</code> o <code>calico</code>, a seconda dei plug-in IPAM installati nell'host del contenitore.</p> <p>Al nome e al valore di questa proprietà si applica la distinzione fra maiuscole e minuscole. Il valore della proprietà non viene convalidato al momento dell'immissione. Se il driver specificato non esiste nell'host del contenitore al momento del provisioning, viene restituito un messaggio di errore e il provisioning non riesce.</p> <p>containers.network.driver</p> <p>Riservata all'utilizzo esclusivo con i contenitori. Specifica il driver di rete da utilizzare quando si aggiunge un componente di rete di Contenitori a un blueprint. I valori supportati dipendono dai driver installati nell'ambiente host del contenitore in cui vengono utilizzati. Per impostazione predefinita, i driver di rete forniti con Docker includono <code>bridge</code>, <code>overlay</code> e <code>macvlan</code>, mentre i driver di rete forniti con VCH (Virtual Container Host) includono il driver <code>bridge</code>. È possibile che siano disponibili anche driver di rete di terze parti, ad esempio <code>weave</code> e <code>calico</code>, a seconda dei plug-in di rete installati nell'host del contenitore.</p> <p>Al nome e al valore di questa proprietà si applica la distinzione fra maiuscole e minuscole. Il valore della proprietà non viene convalidato al momento dell'immissione. Se il driver specificato non esiste nell'host del contenitore al momento del provisioning, viene restituito un messaggio di errore e il provisioning non riesce.</p>

Nota Se si crea la rete senza configurare le opzioni avanzate, vRealize Automation fornirà i valori di tali impostazioni automaticamente.

8 Dal menu a discesa selezionare l'host al quale si desidera connettere la rete.

9 Fare clic su **Crea**.

Aggiunta di una rete a un modello di contenitore

È possibile aggiungere una configurazione di rete a un modello di contenitore per connettere i contenitori tra loro. Questa configurazione di rete viene implementata automaticamente per tutte

le applicazioni che utilizzano il modello. È possibile aggiungere una rete esistente oppure configurare e aggiungere una nuova rete in base alle necessità.

Prerequisiti

- Verificare la disponibilità di un modello. In caso contrario, procedere innanzitutto alla relativa creazione.
- Verificare di disporre dei ruoli di **amministratore dei contenitori**, **architetto dei contenitori** o **amministratore IaaS**.
- Verificare che risulti configurato e disponibile almeno un host per la configurazione di rete dei contenitori.

Procedura

- 1 Accedere a vRealize Automation.
- 2 Fare clic sulla scheda **Contenitori**.
- 3 Selezionare **Libreria > Modelli** nel riquadro a sinistra.
Una serie di icone mostra i modelli e le immagini disponibili per il provisioning.
- 4 (Facoltativo) Modificare la vista in modo da visualizzare solo i modelli facendo clic su **Visualizza: Modelli** nell'intestazione in alto a destra al di sopra delle icone.
- 5 Fare clic su **Modifica** nella sezione in alto a destra del modello da personalizzare.
Viene visualizzata la pagina Modifica modello con le icone dei contenitori e un'icona vuota con un segno +.
- 6 Puntare sull'icona vuota.
Viene visualizzata l'icona **Aggiungi rete**.
- 7 Fare clic sull'icona **Aggiungi rete**.
Viene visualizzato il pannello Aggiungi rete.
- 8 Aggiungere una rete esistente oppure creare e aggiungere una nuova rete.

Opzione	Descrizione
Aggiungere una rete esistente.	<ol style="list-style-type: none"> a Fare clic sulla casella di controllo Esistente. b Fare clic all'interno del campo Nome per visualizzare un elenco di reti esistenti. c Selezionare la rete che si desidera utilizzare e fare clic su Salva.
Configurare e aggiungere una nuova rete.	<ol style="list-style-type: none"> a Immettere il nome per la rete. b Per aggiungere impostazioni di configurazione più dettagliate, fare clic sulla casella di controllo Avanzate. c Fare clic su Salva.

- 9 Connettere la rete a un contenitore trascinando l'icona del connettore di rete dal contenitore a qualsiasi punto nell'icona orizzontale che rappresenta la rete.

Configurazione dei volumi per i contenitori

È possibile creare, modificare e collegare volumi a contenitori e modelli di contenitori nell'applicazione Contenitori per vRealize Automation.

Contenitori per vRealize Automation utilizza i volumi di Docker per la gestione dei dati permanenti. I volumi consentono di eseguire le seguenti attività:

- Condividere volumi tra diversi contenitori all'interno dello stesso host.
- Aggiornare i dati istantaneamente.
- Salvare i dati dei volumi dopo l'eliminazione del contenitore.

Creazione di un nuovo volume per i contenitori

Per espandere lo storage del contenitore, è necessario creare prima un volume di dati.

Prerequisiti

- Verificare di disporre dei ruoli di **amministratore dei contenitori**, **architetto dei contenitori** o **amministratore IaaS**.
- Verificare che risulti configurato e disponibile almeno un host per la configurazione del volume dei contenitori.

Procedura

- 1 Accedere a vRealize Automation.
- 2 Fare clic sulla scheda **Contenitori**.
- 3 Selezionare **Distribuzioni > Volumi** nel riquadro a sinistra.

Nel pannello principale sono visualizzate le configurazioni di volume esistenti che è possibile connettere ai contenitori distribuiti. Le configurazioni di volume includono sia quelle raccolte dagli host Docker aggiunti sia quelle create in vRealize Automation. Le istanze di volume mostrano driver, ambito e opzioni del driver.

- 4 Fare clic su **+Volume**.
- 5 Immettere il nome per il volume.

Una volta completata la creazione della configurazione, un identificatore univoco viene aggiunto al valore del nome.

- 6 Nella casella di testo **Driver**, inserire il driver del plug-in del volume che si desidera utilizzare. Se non si inserisce nulla, il valore predefinito utilizzato sarà "locale".
- 7 (Facoltativo) Per aggiungere impostazioni di configurazione più dettagliate, fare clic sulla casella di controllo **Avanzate**.

Vengono visualizzate altre impostazioni di configurazione.

8 (Facoltativo) Configurare le impostazioni di volume avanzate.

Opzione	Descrizione
Opzioni driver	Specificare le opzioni del driver da utilizzare. Le opzioni dipendono dal plug-in di volume in uso.
Proprietà personalizzate	È possibile specificare proprietà personalizzate per la nuova configurazione di volume.

9 Dal menu a discesa, selezionare l'host al quale si desidera connettere il volume.

10 Fare clic su **Crea**.

Il pannello Crea volume scompare e nella scheda Volumi viene visualizzato il volume aggiunto.

Operazioni successive[Aggiunta di un volume a un modello di contenitore](#)**Aggiunta di un volume a un modello di contenitore**

Collegare un volume a un contenitore aggiungendolo a un modello.

Prerequisiti

- Verificare la disponibilità di un modello. In caso contrario, procedere innanzitutto alla relativa creazione.
- Verificare di disporre dei ruoli di **amministratore dei contenitori**, **architetto dei contenitori** o **amministratore IaaS**.
- Verificare che risulti configurato e disponibile almeno un host per la configurazione del volume dei contenitori.

Procedura

1 Accedere a vRealize Automation.

2 Fare clic sulla scheda **Contenitori**.

3 Selezionare **Libreria > Modelli** nel riquadro a sinistra.

Una serie di icone mostra i modelli e le immagini disponibili per il provisioning.

4 (Facoltativo) Modificare la vista in modo da visualizzare solo i modelli facendo clic su **Visualizza: Modelli** nell'intestazione in alto a destra al di sopra delle icone.

5 Fare clic su **Modifica** nella sezione in alto a destra del modello da personalizzare.

Viene visualizzata la pagina di modifica del modello con le icone dei contenitori, inclusa un'icona vuota con il segno +.

6 Passare con il cursore del mouse sull'icona con il segno più per visualizzare l'icona **Aggiungi volume**.

7 Fare clic sull'icona **Aggiungi volume**.

8 Aggiungere un volume esistente oppure creare e aggiungere un nuovo volume.

Opzione	Descrizione
Aggiungere un volume esistente.	<ul style="list-style-type: none"> a Fare clic sulla casella di controllo Esistente. b Fare clic all'interno del campo Nome per visualizzare un elenco di volumi esistenti. c Selezionare il volume che si desidera utilizzare e fare clic su Salva.
Configurare e aggiungere un nuovo volume.	<ul style="list-style-type: none"> a Immettere il nome per il volume. b Nella casella di testo Driver, inserire il driver del plug-in del volume che si desidera utilizzare. Se non si utilizza un sistema di storage esterno, inserire locale. c Per aggiungere impostazioni di configurazione più dettagliate, fare clic sulla casella di controllo Avanzate. d Fare clic su Salva.

Il pannello Aggiungi volume scompare e il volume aggiunto viene visualizzato come icona orizzontale, sotto le icone dei contenitori nella pagina Modifica modello. Viene inoltre visualizzata l'icona di volume sul bordo inferiore delle icone dei contenitori.

- 9 Connettere il volume a un contenitore trascinando l'icona del connettore di volume dal contenitore a qualsiasi punto nell'icona orizzontale che rappresenta il volume.
- 10 (Facoltativo) Fare clic sul percorso del contenitore per cambiare la posizione in cui viene montato il volume.

Operazioni successive

Provisioning di un contenitore da un modello o un'immagine

Creazione e configurazione dei container PKS

Pivotal Container Service (PKS) consente alle imprese e ai fornitori di servizi di semplificare la distribuzione e le operazioni dei servizi di container basati su Kubernetes.

L'uso dei container PKS offre le seguenti funzionalità chiave:

- Disponibilità elevata
 - PKS offre la tolleranza agli errori integrata con controlli dello stato di routine e funzionalità di correzione automatica per i cluster Kubernetes.
- Servizi di rete e di sicurezza avanzati
 - PKS è profondamente integrato in NSX-T per i servizi di rete avanzati dei container, come micro-segmentazione, bilanciamento del carico e criteri di sicurezza.
- Operazioni semplificate
 - PKS consente la distribuzione dei cluster e la gestione del ciclo di vita di Kubernetes.
- Multi-tenancy
 - PKS supporta il multi-tenancy per l'isolamento dei carichi di lavoro e la privacy all'interno dell'organizzazione e del servizio cloud.

Aggiunta di un endpoint PKS

Prima di creare un contenitore PKS, è necessario aggiungere un endpoint PKS.

Il primo passaggio per creare un contenitore PKS consiste nell'aggiungere un endpoint PKS. Gli endpoint PKS consentono di collegare piani, cluster Kubernetes esistenti e gruppi di business.

Prerequisiti

- Privilegi dell'amministratore del contenitore
- Credenziali PKS
- Indirizzo UAA
- Indirizzo dell'endpoint PKS

Procedura

- 1 Passare alle credenziali utilizzando il percorso **Gestione identità > Credenziali** per creare e salvare le credenziali PKS.
- 2 Selezionare **Endpoint PKS > Crea endpoint**.
- 3 Inserire i dettagli dell'endpoint PKS e provare la connessione prima di salvare.

Se la prova non riesce, verificare che le credenziali PKS, l'indirizzo UAA e l'indirizzo dell'endpoint PKS siano corretti. Potrebbe essere necessario effettuare il ping degli indirizzi per verificare che siano attivi. Riprovare la connessione.

- 4 Fare clic su **Crea** per salvare l'endpoint PKS.

Nota Se viene visualizzata la finestra Verifica certificato, è possibile selezionare **Mostra certificato** per visualizzare i dettagli del certificato. Fare clic su **Si** per procedere e salvare l'endpoint.

Risultati

L'endpoint PKS viene salvato. Dopo averlo salvato, è possibile fare clic sull'endpoint PKS per visualizzare i cluster Kubernetes disponibili associati all'endpoint. Se il cluster non è stato registrato in vRealize Automation, nella colonna Richiesta sarà presente il valore **No**. Per registrare il cluster, è necessario [aggiungere un cluster](#). Se si desidera modificare l'endpoint, fare clic sul nome dell'endpoint PKS e modificarne i dettagli. È possibile rimuovere l'endpoint selezionandolo e facendo clic su **Rimuovi**.

Assegnazione di endpoint PKS a gruppi di business

Dopo aver creato un endpoint PKS, è possibile assegnarlo a gruppi di business specifici per garantire l'accesso.

Dopo aver creato un endpoint PKS, è possibile concedere l'accesso a gruppi di business specifici assegnando dei piani all'endpoint. Ciò consente di limitare e limitare l'accesso per determinati gruppi a funzionalità specifiche.

Nota È possibile creare piani separatamente in PKS. I piani non possono essere aggiunto o modificati in vRealize Automation.

Prerequisiti

- Privilegi dell'amministratore del contenitore
- Endpoint PKS esistente

Procedura

- 1 Aprire l'endpoint PKS e fare clic su **Pianifica assegnazioni**.
- 2 Selezionare il gruppo e il piano scelti nei rispettivi elenchi.

Nota Utilizzando i pulsanti + e -, è possibile assegnare più piani a un gruppo di business e lo stesso piano a più gruppi di business.

- 3 Fare clic su **Salva** per salvare le assegnazioni di piano.

Richiedere un nuovo cluster PKS

Se la configurazione di cluster desiderata non esiste, è possibile richiedere un nuovo cluster per un endpoint PKS esistente.

Come amministratore o sviluppatore contenitore, è possibile richiedere un nuovo cluster per l'endpoint PKS. Ogni endpoint PKS può contenere più cluster. Dopo aver creato un nuovo cluster, è possibile aggiungerlo al proprio ambiente utilizzando **Aggiungi cluster** ed eseguirne il provisioning in base alle esigenze.

Prerequisiti

- Un endpoint PKS esistente
- Privilegi dell'amministratore o dello sviluppatore contenitore

Procedura

- 1 Selezionare **Cluster PKS > Nuovo Cluster**.
- 2 Selezionare l'endpoint PKS.

Dopo aver selezionato un endpoint PKS, il piano viene compilato automaticamente in base ai piani di disponibili per il gruppo di business.

- 3 Inserire i dettagli del cluster.

Nota Anche se il numero di nodi worker è definito dal piano, è possibile modificare il numero in base alle esigenze specifiche.

4 Selezionare il tipo di connessione da stabilire con questo cluster:

- Nome host master - Si connette utilizzando il nome host del cluster, supponendo che esista un record DNS.
- IP nodo master - si connette utilizzando l'indirizzo IP del cluster.

5 Fare clic su **Crea**.

Risultati

Il nuovo cluster è stato creato e viene visualizzata la home page Cluster PKS.

Aggiunta di un cluster PKS

Dopo aver creato un endpoint PKS, è possibile registrare i cluster associati disponibili in vRealize Automation.

Dopo aver creato un endpoint PKS, è possibile registrare i cluster associati aggiungendo un cluster in vRealize Automation. Una volta registrati i cluster è possibile eseguirvi il provisioning di singole immagini.

Prerequisiti

- Privilegi dell'amministratore del contenitore
- Endpoint PKS con cluster disponibili

Procedura

- 1 Verificare che il gruppo di business a cui si sta aggiungendo il cluster sia quello corretto. Il nome del gruppo di business è elencato nel riquadro in alto a sinistra. Per passare da un gruppo di business a un altro, fare clic su **Gruppo**.
- 2 Selezionare **Cluster PKS > Aggiungi cluster**.
- 3 Selezionare l'endpoint PKS per popolare i cluster disponibili.
- 4 Selezionare il tipo di connessione da stabilire con questo cluster:
 - Nome host master - Si connette utilizzando il nome host del cluster, supponendo che esista un record DNS.
 - IP nodo master - Si connette utilizzando l'indirizzo IP del cluster.
- 5 Fare clic su **Aggiungi**.

Risultati

Il cluster viene visualizzato nella pagina dei cluster PKS.

Dettagli del cluster PKS

I dettagli di un cluster forniscono informazioni e strumenti per modificare e interagire con il cluster.

È possibile visualizzare e modificare i cluster PKS esistenti facendo clic sul nome dei cluster nella pagina **Cluster PKS**. Inoltre, i dettagli del cluster contengono strumenti interattivi che è possibile utilizzare per interagire con il cluster per configurazioni più complesse.

Nota È possibile modificare soltanto il numero di nodi worker di un cluster.

Dashboard

Lo stato del campo dashboard indica se il dashboard Kubernetes è installato. Se è installato, è possibile accedervi facendo clic su **Installato** ed effettuando l'accesso.

Nota Il dashboard deve essere configurato sul cluster per l'autenticazione di base. Senza tale autenticazione, non è possibile effettuare l'accesso.

Kubeconfig

Il collegamento kubeconfig è un file di configurazione scaricabile per il cluster. È possibile utilizzare questo file di configurazione, come sviluppatore contenitore, per connettersi al cluster Kubernetes e configurarlo all'interno della finestra del prompt della riga di comando. Ad esempio, utilizzando il comando **kubectl**.

Provisioning di immagini singole su un cluster Kubernetes

La funzionalità dei container all'interno di vRealize Automation consente di eseguire il provisioning di una singola immagine su un cluster PKS.

Dopo l'aggiunta di un cluster PKS, è possibile eseguire il provisioning di una singola immagine su di esso come combinazione di pod Kubernetes e distribuzione.

Prerequisiti

- Privilegio di sviluppatore di container
- Cluster PKS

Procedura

- 1** Passare a **Libreria > Archivi**.
- 2** Selezionare il registro desiderato dal menu a discesa.
- 3** Cercare un'immagine esistente all'interno del registro utilizzando la casella di testo degli archivi.
- 4** Fare clic su **Provisioning** nel file dell'immagine desiderata.
- 5** Immettere i dettagli del provisioning e fare clic su **Provisioning**.

Risultati

Viene eseguito il provisioning dell'immagine selezionata sul cluster Kubernetes e viene visualizzata nella finestra **Richieste** della barra laterale. Viene anche visualizzata in **Kubernetes > Distribuzioni** e **Kubernetes > Pod** a scopo di verifica.

Nota È inoltre possibile eseguire il provisioning del cluster scaricando il file kubeconfig e utilizzando il comando **kubect1**. Per ulteriori informazioni, vedere [Dettagli del cluster PKS](#).

Installazione di plug-in aggiuntivi sul server vRealize Orchestrator predefinito

È possibile installare pacchetti e plug-in aggiuntivi sul server vRealize Orchestrator predefinito utilizzando l'interfaccia di configurazione di vRealize Orchestrator.

È possibile installare plug-in aggiuntivi sul server vRealize Orchestrator predefinito e utilizzare i workflow con XaaS.

È anche possibile importare ulteriori pacchetti sul server vRealize Orchestrator predefinito per la configurazione come tipi di endpoint di provider IPAM esterni di vRealize Automation. Ad esempio, per informazioni su come ottenere, importare e configurare il pacchetto IPAM di Infoblox, consultare [Elenco di controllo per fornire il supporto del provider IPAM di terze parti](#).

I file di pacchetti (.package) e i file di installazione dei plug-in (.vmoapp o .dar) sono disponibili in VMware Solution Exchange all'indirizzo https://solutionexchange.vmware.com/store/category_groups/cloud-management. Per informazioni sui file di plug-in, consultare la documentazione relativa ai plug-in di vRealize Orchestrator all'indirizzo https://www.vmware.com/support/pubs/vco_plugins_pubs.html.

Per ulteriori informazioni sull'installazione di nuovi plug-in, vedere *Installazione e configurazione di VMware vCenter Orchestrator*.

Utilizzo dei criteri di Active Directory

I criteri di Active Directory definiscono le proprietà di un record di macchina, ad esempio, dominio, nonché l'unità organizzativa in cui il record viene creato utilizzando un blueprint vRealize Automation.

Se si applica un criterio a un gruppo di business, tutte le richieste di macchina provenienti dai membri del gruppo di business vengono aggiunte all'unità organizzativa specificata. È possibile creare criteri diversi per unità organizzative diverse, quindi applicare i criteri diversi a gruppi di business diversi.

Utilizzo di proprietà personalizzate per sovrascrivere un criterio di Active Directory

Utilizzando le proprietà personalizzate di Active Directory disponibili è possibile sovrascrivere il criterio di Active Directory, il dominio, l'unità organizzativa e altri valori in un blueprint particolare quando viene distribuito.

L'elenco delle proprietà personalizzate dell'Active Directory disponibile è incluso nella *Guida di riferimento alle proprietà personalizzate*. Il prefisso di proprietà personalizzata è `ext.policy.activedirectory`.

Oltre alle proprietà disponibili è possibile creare proprietà personalizzate. Alle proprietà personalizzate è necessario aggiungere il prefisso `ext.policy.activedirectory`. Ad esempio `ext.policy.activedirectory.domain.extension` o `ext.policy.activedirectory.yourproperty`. Le proprietà vengono passate ai propri workflow personalizzati di Active Directory di vRealize Orchestrator.

Per ulteriori informazioni sulle proprietà personalizzate, vedere *Guida di riferimento alle proprietà personalizzate*. A seconda dei valori che vengono sovrascritti, può essere necessario creare una definizione di proprietà. Ad esempio è possibile creare una definizione di proprietà che recupera i criteri Active Directory disponibili da vRealize Automation. In alternativa è possibile creare una definizione che consente all'utente richiedente di selezionare tra due o più unità organizzative alternative. Vedere *Guida di riferimento alle proprietà personalizzate*.

Creazione e applicazione di criteri di Active Directory

Si creano uno o più criteri di Active Directory in modo da poter assegnare criteri diversi a gruppi di business diversi. È possibile utilizzare i diversi criteri per aggiungere record di macchina a unità organizzative diverse in base all'appartenenza al gruppo di business.

Se necessario, è possibile sovrascrivere il criterio di Active Directory assegnato.

Procedura

1 Creazione di un criterio di Active Directory

La creazione di un criterio di Active Directory consente di definire il punto in cui i record vengono aggiunti in un'istanza di Active Directory quando gli utenti distribuiscono le macchine. È possibile assegnare un criterio a un gruppo di business per cui tutte le macchine distribuite dai membri del gruppo si traducono in un record creato nell'unità organizzativa specificata.

2 Scenario: aggiunta di una proprietà personalizzata ai blueprint per sovrascrivere un criterio di Active Directory

In qualità di architetto di blueprint per il gruppo di business di sviluppo, si dispone di un blueprint che include una macchina per l'applicazione e di un'altra per il database. Si desidera che il record della macchina del database venga aggiunto a un'unità organizzativa diversa dal criterio di Active Directory applicato.

Creazione di un criterio di Active Directory

La creazione di un criterio di Active Directory consente di definire il punto in cui i record vengono aggiunti in un'istanza di Active Directory quando gli utenti distribuiscono le macchine. È possibile assegnare un criterio a un gruppo di business per cui tutte le macchine distribuite dai membri del gruppo si traducono in un record creato nell'unità organizzativa specificata.

Si creano diversi criteri di Active Directory quando si desidera che le macchine distribuite da diversi gruppi aziendali abbiano diversi domini o vengano aggiunte a diverse istanze di Active Directory.

Prerequisiti

- Verificare di aver creato un endpoint di Active Directory. Vedere [Configurazione del plug-in di Active Directory come endpoint](#).
- Se si utilizza un server vRealize Orchestrator esterno, verificare che sia stato configurato correttamente. Vedere [Configurazione di un server vRealize Orchestrator esterno](#).
- Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Criteri Active Directory**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Configurare i dettagli relativi al criterio di Active Directory.

Opzione	Descrizione
ID	Immettere il valore permanente. Il valore non può includere alcuno spazio o carattere speciale. Non è possibile cambiare questo valore in un secondo momento. È possibile solo ricreare il criterio con un ID diverso.
Descrizione	Descrivere il criterio.
Endpoint di Active Directory	Selezionare l'endpoint di Active Directory per il quale viene creato questo criterio.
Dominio	Immettere il dominio root. Il formato è <i>mycompany.com</i> .
Unità organizzativa	Immettere il nome distinto dell'unità organizzativa per questo criterio. La gerarchia deve essere immessa come elenco separato da virgola. Ad esempio, ou=development,dc=corp,dc=domain,dc=com.

- 4 Fare clic su **OK**.

Risultati

L'endpoint di Active Directory vRealize Orchestrator viene aggiunto all'elenco. È possibile applicare il criterio in gruppi di business o utilizzare il criterio in blueprint o gruppi di business.

Operazioni successive

- Per fornire più opzioni di criteri, creare più criteri.
- Per aggiungere record ad Active Directory in base all'appartenenza al gruppo di business quando viene distribuito un blueprint, aggiungere l'adeguato criterio di Active Directory a un gruppo di business. Vedere [Creazione di un gruppo di business](#). È possibile applicare il criterio quando si crea il gruppo di business oppure in un secondo momento.

- Per sovrascrivere il criterio di Active Directory per il gruppo di business o per un blueprint particolare, aggiungere le proprietà personalizzate di Active Directory al blueprint. Vedere [Scenario: aggiunta di una proprietà personalizzata ai blueprint per sovrascrivere un criterio di Active Directory](#).

Scenario: aggiunta di una proprietà personalizzata ai blueprint per sovrascrivere un criterio di Active Directory

In qualità di architetto di blueprint per il gruppo di business di sviluppo, si dispone di un blueprint che include una macchina per l'applicazione e di un'altra per il database. Si desidera che il record della macchina del database venga aggiunto a un'unità organizzativa diversa dal criterio di Active Directory applicato.

Si dispone di un criterio esistente che viene applicato al gruppo di business di sviluppo. Il criterio aggiunge record di macchina a ou=development,dc=corp,dc=domain,dc=com. Si desidera che tutte le macchine del database vengano aggiunte a ou=databases,dc=corp,dc=domain,dc=com. In un blueprint che include un server di database, si sovrascrive l'unità organizzativa in Active Directory per aggiungere il record della macchina del database a ou=databases,dc=corp,dc=domain,dc=com.

Questo scenario si basa sui presupposti seguenti:

- Active Directory include unità organizzative per lo sviluppo e i database.
- Si dispone di un blueprint di test incluso in un servizio che è permesso.

Oltre a questo semplice esempio del modo in cui si può sovrascrivere il criterio, è possibile utilizzare proprietà personalizzate con il criterio di Active Directory per apportare altre modifiche a Active Directory quando si distribuiscono i blueprint. Vedere [Utilizzo dei criteri di Active Directory](#).

Prerequisiti

- Verificare di disporre di almeno un criterio di Active Directory. Vedere [Creazione di un criterio di Active Directory](#). Ad esempio, si crea un criterio di sviluppo che aggiunge record a ou=development,dc=corp,dc=domain,dc=com.
- Verificare di disporre di un gruppo di business a cui sia stato applicato un criterio di Active Directory. Vedere [Creazione di un gruppo di business](#). Ad esempio, il gruppo di business di sviluppo utilizza il criterio di sviluppo.

Procedura

- 1 Nel blueprint di test, selezionare la macchina del database nelle tele.
- 2 Fare clic sulla scheda **Proprietà**.
- 3 Fare clic sulla scheda **Proprietà personalizzate**.
- 4 Fare clic sull'icona **Nuovo** (+).

- 5 Aggiungere la proprietà personalizzata per cambiare l'unità organizzativa predefinita.
 - a Nella casella di testo **Nome** immettere **ext.policy.activedirectory.orgunit**.
 - b Nella casella di testo **Valore** immettere **ou=databases,dc=corp,dc=domain,dc=com**.
 - c Deselezionare **Sovrascrivibile**.
 - d Fare clic su **OK**.
- 6 Fare clic su **Fine**.

Risultati

Il blueprint di test include la proprietà personalizzata, ma gli utenti non la vedono nel modulo di richiesta.

Operazioni successive

Richiedere il blueprint di test. Verificare che il record per la macchina del database sia stato aggiunto all'unità organizzativa del database e che il record per la macchina dell'applicazione venga aggiunto all'unità organizzativa del database. Quando i risultati sono soddisfacenti, è possibile aggiungere la proprietà personalizzata ai blueprint di produzione.

Preferenze utente per notifiche e delegati

Le preferenze utente consentono di sovrascrivere le configurazioni predefinite delle notifiche dell'approvatore di sistema e delle preferenze relative alla lingua delle notifiche.

Per accedere alle preferenze dell'utente, fare clic sul proprio nome utente nell'intestazione di vRealize Automation e selezionare **Preferenze**.

Le opzioni indicate di seguito sono specifiche dell'utente connesso.

Tabella 2-21. Opzioni di Preferenze utente

Opzione	Descrizione
Assegna delegati	Consente di riassegnare le richieste di approvazione ad altri utenti. Ad esempio, se l'utente è un approvatore delle richieste del catalogo e deve andare in vacanza, delegherà tutte le notifiche di approvazione a uno o più approvatori. In seguito a questa assegnazione, le richieste vengono immediatamente inoltrate al delegato. I delegati sono attivi finché non vengono rimossi dall'elenco.
Notifiche	Questa opzione consente di modificare la lingua delle notifiche in modo che i messaggi email vengano inviati nella lingua impostata anziché in quella predefinita. Selezionare la lingua e aggiungere la sottoscrizione di notifica che supporta la preferenza della lingua.

Fornire blueprint di servizio agli utenti

3

È possibile offrire servizi su richiesta agli utenti creando elementi di catalogo e azioni e successivamente utilizzando i permessi e le approvazioni per controllare quali utenti possono richiedere detti servizi.

Questo capitolo include i seguenti argomenti:

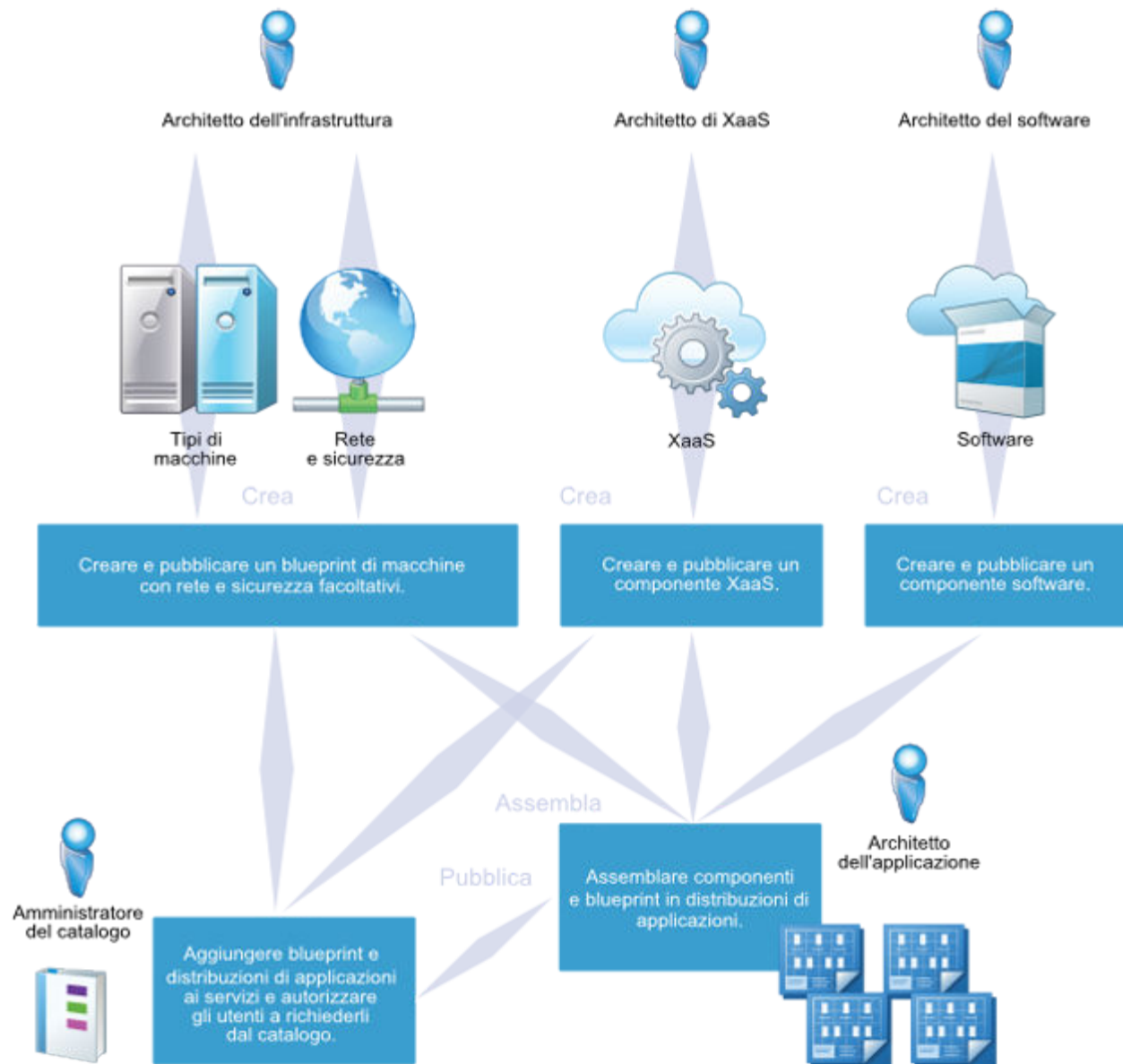
- [Progettazione dei blueprint](#)
- [Creazione di una libreria di progettazione](#)
- [Utilizzo di blueprint gestiti dagli sviluppatori](#)
- [Assemblaggio di blueprint compositi](#)
- [Personalizzazione dei moduli di richiesta di blueprint](#)
- [Richieste di provisioning non riuscite per test e risoluzione dei problemi](#)
- [Gestione del catalogo dei servizi](#)

Progettazione dei blueprint

Gli architetti dei blueprint creano componenti di Software, blueprint di macchine e blueprint di XaaS personalizzati, e quindi assemblano questi componenti nei blueprint che definiscono gli elementi che gli utenti richiedono dal catalogo. Il catalogo può visualizzare un modulo di richiesta predefinito, oppure è possibile creare un modulo personalizzato per ogni blueprint pubblicato.

È possibile creare e pubblicare blueprint per una singola macchina o un singolo blueprint di XaaS personalizzato, ma è anche possibile combinare componenti macchina e blueprint di XaaS con altri componenti costitutivi per progettare blueprint di elementi di catalogo elaborati che includono macchine multiple, rete e sicurezza, software con supporto per l'intero ciclo di vita e funzionalità di XaaS personalizzate.

A seconda dell'elemento di catalogo da definire il processo può essere piuttosto semplice, con un singolo architetto di infrastruttura che pubblica un componente macchina come blueprint, oppure più complesso e prevedere più architetti che creano molti tipi differenti di componenti per la progettazione di uno stack di applicazioni completo che gli utenti possono richiedere.



Componenti di Software

È possibile creare e pubblicare componenti software per installare software durante il processo di provisioning delle macchine e supportarne il ciclo di vita. Ad esempio, è possibile creare un blueprint che consente agli sviluppatori di richiedere una macchina con il loro ambiente di sviluppo già installato e configurato. I componenti software non sono elementi di catalogo veri e propri, ed è necessario combinarli con un componente macchina per creare un blueprint di elementi di catalogo. Vedere [Progettazioni di componenti Software](#).

Blueprint delle macchine

È possibile creare e pubblicare blueprint semplici per eseguire il provisioning di singole macchine oppure creare blueprint più complessi che contengono componenti di macchine aggiuntivi e, facoltativamente, una qualsiasi combinazione dei seguenti tipi di componente:

- Componenti di Software
- Blueprint esistenti
- Componenti rete NSX e sicurezza
- Componenti di XaaS
- Componenti di Contenitori
- Componenti personalizzati o altri componenti

Vedere [Progettazione dei blueprint delle macchine](#).

Blueprint di XaaS

È possibile pubblicare i workflow di vRealize Orchestrator come blueprint di XaaS. Ad esempio, è possibile creare una risorsa personalizzata per gli utenti di Active Directory e progettare un blueprint di XaaS per consentire ai manager di eseguire il provisioning di nuovi utenti nel rispettivo gruppo di Active Directory. È possibile creare e gestire componenti di XaaS all'esterno della scheda di progettazione. I blueprint di XaaS pubblicati si possono riutilizzare per creare blueprint di applicazioni, ma solo in combinazione con almeno un componente macchina. Vedere [Progettazione di blueprint e azioni risorsa di XaaS](#).

Blueprint di applicazione con componenti di più macchine, XaaS e Software.

È possibile aggiungere un numero qualsiasi di componenti macchina, componenti di Software e blueprint di XaaS a un blueprint di macchina per offrire agli utenti funzionalità complesse e articolate.

Ad esempio, è possibile creare un blueprint che consenta ai manager di eseguire il provisioning della configurazione di una nuova assunzione. È possibile combinare componenti di più macchine, componenti software e un blueprint di XaaS per il provisioning di nuovi utenti di Active Directory. Il manager QE può richiedere l'elemento di catalogo Nuova assunzione e il nuovo tecnico della qualità verrà inserito in Active Directory e dotato di due macchine virtuali funzionanti, una Windows e una Linux, ognuna delle quali con tutto il software richiesto per i casi di test in questi ambienti.

Creazione di una libreria di progettazione

È possibile creare una libreria di componenti per blueprint che potranno essere riutilizzati dagli architetti per assemblare i blueprint di applicazioni per la distribuzione di servizi on-demand articolati per gli utenti.

Creare una libreria composta dei componenti di base per la progettazione di blueprint: blueprint per singole macchine, componenti Software e blueprint XaaS. Quindi combinare i componenti di base secondo le esigenze per creare elementi di catalogo complessi, con cui fornire agli utenti livelli di funzionalità incrementali.

Nota: sono disponibili blueprint di esempio in VMware Solution Exchange agli indirizzi <https://solutionexchange.vmware.com> e <https://code.vmware.com>.

Tabella 3-1. Creazione di una libreria di progettazione

Elemento del catalogo	Ruolo	Componenti	Descrizione	Dettagli
Macchine	Architetto dell'infrastruttura	Creare blueprint di macchine dalla scheda Blueprint .	<p>È possibile creare blueprint di macchine per erogare rapidamente agli utenti macchine cloud virtuali, private e pubbliche, o ibride.</p> <p>Gli amministratori del catalogo possono includere i blueprint delle macchine pubblicati nel catalogo come blueprint autonomi. Inoltre, è possibile combinare i blueprint delle macchine con altri componenti per creare elementi di catalogo più articolati che includano più blueprint di macchine, Software o blueprint di XaaS.</p>	Configurazione del blueprint di una macchina
Rete e sicurezza di NSX su macchine	Architetto dell'infrastruttura	Aggiungere componenti di rete e sicurezza di NSX ai blueprint delle macchine vSphere dalla scheda Blueprint .	<p>È possibile configurare componenti rete e sicurezza, come i profili di rete e i gruppi di sicurezza, per consentire alle macchine virtuali di comunicare tra loro su reti fisiche e virtuali in maniera sicura ed efficiente.</p> <p>Prima che gli amministratori del catalogo li possano includere nel catalogo, è necessario combinare componenti di rete e sicurezza ad almeno un componente macchina vSphere. È possibile applicare componenti rete e sicurezza di NSX solo a blueprint di macchine vSphere.</p>	Progettazione di blueprint con impostazioni NSX

Tabella 3-1. Creazione di una libreria di progettazione (continua)

Elemento del catalogo	Ruolo	Componenti	Descrizione	Dettagli
Software su macchine	Architetto del software Per aggiungere correttamente componenti software alla tela di progettazione, è inoltre necessario poter accedere al catalogo target con ruolo di membro del gruppo di business, amministratore del gruppo di business o amministratore tenant.	Creare e pubblicare componenti Software dalla scheda Software , quindi combinarli con i blueprint delle macchine nella scheda Blueprint .	Aggiungere componenti Software ai blueprint delle macchine per standardizzare, distribuire, configurare, aggiornare e scalare applicazioni complesse in ambienti cloud. Queste applicazioni vanno dalle semplici applicazioni Web alle applicazioni personalizzate complesse, fino ai pacchetti di applicazioni. I componenti Software non possono apparire nel catalogo in forma autonoma. È necessario creare e pubblicare innanzitutto i componenti Software, quindi assemblare un blueprint di applicazioni che contenga almeno una macchina.	Creazione di un componente Software

Tabella 3-1. Creazione di una libreria di progettazione (continua)

Elemento del catalogo	Ruolo	Componenti	Descrizione	Dettagli
Servizi IT personalizzati	Architetti di XaaS	Creare e pubblicare blueprint di XaaS dalla scheda XaaS .	È possibile creare elementi di catalogo XaaS che estendono le funzionalità di vRealize Automation oltre il provisioning di macchine, rete, sicurezza e software. Utilizzando i workflow e i plug-in di vRealize Orchestrator esistenti, o gli script personalizzati sviluppati in vRealize Orchestrator, è possibile automatizzare l'offerta di qualsiasi servizio IT. Gli amministratori del catalogo possono includere i blueprint di XaaS pubblicati nel catalogo come blueprint autonomi, ma i blueprint pubblicati possono essere anche combinati con altri componenti nella scheda Blueprint per creare elementi di catalogo più elaborati.	Progettazione di blueprint e azioni risorsa di XaaS
Assemblare i componenti costitutivi dei blueprint pubblicati in nuovi elementi di catalogo	<ul style="list-style-type: none"> Architetto dell'applicazione Architetto dell'infrastruttura Architetto del software 	Combinare altri blueprint di macchine, blueprint XaaS e componenti Software con almeno un componente o blueprint di macchina nella scheda Blueprint .	I componenti e blueprint pubblicati possono essere riutilizzati, combinandoli per creare nuovi pacchetti di servizi IT con cui offrire agli utenti funzionalità articolate.	Assemblaggio di blueprint compositi

Progettazione dei blueprint delle macchine

I blueprint delle macchine descrivono completamente le specifiche una macchina. Essi definiscono gli attributi di una macchina, il modo in cui ne viene eseguito il provisioning e le sue impostazioni di criteri e gestione. In base alla complessità dell'elemento di catalogo che si sta creando, è possibile combinare uno o più componenti macchina nel blueprint insieme con altri componenti nella tela di progettazione e creare così elementi di catalogo più elaborati, che includono rete e sicurezza, componenti Software, componenti XaaS e altri componenti blueprint.

Storage con ottimizzazione dello spazio per il provisioning virtuale

La tecnologia di storage con ottimizzazione dello spazio elimina le inefficienze dei metodi di storage tradizionali grazie alla capacità di utilizzare solo lo storage effettivamente richiesto per le operazioni di una macchina, che quasi sempre è solo una frazione dello storage allocato per le macchine. vRealize Automation supporta due metodi di provisioning con tecnologia con ottimizzazione dello spazio, ovvero thin provisioning e provisioning FlexClone.

Quando si utilizza lo storage standard, tutto lo storage allocato a una macchina con provisioning eseguito è totalmente destinato a quella macchina, anche quando è spenta. Ciò implica uno spreco significativo di risorse di storage perché sono poche le macchine virtuali che effettivamente utilizzano tutto lo storage a loro allocato, proprio come sono poche le macchine fisiche che lavorano con un disco pieno al 100%. Quando si utilizza la tecnologia di storage con ottimizzazione dello spazio, lo storage allocato e lo storage utilizzato vengono tenuti sotto controllo separatamente e solo lo storage utilizzato viene dedicato completamente alla macchina con provisioning eseguito.

Thin provisioning

Il thin provisioning è supportato per tutti i metodi di provisioning virtuale. In base a piattaforma di virtualizzazione, tipo di storage e configurazione di storage predefinita, il thin provisioning potrebbe essere sempre utilizzato nel provisioning delle macchine. Ad esempio, nelle integrazioni di vSphere ESX Server che utilizzano storage NFS viene utilizzato sempre il thin provisioning. Tuttavia, nelle integrazioni di vSphere ESX Server che utilizzano storage locale o iSCSI, il thin provisioning è utilizzato per eseguire il provisioning di macchine solo se nel blueprint è specificata la proprietà personalizzata `VirtualMachine.Admin.ThinProvision`. Per ulteriori informazioni sul thin provisioning, consultare la documentazione fornita a corredo con la piattaforma di virtualizzazione.

Provisioning Net App FlexClone

È possibile creare un blueprint per il provisioning NetApp FlexClone se si opera in un ambiente vSphere che utilizza lo storage Network File System (NFS) e la tecnologia FlexClone.

Per poter eseguire il provisioning delle macchine, è necessario utilizzare solo storage NFS. È possibile specificare un percorso di storage FlexClone per altri tipi di provisioning della macchina, ma il percorso di storage FlexClone si comporta come uno storage standard.

L'elenco che segue è un riepilogo dettagliato della sequenza di passaggi necessari per eseguire il provisioning di macchine che utilizzano la tecnologia FlexClone:

- 1 Un amministratore IaaS crea un endpoint NetApp ONTAP. Vedere [Riferimenti delle impostazioni degli endpoint](#).
- 2 Un amministratore IaaS esegue la raccolta dati sull'endpoint per abilitare la visibilità dell'endpoint nelle pagine della risorsa di elaborazione e della prenotazione.

Se esiste un endpoint NetApp ONTAP e se l'host è virtuale, nella colonna dell'endpoint di una pagina di prenotazione è presente l'opzione FlexClone. Se è presente un endpoint NetApp ONTAP, nella pagina della prenotazione viene visualizzato l'endpoint assegnato al percorso di storage.
- 3 Un amministratore di struttura crea una prenotazione di vSphere, abilita lo storage FlexClone e specifica un percorso di storage NFS che utilizza la tecnologia FlexClone. Vedere [Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer](#).
- 4 Un architetto dell'infrastruttura o un altro utente autorizzato crea un blueprint per il provisioning FlexClone.

Aspetti da conoscere e utilizzo della parametrizzazione dei blueprint

È possibile utilizzare i profili componente per parametrizzare i blueprint. Invece di creare blueprint separati per macchine di dimensioni piccole, medie e grandi per un particolare tipo di distribuzione, è possibile creare un unico blueprint che permette di scegliere macchine virtuali di dimensioni piccole, medie o grandi. Gli utenti possono scegliere una di queste dimensioni quando distribuiscono l'elemento del catalogo.

I profili componente minimizzano l'espansione dei blueprint e semplificano le offerte del catalogo. È possibile utilizzare i profili componente per definire componenti macchina vSphere in un blueprint. I tipi di profili componente disponibili sono **Size** e **Image**. Quando si aggiungono profili componente a un componente macchina, le impostazioni del profilo componente sovrascrivono le altre impostazioni del componente macchina, come ad esempio il numero di CPU o la quantità di storage.

I profili componente sono disponibili solo per componenti macchina vSphere.

Per informazioni sulla definizione dei set di valori per i profili componente **Size** e **Image**, vedere in *Guida di riferimento alle proprietà personalizzate*.

Per informazioni sull'aggiunta di profili componente e set di valori selezionati per un componente macchina vSphere in un blueprint, vedere [vSphereImpostazioni dei componenti macchina in vRealize Automation](#).

Per informazioni sull'aggiunta di informazioni di profilo del componente mediante le impostazioni importate da un OVF, vedere [Configurazione di un blueprint per il provisioning da un OVF](#).

Per informazioni sull'uso dei profili componente quando si richiede il provisioning di una macchina, vedere [Richiesta di provisioning di una macchina mediante un blueprint con parametri](#).

È possibile creare criteri di approvazione per richiedere l'approvazione preventiva durante la richiesta di provisioning delle macchine di blueprint in relazione a condizioni dei set di valori per il profilo componente **Size** e **Image**. Per ulteriori informazioni, vedere [Esempi di criteri di approvazione basati sul tipo di criterio macchina virtuale](#).

Nota

Per informazioni sull'uso della parametrizzazione dei blueprint quando si richiede il provisioning di una macchina, vedere [Richiesta di provisioning di una macchina mediante un blueprint con parametri](#).

Configurazione del blueprint di una macchina

Configurando e pubblicando un componente macchina come blueprint autonomo, questo potrà essere riutilizzato da altri architetti come componente in blueprint applicazione e dagli amministratori di catalogo per essere incluso nei servizi dei cataloghi.

Questa procedura offre una panoramica semplice del processo di creazione del blueprint. Per ulteriori dettagli, vedere quanto segue:

- [Progettazione di blueprint con impostazioni NSX](#)

- [Aspetti da conoscere e utilizzo della parametrizzazione dei blueprint](#)
- [Impostazioni delle proprietà dei blueprint](#)
- [Configurazione di un blueprint per il provisioning da un OVF](#)
- [Esportazione e importazione di blueprint e contenuti](#)
- [Creazione di blueprint di Microsoft Azure e incorporazione di azioni risorse](#)
- [Aggiunta di funzionalità di gestione della configurazione ai blueprint vSphere](#)

Prerequisiti

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Completare le preparazioni esterne per il provisioning, come la creazione di modelli, WinPE e ISO o ottenere dagli amministratori le informazioni sulle preparazioni esterne.
- Configurare il tenant. Vedere [Configurazione delle impostazioni del tenant](#).
- Configurare le risorse IaaS. Vedere [Elenco di controllo per la configurazione di risorse di IaaS](#).
- Vedere *Configurazione di vRealize Automation*.

Procedura

- 1 Scegliere **Progettazione > Blueprint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Attenersi alle istruzioni presentate nella finestra di dialogo **Nuovo blueprint** per configurare le impostazioni generali.
- 4 Fare clic su **OK**.
- 5 Fare clic su **Tipi di macchine** nell'area Categorie per visualizzare l'elenco dei tipi di macchine disponibili.
- 6 Trascinare il tipo di macchina di cui si desidera eseguire il provisioning sulla tela di progettazione.
- 7 Immettere le informazioni in ciascuna delle schede per configurare i dettagli del provisioning delle macchine come descritto in [Impostazioni delle proprietà dei blueprint](#).
- 8 Fare clic su **Fine**.
- 9 Selezionare il blueprint e fare clic su **Pubblica**.

Risultati

Il componente macchina è stato configurato e pubblicato come blueprint autonomo. Gli amministratori di catalogo possono includere questo blueprint di macchina nei servizi dei cataloghi e autorizzare gli utenti a richiedere il blueprint. Altri architetti possono riutilizzare questo blueprint di macchina per creare blueprint di applicazione più complessi che includono componenti Software, blueprint XaaS o blueprint di macchina aggiuntivi.

Operazioni successive

È possibile combinare un blueprint di macchina con componenti Software, blueprint XaaS o blueprint di macchina aggiuntivi per creare blueprint di applicazione più complessi. Vedere [Assemblaggio di blueprint compositi](#) e [Informazioni sul comportamento dei blueprint nidificati](#).

Impostazioni dei blueprint macchina

È possibile definire le impostazioni di configurazione e le proprietà personalizzate per l'intero blueprint.

Impostazioni delle proprietà dei blueprint

Quando si crea il blueprint, è possibile specificare impostazioni valide per l'intero blueprint utilizzando la pagina **Proprietà blueprint**. Dopo aver creato il blueprint, è possibile modificare le impostazioni nella pagina **Proprietà blueprint**.

Scheda Generale

Le impostazioni nella scheda Generale si applicano all'intero blueprint di vRealize Automation.

Tabella 3-2. Impostazioni della scheda **Generale**

Impostazione	Descrizione
Nome	Immettere il nome del blueprint.
Identificatore	Il campo dell'identificatore viene compilato automaticamente in base al nome immesso. È possibile modificare il campo, ma dopo aver salvato il blueprint il campo non potrà più essere modificato. Gli identificatori sono permanenti e univoci all'interno del tenant. È possibile utilizzarli per interagire in modo programmatico con i blueprint e creare binding di proprietà.
Descrizione	Testo che riassume il blueprint a vantaggio di altri architetti. Questa descrizione viene anche visualizzata per gli utenti nel modulo di richiesta.
Limite distribuzione	Specificare il numero massimo di distribuzioni che è possibile creare quando questo blueprint viene utilizzato per il provisioning delle macchine.
Giorni di lease: Minimo e Massimo	Immettere un valore minimo e massimo per consentire agli utenti di scegliere da un intervallo di lunghezze di lease. Al termine del lease, la distribuzione viene eliminata o archiviata. Se non si specifica un valore minimo o massimo, il lease viene impostato senza una scadenza. Immettere le informazioni sul lease per le macchine nel blueprint di vRealize Automation, non nell'applicazione dell'endpoint di origine. Se si specificano le informazioni sul lease in un'applicazione esterna, non vengono riconosciute in vRealize Automation.

Tabella 3-2. Impostazioni della scheda **Generale** (continua)

Impostazione	Descrizione
Giorni di archiviazione	Invece di eliminare le distribuzioni immediatamente alla scadenza del lease, è possibile specificare un periodo di archiviazione temporanea. Specificare 0 per eliminare la distribuzione alla scadenza del suo lease. Il periodo di archiviazione inizia il giorno in cui scade il lease. Al termine del periodo di archiviazione, la distribuzione viene eliminata. Il valore predefinito è 0.
Propaga aggiornamenti alle distribuzioni esistenti	Gli intervalli minimo-massimo estesi per CPU, memoria o storage vengono inseriti nelle distribuzioni attive di cui è stato eseguito il provisioning dal blueprint. Il nuovo intervallo deve includere l'intero vecchio intervallo. Ad esempio, per un valore originale minimo di 32 e massimo di 128 (32, 128), una modifica come (16, 128) o (32, 256) o (2, 1000) può essere applicata dopo la riconfigurazione o la scalabilità orizzontale, mentre una modifica di (33, 512) o (4, 64) non può.

Scheda **Impostazioni NSX**

Se è stato configurato NSX, quando si crea o si modifica un blueprint è possibile specificare le impostazioni di NSX relative a zona di trasporto, criterio di prenotazione della rete e isolamento app. Queste impostazioni sono disponibili nella scheda **Impostazioni NSX** nelle pagine **Blueprint** e **Proprietà blueprint**.

Per informazioni sulle impostazioni di NSX, vedere [Nuovo blueprint e impostazioni della pagina delle proprietà del blueprint con NSX in vRealize Automation](#).

Scheda **Proprietà**

Le proprietà personalizzate aggiunte a livello del blueprint vengono applicate all'intero blueprint, inclusi tutti i componenti. Per informazioni sull'ordine di precedenza, vedere *Guida di riferimento alle proprietà personalizzate*.

Tabella 3-3. Impostazioni della scheda **Proprietà**

Scheda	Impostazione	Descrizione
Gruppi di proprietà		I gruppi di proprietà sono gruppi riutilizzabili che semplificano l'aggiunta di proprietà personalizzate ai blueprint.
	Aggiungi	<p>Aggiungere uno o più gruppi di proprietà esistenti e applicarli all'intero blueprint.</p> <p>Sono forniti i seguenti gruppi di proprietà correlati ai contenitori:</p> <ul style="list-style-type: none"> ■ Proprietà dell'host del contenitore con autenticazione mediante certificato ■ Proprietà dell'host del contenitore con autenticazione mediante utente/password

Tabella 3-3. Impostazioni della scheda **Proprietà** (continua)

Scheda	Impostazione	Descrizione
	Sposta su /Sposta giù	Controllano l'ordine di precedenza di ciascun gruppo di proprietà rispetto agli altri in base alle priorità desiderate. Il primo gruppo dell'elenco ha la priorità maggiore e le sue proprietà personalizzate hanno la precedenza rispetto a tutte le altre. È inoltre possibile scorrere per riordinare.
	Visualizza proprietà	Consente di visualizzare le proprietà personalizzate nel gruppo di proprietà selezionato.
	Visualizza proprietà unite	Se una proprietà personalizzata è inclusa in più di un gruppo di proprietà, la precedenza è assegnata al valore incluso nel gruppo di proprietà con la priorità più elevata.
Proprietà personalizzate	È possibile aggiungere singole proprietà personalizzate invece di gruppi di proprietà.	
	Nuovo	Aggiungere una singola proprietà personalizzata e applicarla all'intero blueprint.
	Nome	Specificare il nome della proprietà. Per un elenco delle proprietà personalizzate e delle relative definizioni, vedere <i>Guida di riferimento alle proprietà personalizzate</i> .
	Valore	Immettere il valore della proprietà personalizzata.
	Codificato	Codificare il valore della proprietà, ad esempio se il valore è una password.
	Sovrascrivibile	L'utente del blueprint può sovrascrivere il valore della proprietà. Se si seleziona Mostra nella richiesta , gli utenti possono visualizzare e modificare i valori delle proprietà quando richiedono elementi del catalogo.
	Mostra nella richiesta	Il nome e il valore della proprietà sono visibili per gli utenti nel modulo di richiesta di provisioning. Selezionare Sovrascrivibile se si consente agli utenti di fornire un valore.

vSphereImpostazioni dei componenti macchina in vRealize Automation

Di seguito sono elencate le impostazioni e le opzioni che è possibile configurare per un componente macchina di vSphere nella tela di progettazione di un blueprint vRealize Automation.

Scheda **Generale**

Configurare le impostazioni generali di un componente macchina di vSphere.

Tabella 3-4. Impostazioni della scheda Generale

Impostazione	Descrizione
ID	Specificare il nome del componente macchina o confermare il valore predefinito.
Descrizione	Testo che riassume il componente macchina a vantaggio di altri architetti.
Visualizza posizione su richiesta	<p>In un ambiente cloud, come vCloud Air, questo permette agli utenti di selezionare una regione per le macchine di cui è stato eseguito il provisioning.</p> <p>In un ambiente virtuale è possibile consentire agli utenti di selezionare la posizione di un data center per il provisioning di una macchina richiesta. Un amministratore di sistema deve aggiungere le informazioni del data center a un file delle posizioni. Un amministratore di struttura deve modificare una risorsa di elaborazione per associarla a una posizione.</p>
Criterio di prenotazione	Applicare un criterio di prenotazione a un blueprint per limitare le macchine di cui viene eseguito il provisioning da tale blueprint a un sottoinsieme di prenotazioni disponibili. Sono disponibili solo i criteri di prenotazione applicabili al tenant corrente.
Prefisso macchina	<p>I prefissi macchina vengono utilizzati per assegnare un nome alle macchine con provisioning. Se si seleziona Utilizza impostazione predefinita gruppo, le macchine vengono denominate in base al prefisso macchina predefinito per il gruppo di business. Se non si specifica un prefisso, ne viene generato uno basato sul nome del gruppo di business. Sono disponibili solo i prefissi macchina applicabili al tenant corrente.</p> <p>Se l'amministratore di struttura configura altri prefissi macchina selezionabili, è possibile applicare un prefisso a tutte le macchine di cui è stato eseguito il provisioning dal blueprint, indipendentemente da chi sia il richiedente.</p>
Istanze: Minimo e Massimo	<p>Configurare il numero massimo e minimo delle istanze che gli utenti possono richiedere per una distribuzione oppure un'azione di scalabilità verticale o orizzontale. Se si immette lo stesso valore nei campi Minimo e Massimo, viene configurato esattamente il numero di istanze di cui eseguire il provisioning.</p> <p>I componenti di XaaS non sono scalabili e non vengono aggiornati durante un'operazione di scalabilità. Se si stanno utilizzando i componenti di XaaS nel blueprint, è possibile creare un'azione di risorsa per gli utenti da eseguire dopo un'operazione di scalabilità, che potrebbe scalare o aggiornare i componenti di XaaS in base alle necessità. È possibile disattivare la scalabilità configurando il numero di istanze da consentire per ogni componente di macchina.</p>

Scheda **Informazioni build**

Configurare le impostazioni delle informazioni build di un componente macchina vSphere.

Tabella 3-5. Scheda Informazioni build

Impostazione	Descrizione
Tipo di blueprint	Per finalità di conservazione dei registri e gestione delle licenze, scegliere se le macchine di cui viene eseguito il provisioning dal blueprint sono classificate come Desktop o Server.
Azione	<p>Le opzioni visualizzate nel menu a discesa delle azioni dipendono dal tipo di macchina selezionato.</p> <p>Sono disponibili le seguenti azioni:</p> <ul style="list-style-type: none"> ■ Crea <p>Crea la specifica del componente macchina senza utilizzare un'opzione di clonazione.</p> ■ Clona <p>Crea copie di una macchina virtuale da un modello e da un oggetto di personalizzazione.</p> ■ Clone collegato <p>Esegue il provisioning di una copia dalle dimensioni ottimizzate di una macchina virtuale chiamata clone collegato. I cloni collegati sono basati su uno snapshot di una VM e utilizzano una catena di dischi delta per tenere traccia delle differenze rispetto a una macchina padre.</p> <p>Prima di eseguire il provisioning delle macchine virtuali dei cloni collegati, spegnere lo snapshot della macchina virtuale.</p> ■ NetApp FlexClone <p>Se le prenotazioni utilizzano lo storage NetApp FlexClone, è possibile clonare copie delle macchine di dimensioni ridotte.</p>

Tabella 3-5. Scheda Informazioni build (continua)

Impostazione	Descrizione
Provisioning workflow	<p>Le opzioni visualizzate nel menu a discesa provisioning workflow dipendono dal tipo di macchina selezionato e dall'azione selezionata.</p> <ul style="list-style-type: none"> ■ BasicVmWorkflow <p>Esegue il provisioning di una macchina senza sistema operativo guest.</p> ■ ExternalProvisioningWorkflow <p>Crea una macchina a partire da un'istanza di macchina virtuale o un'immagine basata su cloud.</p> ■ ImportOvfWorkflow <p>Consente di distribuire una macchina virtuale vSphere da un modello OVF nello stesso modo in cui CloneWorkflow consente di distribuire una macchina virtuale vSphere da un modello di macchina virtuale. È possibile importare a un componente vSphere in un blueprint di macchina o in un profilo componente Image per un blueprint parametrizzato.</p> ■ LinuxKickstartWorkflow <p>Esegue il provisioning di una macchina effettuando l'avvio da un'immagine ISO, utilizzando un file di configurazione kickstart o autoYaSt e un'immagine di distribuzione Linux per installare il sistema operativo sulla macchina.</p> ■ VirtualSccmProvisioningWorkflow <p>Esegue il provisioning di una macchina e trasferisce il controllo a una sequenza di attività SCCM per eseguire l'avvio da un'immagine ISO, distribuisce un sistema operativo Windows e installa l'agente guest di vRealize Automation.</p> ■ WIMImageWorkflow <p>Esegue il provisioning di una macchina effettuando l'avvio in un ambiente WinPE e installando un sistema operativo utilizzando l'immagine in formato WIM (Windows Imaging File Format) di una macchina di riferimento Windows esistente.</p> <p>Quando si utilizza un workflow di provisioning WIM in un blueprint, specificare un valore di storage che tenga conto della dimensione di ciascun disco da utilizzare sulla macchina. Utilizzare il valore totale di tutti i dischi come valore di storage minimo per il componente macchina. Specificare anche la dimensione di ogni disco in modo che sia sufficientemente grande da accogliere il sistema operativo.</p>

Tabella 3-5. Scheda Informazioni build (continua)

Impostazione	Descrizione
Clona da	<p>Consente di selezionare il modello di una macchina da cui clonare. È possibile perfezionare l'elenco dei modelli disponibili utilizzando l'opzione Filtri nel menu a discesa di ciascuna colonna.</p> <p>Per il clone collegato, sono visibili solo le macchine che dispongono di snapshot da cui eseguire la clonazione e che l'utente gestisce in qualità di amministratore tenant o manager del gruppo di business.</p> <p>È possibile clonare solo da modelli esistenti sulle macchine gestite in qualità di manager del gruppo di business o amministratore tenant.</p>
Clona da snapshot	<p>Per il clone collegato, selezionare uno snapshot esistente da cui eseguire la clonazione in base al modello di macchina selezionato. Le macchine vengono incluse nell'elenco solo se dispongono già di uno snapshot e se l'utente le gestisce come amministratore tenant o manager di gruppo di business.</p> <p>Se si seleziona Utilizza snapshot corrente, il clone viene definito con le stesse caratteristiche dello stato più recente della macchina virtuale. Se invece si desidera clonare uno snapshot effettivo, fare clic sull'opzione del menu a discesa e selezionare lo snapshot specifico dall'elenco.</p> <p>Nota L'uso del termine snapshot può creare confusione. Se si seleziona uno snapshot esistente, questa opzione crea un nuovo disco che ha come elemento padre lo snapshot. L'opzione Utilizza snapshot corrente non prevede un disco di base da utilizzare come padre e comporta l'esecuzione automatica di un'operazione di clonazione completa. Come soluzione alternativa, è possibile creare gli snapshot sul disco di base oppure utilizzare un workflow di vRealize Orchestrator per creare uno snapshot ed eseguire immediatamente la clonazione da tale snapshot.</p> <p>Questa opzione è disponibile solo per l'azione Clone collegato.</p>
Specifica personalizzazione	<p>Consente di impostare una specifica di personalizzazione disponibile. Una specifica di personalizzazione è necessaria solo se si sta effettuando la clonazione con indirizzi IP statici.</p> <p>Non è possibile eseguire la personalizzazione di macchine Windows senza una specifica di personalizzazione. Per macchine clonate Linux, è possibile eseguire la personalizzazione utilizzando una specifica di personalizzazione, uno script esterno o entrambi.</p>

Scheda Risorse macchina

Specificare le impostazioni relative a CPU, memoria e storage per un componente macchina di vSphere.

Tabella 3-6. Scheda **Risorse macchina**

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU che possono essere utilizzate dalle macchine di cui è stato effettuato il provisioning.
Memoria (MB): Minimo e Massimo	Immettere la quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning.
Storage (GB): Minimo e Massimo	Immettere la quantità minima e massima di storage che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning. Quando si utilizza un workflow di provisioning WIM in un blueprint, specificare un valore di storage che tenga conto della dimensione di ciascun disco da utilizzare sulla macchina. Utilizzare il valore totale di tutti i dischi come valore di storage minimo per il componente macchina. Specificare anche la dimensione di ogni disco in modo che sia sufficientemente grande da accogliere il sistema operativo.

Scheda Storage

È possibile aggiungere impostazioni dei volumi di storage, incluso uno o più criteri di prenotazione storage, al componente macchina per controllare lo spazio di storage.

Tabella 3-7. Impostazioni della scheda **Storage**

Impostazione	Descrizione
ID	Consente di immettere un ID o un nome per il volume di storage.
Capacità (GB)	Consente di immettere la capacità di storage per il volume di storage.
Lettera di unità/Percorso di montaggio	Consente di specificare una lettera di unità e un percorso di montaggio per il volume di storage. Questa opzione viene utilizzata durante il provisioning in associazione con un agente guest. Non può essere modificata dopo il provisioning della macchina. Se non si utilizza un agente guest, questa opzione viene ignorata.
Etichetta	Consente di specificare un'etichetta per la lettera di unità e un percorso di montaggio per il volume di storage. Questa opzione viene utilizzata durante il provisioning in associazione con un agente guest. Non può essere modificata dopo il provisioning della macchina. Se non si utilizza un agente guest, questa opzione viene ignorata.

Tabella 3-7. Impostazioni della scheda **Storage** (continua)

Impostazione	Descrizione
Criterio di prenotazione storage	Consente di specificare il criterio di prenotazione storage da utilizzare con questo volume di storage. Sono disponibili solo i criteri di prenotazione storage applicabili al tenant corrente.
Proprietà personalizzate	Consente di specificare le eventuali proprietà personalizzate da utilizzare con questo volume di storage.
Volumi massimi	Consente di specificare il numero massimo di volumi di storage consentiti che è possibile utilizzare al momento del provisioning dal componente macchina. Specificare 0 per impedire ad altri di aggiungere volumi di storage. Il valore predefinito è 60.
Consenti all'utente di vedere e modificare i criteri di prenotazione storage	Selezionare questa casella di controllo per consentire agli utenti di rimuovere un criterio di prenotazione associato o specificare un criterio di prenotazione diverso al momento del provisioning.

Scheda Rete

È possibile configurare le impostazioni di rete per un componente macchina vSphere basato sulle impostazioni della rete NSX e del bilanciamento del carico configurate all'esterno di vRealize Automation. È possibile utilizzare impostazioni provenienti da uno o più componenti rete NSX su richiesta nella tela di progettazione.

Per informazioni correlate, vedere [Configurazione delle impostazioni dei componenti rete e sicurezza in vRealize Automation](#) e [Nuovo blueprint e impostazioni della pagina delle proprietà del blueprint con NSX in vRealize Automation](#).

Tabella 3-8. Impostazioni della scheda **Rete**

Impostazione	Descrizione
Rete	Selezionare un componente di rete dal menu a discesa. Vengono elencati solo i componenti di rete esistenti nella tela di progettazione. Sono disponibili solo i profili di rete applicabili al tenant corrente. La rete selezionata determina il tipo di rete e anche se il cluster da distribuire nella rete è gestito da NSX for vSphere o NSX-T.
Tipo di assegnazione	Consente di accettare l'assegnazione predefinita mutuata dal componente di rete o selezionare un tipo di assegnazione dal menu a discesa. I valori delle opzioni DHCP e Statico derivano dalle impostazioni contenute nel componente rete.
Indirizzo	Specificare l'indirizzo IP per la rete. Questa opzione è disponibile solo per il tipo di indirizzo statico.
Bilanciamento del carico	Immettere il servizio da utilizzare per il bilanciamento del carico.

Tabella 3-8. Impostazioni della scheda **Rete** (continua)

Impostazione	Descrizione
Proprietà personalizzate	Visualizza le proprietà personalizzate configurate per il componente di rete o il profilo di rete selezionato.
Schede di rete massime	Consente di specificare il numero massimo di schede di rete (o NIC) consentite per questo componente macchina. L'impostazione predefinita è illimitata. Impostare su 0 per disattivare l'aggiunta di NIC per i componenti macchina.

Scheda **Sicurezza**

È possibile configurare le impostazioni di sicurezza per un componente macchina vSphere sulla base delle impostazioni di NSX configurate all'esterno di vRealize Automation. Facoltativamente è possibile utilizzare impostazioni provenienti da componenti di sicurezza NSX esistenti o su richiesta nella tela di progettazione.

Vengono rese automaticamente disponibili le impostazioni di sicurezza dai componenti tag di sicurezza e gruppo di sicurezza esistente e su richiesta nella tela di progettazione.

Per informazioni sull'aggiunta e la configurazione di componenti rete e sicurezza di NSX prima di utilizzare le impostazioni della scheda Sicurezza in un componente macchina vSphere, vedere [Configurazione delle impostazioni dei componenti rete e sicurezza in vRealize Automation](#).

Per informazioni su come specificare le informazioni di NSX che si applicano a tutti i componenti della macchina vSphere nel blueprint, vedere [Nuovo blueprint e impostazioni della pagina delle proprietà del blueprint con NSX in vRealize Automation](#).

Tabella 3-9. Impostazioni della scheda **Sicurezza**

Impostazione	Descrizione
Nome	Visualizza il nome di un tag o un gruppo di sicurezza di NSX. I nomi sono derivati dai componenti sicurezza e presentati nella tela di progettazione. Selezionare la casella di controllo accanto a un gruppo o un tag di sicurezza elencato per utilizzare tale gruppo o tag per il provisioning da questo componente macchina.
Tipo	Consente di indicare se l'elemento di sicurezza è un gruppo di sicurezza su richiesta, un gruppo di sicurezza esistente o un tag di sicurezza.
Descrizione	Consente di visualizzare la descrizione definita per il gruppo o il tag di sicurezza.
Endpoint	Consente di visualizzare l'endpoint utilizzato dal gruppo o dal tag di sicurezza di NSX.

Scheda **Proprietà**

È possibile specificare informazioni relative a proprietà personalizzate e gruppi di proprietà per il componente macchina di vSphere.

Attraverso la scheda **Proprietà** è possibile aggiungere al componente macchina proprietà personalizzate singole e gruppi di proprietà personalizzate. È inoltre possibile aggiungere proprietà personalizzate e gruppi di proprietà all'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint mediante la pagina **Proprietà blueprint**.

È possibile utilizzare la scheda **Proprietà personalizzate** per aggiungere e configurare opzioni di proprietà personalizzate esistenti. vRealize Automation dispone già di alcune proprietà personalizzate ed è inoltre possibile creare definizioni di proprietà.

Tabella 3-10. Impostazioni della scheda **Proprietà > Proprietà personalizzate**

Impostazione	Descrizione
Nome	Consente di specificare il nome di una proprietà personalizzata o selezionare una proprietà personalizzata disponibile dal menu a discesa. Nel menu a discesa vengono elencate solo le proprietà delle quali l'amministratore tenant o di struttura ha creato le definizioni.
Valore	Consente di immettere o modificare un valore da associare al nome della proprietà personalizzata. Ad esempio, impostare il valore su <code>true</code> per consentire agli utenti autorizzati di connettersi alle macchine virtuali mediante SSH.
Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.
Sovrascrivibile	È possibile specificare che il valore di una proprietà può essere sovrascritto dalla persona successiva che utilizza tale proprietà. Se si seleziona Mostra nella richiesta , gli utenti possono modificare i valori delle proprietà quando richiedono elementi del catalogo.
Mostra nella richiesta	È possibile visualizzare il nome e il valore della proprietà per gli utenti quando richiedono il provisioning della macchina. Selezionare l'opzione sovrascrivibile se si desidera che gli utenti forniscano un valore.

È possibile utilizzare la scheda **Gruppi di proprietà** per aggiungere e configurare le impostazioni dei gruppi di proprietà personalizzate esistenti. L'utente può creare i gruppi di proprietà propri o utilizzare gruppi di proprietà creati da altri per lui.

Tabella 3-11. Impostazioni della scheda **Proprietà > Gruppi di proprietà**

Impostazione	Descrizione
Nome	Consente di selezionare un gruppo di proprietà disponibile dal menu a discesa.
Sposta su e Sposta giù	Consente di controllare il livello di precedenza dei gruppi di proprietà in ordine decrescente. Un gruppo di proprietà elencato prima ha la precedenza sui gruppi di proprietà elencati dopo e così via.

Tabella 3-11. Impostazioni della scheda **Proprietà > Gruppi di proprietà** (continua)

Impostazione	Descrizione
Visualizza proprietà	Visualizza le proprietà personalizzate nel gruppo di proprietà selezionato.
Visualizza proprietà unite	Visualizzare le proprietà personalizzate nell'ordine in cui sono presenti nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi, la proprietà compare una volta nell'elenco in base alla sua prima occorrenza.

Scheda Profili

I profili dei componenti forniscono un mezzo di parametrizzazione dei blueprint. Ad esempio, anziché creare blueprint separati, è possibile creare una funzione di piccole, medie e grandi dimensioni in un singolo blueprint. È possibile selezionare una dimensione del blueprint durante la distribuzione. I profili dei componenti sono progettati per semplificare il catalogo.

Se sono stati creati set di valori per i profili componente di vRealize Automation **Size** e **Image** forniti, è possibile configurare queste impostazioni per il componente macchina nel blueprint. È possibile anche selezionare un set di valori diverso quando si distribuisce l'elemento del catalogo.

I profili componente sono disponibili solo per componenti macchina vSphere.

Un profilo componente sovrascrive le impostazioni sul componente macchina, come numero di CPU e storage.

Il set di valori del profilo componente viene applicato a tutte le macchine vSphere di un cluster.

Non è possibile riconfigurare le macchine utilizzando i profili componente **Size** o **Image**.

L'intervallo di CPU, memoria e storage viene calcolato dal profilo e rimane disponibile per le azioni di riconfigurazione. Ad esempio, utilizzare un set di valori **Size** piccolo (1 CPU, 1024 MB di memoria e 10 GB di storage), medio (3 CPU, 2048 MB di memoria, 12 GB di storage) e grande (5 CPU, 3072 MB di memoria, 15 GB di storage). Gli intervalli disponibili durante la riconfigurazione della macchina sono 1-5 CPU, 1024-3072 MB di memoria e 1-15 GB di storage.

Per ulteriori informazioni, vedere *Guida di riferimento alle proprietà personalizzate*.

Tabella 3-12. Impostazioni della scheda **Profili**

Impostazione	Descrizione
Aggiungi	Aggiungere il profilo componente Size o Image .
Modifica set di valori	Assegnare uno o più set di valori per il profilo componente selezionato scegliendo da un elenco di set di valori definiti. È possibile impostare uno dei set di valori come predefinito.
Rimuovi	Rimuovere il profilo componente Size o Image .

Impostazioni dei componenti macchina di vCloud Air

Di seguito sono elencate le impostazioni e le opzioni che è possibile configurare per un componente macchina di vCloud Air nella tela di progettazione di un blueprint vRealize Automation.

Scheda **Generale**

Configurare le impostazioni generali di un componente macchina di vCloud Air.

Tabella 3-13. Impostazioni della scheda Generale

Impostazione	Descrizione
ID	Specificare il nome del componente macchina o confermare il valore predefinito.
Descrizione	Testo che riepiloga il componente macchina a vantaggio di altri architetti.
Visualizza posizione su richiesta	<p>In un ambiente cloud, come vCloud Air, questo permette agli utenti di selezionare una regione per le macchine di cui è stato eseguito il provisioning.</p> <p>In un ambiente virtuale è possibile consentire agli utenti di selezionare la posizione di un data center per il provisioning di una macchina richiesta. Un amministratore di sistema deve aggiungere le informazioni del data center a un file delle posizioni. Un amministratore di struttura deve modificare una risorsa di elaborazione per associarla a una posizione.</p>
Criterio di prenotazione	Applicare un criterio di prenotazione a un blueprint per limitare le macchine di cui viene eseguito il provisioning da tale blueprint a un sottoinsieme di prenotazioni disponibili. Sono disponibili solo i criteri di prenotazione applicabili al tenant corrente.

Tabella 3-13. Impostazioni della scheda **Generale** (continua)

Impostazione	Descrizione
Prefisso macchina	<p>I prefissi macchina vengono utilizzati per assegnare un nome alle macchine con provisioning. Se si seleziona Utilizza impostazione predefinita gruppo, le macchine vengono denominate in base al prefisso macchina predefinito per il gruppo di business. Se non si specifica un prefisso, ne viene generato uno basato sul nome del gruppo di business. Sono disponibili solo i prefissi macchina applicabili al tenant corrente.</p> <p>Se l'amministratore di struttura configura altri prefissi macchina selezionabili, è possibile applicare un prefisso a tutte le macchine di cui è stato eseguito il provisioning dal blueprint, indipendentemente da chi sia il richiedente.</p>
Istanze: Minimo e Massimo	<p>Configurare il numero massimo e minimo delle istanze che gli utenti possono richiedere per una distribuzione oppure un'azione di scalabilità verticale o orizzontale. Se si immette lo stesso valore nei campi Minimo e Massimo, viene configurato esattamente il numero di istanze di cui eseguire il provisioning.</p> <p>I componenti di XaaS non sono scalabili e non vengono aggiornati durante un'operazione di scalabilità. Se si stanno utilizzando i componenti di XaaS nel blueprint, è possibile creare un'azione di risorsa per gli utenti da eseguire dopo un'operazione di scalabilità, che potrebbe scalare o aggiornare i componenti di XaaS in base alle necessità. È possibile disattivare la scalabilità configurando il numero di istanze da consentire per ogni componente di macchina.</p>

Scheda **Informazioni build**

Configurare le impostazioni delle informazioni build di un componente macchina vCloud Air.

Tabella 3-14. Scheda **Informazioni build**

Impostazione	Descrizione
Tipo di blueprint	Per finalità di conservazione dei registri e gestione delle licenze, scegliere se le macchine di cui viene eseguito il provisioning dal blueprint sono classificate come Desktop o Server.
Azione	<p>Le opzioni visualizzate nel menu a discesa delle azioni dipendono dal tipo di macchina selezionato.</p> <p>L'unica azione di provisioning disponibile per un componente macchina di vCloud Air è Clone.</p> <ul style="list-style-type: none"> ■ Clona <p>Crea copie di una macchina virtuale da un modello e da un oggetto di personalizzazione.</p>

Tabella 3-14. Scheda **Informazioni build** (continua)

Impostazione	Descrizione
Provisioning workflow	<p>Le opzioni visualizzate nel menu a discesa provisioning workflow dipendono dal tipo di macchina selezionato e dall'azione selezionata.</p> <p>L'unica azione di provisioning disponibile per un componente macchina di vCloud Air è CloneWorkflow.</p> <p>■ CloneWorkflow</p> <p>Crea copie di una macchina virtuale mediante clone, clone collegato o NetApp Flexclone.</p>
Clona da	<p>Consente di selezionare il modello di una macchina da cui clonare. È possibile perfezionare l'elenco dei modelli disponibili utilizzando l'opzione Filtri nel menu a discesa di ciascuna colonna.</p> <p>Per il clone collegato, sono visibili solo le macchine che dispongono di snapshot da cui eseguire la clonazione e che l'utente gestisce in qualità di amministratore tenant o manager del gruppo di business.</p> <p>È possibile clonare solo da modelli esistenti sulle macchine gestite in qualità di manager del gruppo di business o amministratore tenant.</p>

Scheda **Risorse macchina**

Specificare le impostazioni relative a CPU, memoria e storage per il componente macchina di vCloud Air.

Tabella 3-15. Scheda **Risorse macchina**

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU che possono essere utilizzate dalle macchine di cui è stato effettuato il provisioning.
Memoria (MB): Minimo e Massimo	Immettere la quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning.
Storage (GB): Minimo e Massimo	Immettere la quantità minima e massima di storage che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning.

Scheda **Storage**

È possibile aggiungere impostazioni dei volumi di storage, incluso uno o più criteri di prenotazione storage, al componente macchina per controllare lo spazio di storage.

Tabella 3-16. Impostazioni della scheda **Storage**

Impostazione	Descrizione
ID	Consente di immettere un ID o un nome per il volume di storage.
Capacità (GB)	Consente di immettere la capacità di storage per il volume di storage.
Lettera di unità/Percorso di montaggio	Consente di specificare una lettera di unità e un percorso di montaggio per il volume di storage. Questa opzione viene utilizzata durante il provisioning in associazione con un agente guest. Non può essere modificata dopo il provisioning della macchina. Se non si utilizza un agente guest, questa opzione viene ignorata.
Etichetta	Consente di specificare un'etichetta per la lettera di unità e un percorso di montaggio per il volume di storage. Questa opzione viene utilizzata durante il provisioning in associazione con un agente guest. Non può essere modificata dopo il provisioning della macchina. Se non si utilizza un agente guest, questa opzione viene ignorata.
Criterio di prenotazione storage	Consente di specificare il criterio di prenotazione storage da utilizzare con questo volume di storage. Sono disponibili solo i criteri di prenotazione storage applicabili al tenant corrente.
Proprietà personalizzate	Consente di specificare le eventuali proprietà personalizzate da utilizzare con questo volume di storage.
Volumi massimi	Consente di specificare il numero massimo di volumi di storage consentiti che è possibile utilizzare al momento del provisioning dal componente macchina. Specificare 0 per impedire ad altri di aggiungere volumi di storage. Il valore predefinito è 60.
Consenti all'utente di vedere e modificare i criteri di prenotazione storage	Selezionare questa casella di controllo per consentire agli utenti di rimuovere un criterio di prenotazione associato o specificare un criterio di prenotazione diverso al momento del provisioning.

Scheda **Proprietà**

Facoltativamente è possibile specificare informazioni relative a proprietà personalizzate e gruppi di proprietà per il componente macchina di vCloud Air.

Attraverso la scheda **Proprietà** è possibile aggiungere al componente macchina proprietà personalizzate singole e gruppi di proprietà personalizzate. È inoltre possibile aggiungere proprietà personalizzate e gruppi di proprietà all'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint mediante la pagina **Proprietà blueprint**.

È possibile utilizzare la scheda **Proprietà personalizzate** per aggiungere e configurare opzioni di proprietà personalizzate esistenti. vRealize Automation dispone già di alcune proprietà personalizzate ed è inoltre possibile creare definizioni di proprietà.

Tabella 3-17. Impostazioni della scheda **Proprietà > Proprietà personalizzate**

Impostazione	Descrizione
Nome	Consente di specificare il nome di una proprietà personalizzata o selezionare una proprietà personalizzata disponibile dal menu a discesa. Nel menu a discesa vengono elencate solo le proprietà delle quali l'amministratore tenant o di struttura ha creato le definizioni.
Valore	Consente di immettere o modificare un valore da associare al nome della proprietà personalizzata. Ad esempio, impostare il valore su true per consentire agli utenti autorizzati di connettersi alle macchine virtuali mediante SSH.
Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.
Sovrascrivibile	È possibile specificare che il valore di una proprietà può essere sovrascritto dalla persona successiva che utilizza tale proprietà. Se si seleziona Mostra nella richiesta , gli utenti possono modificare i valori delle proprietà quando richiedono elementi del catalogo.
Mostra nella richiesta	È possibile visualizzare il nome e il valore della proprietà per gli utenti quando richiedono il provisioning della macchina. Selezionare l'opzione sovrascrivibile se si desidera che gli utenti forniscano un valore.

È possibile utilizzare la scheda **Gruppi di proprietà** per aggiungere e configurare le impostazioni dei gruppi di proprietà personalizzate esistenti. L'utente può creare i gruppi di proprietà propri o utilizzare gruppi di proprietà creati da altri per lui.

Tabella 3-18. Impostazioni della scheda **Proprietà > Gruppi di proprietà**

Impostazione	Descrizione
Nome	Consente di selezionare un gruppo di proprietà disponibile dal menu a discesa.
Sposta su e Sposta giù	Consente di controllare il livello di precedenza dei gruppi di proprietà in ordine decrescente. Un gruppo di proprietà elencato prima ha la precedenza sui gruppi di proprietà elencati dopo e così via.
Visualizza proprietà	Visualizza le proprietà personalizzate nel gruppo di proprietà selezionato.
Visualizza proprietà unite	Visualizzare le proprietà personalizzate nell'ordine in cui sono presenti nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi, la proprietà compare una volta nell'elenco in base alla sua prima occorrenza.

Impostazioni dei componenti macchina Amazon

Di seguito sono elencate le impostazioni e le opzioni che è possibile configurare per un componente macchina Amazon nella tela di progettazione di un blueprint vRealize Automation.

Scheda **Generale**

Configurare le impostazioni generali di un componente macchina Amazon.

Tabella 3-19. Impostazioni della scheda Generale

Impostazione	Descrizione
ID	Specificare il nome del componente macchina o confermare il valore predefinito.
Descrizione	Testo che riepiloga il componente macchina a vantaggio di altri architetti.
Visualizza posizione su richiesta	<p>In un ambiente cloud, come vCloud Air, questo permette agli utenti di selezionare una regione per le macchine di cui è stato eseguito il provisioning.</p> <p>In un ambiente virtuale è possibile consentire agli utenti di selezionare la posizione di un data center per il provisioning di una macchina richiesta. Un amministratore di sistema deve aggiungere le informazioni del data center a un file delle posizioni. Un amministratore di struttura deve modificare una risorsa di elaborazione per associarla a una posizione.</p>
Criterio di prenotazione	Applicare un criterio di prenotazione a un blueprint per limitare le macchine di cui viene eseguito il provisioning da tale blueprint a un sottoinsieme di prenotazioni disponibili. Sono disponibili solo i criteri di prenotazione applicabili al tenant corrente.
Prefisso macchina	<p>I prefissi macchina vengono utilizzati per assegnare un nome alle macchine con provisioning. Se si seleziona Utilizza impostazione predefinita gruppo, le macchine vengono denominate in base al prefisso macchina predefinito per il gruppo di business. Se non si specifica un prefisso, ne viene generato uno basato sul nome del gruppo di business. Sono disponibili solo i prefissi macchina applicabili al tenant corrente.</p> <p>Se l'amministratore di struttura configura altri prefissi macchina selezionabili, è possibile applicare un prefisso a tutte le macchine di cui è stato eseguito il provisioning dal blueprint, indipendentemente da chi sia il richiedente.</p>
Istanze: Minimo e Massimo	<p>Configurare il numero massimo e minimo delle istanze che gli utenti possono richiedere per una distribuzione oppure un'azione di scalabilità verticale o orizzontale. Se si immette lo stesso valore nei campi Minimo e Massimo, viene configurato esattamente il numero di istanze di cui eseguire il provisioning.</p> <p>I componenti di XaaS non sono scalabili e non vengono aggiornati durante un'operazione di scalabilità. Se si stanno utilizzando i componenti di XaaS nel blueprint, è possibile creare un'azione di risorsa per gli utenti da eseguire dopo un'operazione di scalabilità, che potrebbe scalare o aggiornare i componenti di XaaS in base alle necessità. È possibile disattivare la scalabilità configurando il numero di istanze da consentire per ogni componente di macchina.</p>

Scheda Informazioni build

Configurare le impostazioni delle informazioni build di un componente macchina Amazon.

Tabella 3-20. Scheda Informazioni build

Impostazione	Descrizione
Tipo di blueprint	Per finalità di conservazione dei registri e gestione delle licenze, scegliere se le macchine di cui viene eseguito il provisioning dal blueprint sono classificate come Desktop o Server.
Provisioning workflow	<p>L'unico workflow di provisioning disponibile per un componente macchina Amazon è CloudProvisioningWorkflow.</p> <ul style="list-style-type: none"> ■ CloudProvisioningWorkflow <p>Crea una macchina a partire da un'istanza di macchina virtuale o un'immagine basata su cloud.</p>
Immagine macchina Amazon	Consente di selezionare un'immagine di macchina Amazon disponibile. Le immagini delle macchine Amazon sono modelli contenenti una configurazione software, che include un sistema operativo. Le immagini delle macchine sono gestite da account di Amazon Web Services. È possibile ridefinire l'elenco di nomi di immagine delle macchine Amazon nel display utilizzando l'opzione Filtri nel menu a discesa della colonna ID AMI .
Coppia di chiavi	<p>Le coppie di chiavi sono necessarie per il provisioning con Amazon Web Services.</p> <p>Le coppie di chiavi sono utilizzate per eseguire il provisioning e connettersi a un'istanza cloud. Vengono anche utilizzate per decrittografare le password di Windows o accedere a una macchina Linux.</p> <p>Sono disponibili le seguenti opzioni di coppie di chiavi:</p> <ul style="list-style-type: none"> ■ Non specificato <p>Controlla il comportamento della coppia di chiavi al livello del blueprint invece che al livello di prenotazione.</p> ■ Generato automaticamente per gruppo di business <p>Specifica che ogni macchina con provisioning effettuato nello stesso gruppo di business ha la stessa coppia di chiavi, incluse le macchine con provisioning effettuato su altre prenotazioni quando la macchina ha la stessa risorsa di elaborazione e lo stesso gruppo di business. Dato che le coppie di chiavi sono associate a un gruppo di business, vengono eliminate quando il gruppo di business viene eliminato.</p> ■ Generato automaticamente per macchina <p>Specifica che ogni macchina ha una coppia di chiavi univoca. Questa opzione è il metodo più sicuro perché non vengono condivise coppie di chiavi tra macchine.</p>

Tabella 3-20. Scheda Informazioni build (continua)

Impostazione	Descrizione
Attiva opzioni di rete Amazon sulla macchina	Permette di scegliere se consentire agli utenti di eseguire il provisioning di una macchina in una posizione Virtual Private Cloud (VPC) o non VPC quando inviano la richiesta.
Tipi di istanze	<p>Selezionare uno o più tipi di istanze Amazon. Un'istanza Amazon è un server virtuale che può eseguire applicazioni in Amazon Web Services. Le istanze vengono create dall'immagine di una macchina Amazon e scegliendo un tipo di istanza appropriato. vRealize Automation gestisce i tipi di istanze di immagini macchina disponibili per il provisioning.</p> <p>Per ulteriori informazioni sull'utilizzo dei tipi di istanze di Amazon in vRealize Automation, vedere I tipi di istanze di Amazon e Aggiunta di un tipo di istanza Amazon.</p>

Scheda Risorse macchina

Specificare le impostazioni relative a CPU, memoria, storage e volume EBS per il componente macchina Amazon.

È inoltre possibile riconfigurare tutti i volumi di archiviazione della macchina Amazon nella distribuzione ad eccezione del volume root.

Tabella 3-21. Scheda Risorse macchina

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU che possono essere utilizzate dalle macchine di cui è stato effettuato il provisioning.
Memoria (MB): Minimo e Massimo	Immettere la quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning.
Storage (GB): Minimo e Massimo	Immettere la quantità minima e massima di storage che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning.

Tabella 3-21. Scheda **Risorse macchina** (continua)

Impostazione	Descrizione
Storage EBS (GB): Minimo e Massimo	<p>Immettere la quantità minima e massima di volume di storage di Amazon Elastic Block Store (EBS) che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning.</p> <p>Quando si elimina una distribuzione contenente un componente macchina Amazon, tutti i volumi EBS aggiunti alla macchina durante il suo ciclo di vita vengono scollegati anziché eliminati. vRealize Automation non fornisce alcuna opzione per l'eliminazione dei volumi EBS.</p>
Eliminare i volumi	<p>Specifica se è possibile eliminare i volumi EC2 singolarmente o in blocco quando vengono eliminate le distribuzioni Amazon.</p> <p>Sia la scelta di Sì che la scelta di No consentono un'azione di eliminazione di massa di tutti i volumi nella distribuzione. Il valore predefinito è null o vuoto.</p> <ul style="list-style-type: none"> ■ Sì: consente di eliminare la distribuzione Amazon ed eliminare i volumi. ■ No: consente di eliminare la distribuzione Amazon e mantenere i volumi. ■ null o vuoto: richiede all'utente di specificare il valore Sì o No quando vengono eliminate le distribuzioni Amazon.

Scheda **Proprietà**

Facoltativamente è possibile specificare informazioni relative a proprietà personalizzate e gruppi di proprietà per il componente macchina Amazon.

Attraverso la scheda **Proprietà** è possibile aggiungere al componente macchina proprietà personalizzate singole e gruppi di proprietà personalizzate. È inoltre possibile aggiungere proprietà personalizzate e gruppi di proprietà all'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint mediante la pagina **Proprietà blueprint**.

È possibile utilizzare la scheda **Proprietà personalizzate** per aggiungere e configurare opzioni di proprietà personalizzate esistenti. vRealize Automation dispone già di alcune proprietà personalizzate ed è inoltre possibile creare definizioni di proprietà.

Tabella 3-22. Impostazioni della scheda **Proprietà > Proprietà personalizzate**

Impostazione	Descrizione
Nome	Consente di specificare il nome di una proprietà personalizzata o selezionare una proprietà personalizzata disponibile dal menu a discesa. Nel menu a discesa vengono elencate solo le proprietà delle quali l'amministratore tenant o di struttura ha creato le definizioni.
Valore	Consente di immettere o modificare un valore da associare al nome della proprietà personalizzata. Ad esempio, impostare il valore su true per consentire agli utenti autorizzati di connettersi alle macchine virtuali mediante SSH.
Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.
Sovrascrivibile	È possibile specificare che il valore di una proprietà può essere sovrascritto dalla persona successiva che utilizza tale proprietà. Se si seleziona Mostra nella richiesta , gli utenti possono modificare i valori delle proprietà quando richiedono elementi del catalogo.
Mostra nella richiesta	È possibile visualizzare il nome e il valore della proprietà per gli utenti quando richiedono il provisioning della macchina. Selezionare l'opzione sovrascrivibile se si desidera che gli utenti forniscano un valore.

È possibile utilizzare la scheda **Gruppi di proprietà** per aggiungere e configurare le impostazioni dei gruppi di proprietà personalizzate esistenti. L'utente può creare i gruppi di proprietà propri o utilizzare gruppi di proprietà creati da altri per lui.

Tabella 3-23. Impostazioni della scheda **Proprietà > Gruppi di proprietà**

Impostazione	Descrizione
Nome	Consente di selezionare un gruppo di proprietà disponibile dal menu a discesa.
Sposta su e Sposta giù	Consente di controllare il livello di precedenza dei gruppi di proprietà in ordine decrescente. Un gruppo di proprietà elencato prima ha la precedenza sui gruppi di proprietà elencati dopo e così via.
Visualizza proprietà	Visualizza le proprietà personalizzate nel gruppo di proprietà selezionato.
Visualizza proprietà unite	Visualizzare le proprietà personalizzate nell'ordine in cui sono presenti nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi, la proprietà compare una volta nell'elenco in base alla sua prima occorrenza.

Impostazioni dei componenti macchina OpenStack

Di seguito sono elencate le impostazioni e le opzioni che è possibile configurare per un componente macchina OpenStack nella tela di progettazione di un blueprint vRealize Automation.

Scheda **Generale**

Configurare le impostazioni generali di un componente macchina OpenStack.

Tabella 3-24. Impostazioni della scheda Generale

Impostazione	Descrizione
ID	Specificare il nome del componente macchina o confermare il valore predefinito.
Descrizione	Testo che riepiloga il componente macchina a vantaggio di altri architetti.
Visualizza posizione su richiesta	<p>In un ambiente cloud, come vCloud Air, questo permette agli utenti di selezionare una regione per le macchine di cui è stato eseguito il provisioning.</p> <p>In un ambiente virtuale è possibile consentire agli utenti di selezionare la posizione di un data center per il provisioning di una macchina richiesta. Un amministratore di sistema deve aggiungere le informazioni del data center a un file delle posizioni. Un amministratore di struttura deve modificare una risorsa di elaborazione per associarla a una posizione.</p>
Criterio di prenotazione	Applicare un criterio di prenotazione a un blueprint per limitare le macchine di cui viene eseguito il provisioning da tale blueprint a un sottoinsieme di prenotazioni disponibili. Sono disponibili solo i criteri di prenotazione applicabili al tenant corrente.

Tabella 3-24. Impostazioni della scheda **Generale** (continua)

Impostazione	Descrizione
Prefisso macchina	<p>I prefissi macchina vengono utilizzati per assegnare un nome alle macchine con provisioning. Se si seleziona Utilizza impostazione predefinita gruppo, le macchine vengono denominate in base al prefisso macchina predefinito per il gruppo di business. Se non si specifica un prefisso, ne viene generato uno basato sul nome del gruppo di business. Sono disponibili solo i prefissi macchina applicabili al tenant corrente.</p> <p>Se l'amministratore di struttura configura altri prefissi macchina selezionabili, è possibile applicare un prefisso a tutte le macchine di cui è stato eseguito il provisioning dal blueprint, indipendentemente da chi sia il richiedente.</p>
Istanze: Minimo e Massimo	<p>Configurare il numero massimo e minimo delle istanze che gli utenti possono richiedere per una distribuzione oppure un'azione di scalabilità verticale o orizzontale. Se si immette lo stesso valore nei campi Minimo e Massimo, viene configurato esattamente il numero di istanze di cui eseguire il provisioning.</p> <p>I componenti di XaaS non sono scalabili e non vengono aggiornati durante un'operazione di scalabilità. Se si stanno utilizzando i componenti di XaaS nel blueprint, è possibile creare un'azione di risorsa per gli utenti da eseguire dopo un'operazione di scalabilità, che potrebbe scalare o aggiornare i componenti di XaaS in base alle necessità. È possibile disattivare la scalabilità configurando il numero di istanze da consentire per ogni componente di macchina.</p>

Scheda **Informazioni build**

Configurare le impostazioni delle informazioni build di un componente macchina OpenStack.

Tabella 3-25. Scheda **Informazioni build**

Impostazione	Descrizione
Tipo di blueprint	Per finalità di conservazione dei registri e gestione delle licenze, scegliere se le macchine di cui viene eseguito il provisioning dal blueprint sono classificate come Desktop o Server.
Provisioning workflow	<p>Per un componente macchina OpenStack sono disponibili i seguenti workflow di provisioning.</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow Esegue il provisioning di una macchina effettuando l'avvio da un'immagine ISO, utilizzando un file di configurazione kickstart o autoYaSt e un'immagine di distribuzione Linux per installare il sistema operativo sulla macchina. ■ CloudProvisioningWorkflow Crea una macchina a partire da un'istanza di macchina virtuale o un'immagine basata su cloud. ■ CloudWIMImageWorkflow Esegue il provisioning di una macchina effettuando l'avvio in un ambiente WinPE e installando un sistema operativo utilizzando l'immagine in formato WIM (Windows Imaging File Format) di una macchina di riferimento Windows esistente. Quando si utilizza un workflow di provisioning WIM in un blueprint, specificare un valore di storage che tenga conto della dimensione di ciascun disco da utilizzare sulla macchina. Utilizzare il valore totale di tutti i dischi come valore di storage minimo per il componente macchina. Specificare anche la dimensione di ogni disco in modo che sia sufficientemente grande da accogliere il sistema operativo.
Immagine OpenStack	Selezionare un'immagine OpenStack disponibile. L'immagine OpenStack è un modello contenente una configurazione software, che include un sistema operativo. Le immagini sono gestite da account di OpenStack. È possibile ridefinire l'elenco di nomi di immagini OpenStack nel display utilizzando l'opzione Filtri nel menu a discesa della colonna Nomi .

Tabella 3-25. Scheda **Informazioni build** (continua)

Impostazione	Descrizione
Coppia di chiavi	<p>Per il provisioning con OpenStack le coppie di chiavi sono facoltative.</p> <p>Le coppie di chiavi sono utilizzate per eseguire il provisioning e connettersi a un'istanza cloud. Vengono anche utilizzate per decrittografare le password di Windows o accedere a una macchina Linux.</p> <p>Sono disponibili le seguenti opzioni di coppie di chiavi:</p> <ul style="list-style-type: none"> ■ Non specificato <p>Controlla il comportamento della coppia di chiavi al livello del blueprint invece che al livello di prenotazione.</p> ■ Generato automaticamente per gruppo di business <p>Specifica che ogni macchina con provisioning effettuato nello stesso gruppo di business ha la stessa coppia di chiavi, incluse le macchine con provisioning effettuato su altre prenotazioni quando la macchina ha la stessa risorsa di elaborazione e lo stesso gruppo di business. Dato che le coppie di chiavi sono associate a un gruppo di business, vengono eliminate quando il gruppo di business viene eliminato.</p> ■ Generato automaticamente per macchina <p>Specifica che ogni macchina ha una coppia di chiavi univoca. Questa opzione è il metodo più sicuro perché non vengono condivise coppie di chiavi tra macchine.</p>
Caratteristiche	<p>Selezionare una o più caratteristiche di OpenStack. Una caratteristica di OpenStack è un modello hardware virtuale che definisce le specifiche delle risorse macchina relative a istanze il cui provisioning è stato eseguito in OpenStack. Le caratteristiche sono gestite all'interno del provider di OpenStack e vengono importate durante la raccolta dati.</p>

Scheda **Risorse macchina**

Specificare le impostazioni relative a CPU, memoria e storage per il componente macchina OpenStack.

Tabella 3-26. Scheda **Risorse macchina**

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU che possono essere utilizzate dalle macchine di cui è stato effettuato il provisioning.
Memoria (MB): Minimo e Massimo	Immettere la quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning.
Storage (GB): Minimo e Massimo	Immettere la quantità minima e massima di storage che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning. Quando si utilizza un workflow di provisioning WIM in un blueprint, specificare un valore di storage che tenga conto della dimensione di ciascun disco da utilizzare sulla macchina. Utilizzare il valore totale di tutti i dischi come valore di storage minimo per il componente macchina. Specificare anche la dimensione di ogni disco in modo che sia sufficientemente grande da accogliere il sistema operativo.

Scheda **Proprietà**

Facoltativamente è possibile specificare informazioni relative a proprietà personalizzate e gruppi di proprietà per il componente macchina OpenStack.

Attraverso la scheda **Proprietà** è possibile aggiungere al componente macchina proprietà personalizzate singole e gruppi di proprietà personalizzate. È inoltre possibile aggiungere proprietà personalizzate e gruppi di proprietà all'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint mediante la pagina **Proprietà blueprint**.

È possibile utilizzare la scheda **Proprietà personalizzate** per aggiungere e configurare opzioni di proprietà personalizzate esistenti. vRealize Automation dispone già di alcune proprietà personalizzate ed è inoltre possibile creare definizioni di proprietà.

Tabella 3-27. Impostazioni della scheda **Proprietà > Proprietà personalizzate**

Impostazione	Descrizione
Nome	Consente di specificare il nome di una proprietà personalizzata o selezionare una proprietà personalizzata disponibile dal menu a discesa. Nel menu a discesa vengono elencate solo le proprietà delle quali l'amministratore tenant o di struttura ha creato le definizioni.
Valore	Consente di immettere o modificare un valore da associare al nome della proprietà personalizzata. Ad esempio, impostare il valore su <code>true</code> per consentire agli utenti autorizzati di connettersi alle macchine virtuali mediante SSH.
Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.

Tabella 3-27. Impostazioni della scheda **Proprietà > Proprietà personalizzate** (continua)

Impostazione	Descrizione
Sovrascrivibile	È possibile specificare che il valore di una proprietà può essere sovrascritto dalla persona successiva che utilizza tale proprietà. Se si seleziona Mostra nella richiesta , gli utenti possono modificare i valori delle proprietà quando richiedono elementi del catalogo.
Mostra nella richiesta	È possibile visualizzare il nome e il valore della proprietà per gli utenti quando richiedono il provisioning della macchina. Selezionare l'opzione sovrascrivibile se si desidera che gli utenti forniscano un valore.

È possibile utilizzare la scheda **Gruppi di proprietà** per aggiungere e configurare le impostazioni dei gruppi di proprietà personalizzate esistenti. L'utente può creare i gruppi di proprietà propri o utilizzare gruppi di proprietà creati da altri per lui.

Tabella 3-28. Impostazioni della scheda **Proprietà > Gruppi di proprietà**

Impostazione	Descrizione
Nome	Consente di selezionare un gruppo di proprietà disponibile dal menu a discesa.
Sposta su e Sposta giù	Consente di controllare il livello di precedenza dei gruppi di proprietà in ordine decrescente. Un gruppo di proprietà elencato prima ha la precedenza sui gruppi di proprietà elencati dopo e così via.
Visualizza proprietà	Visualizza le proprietà personalizzate nel gruppo di proprietà selezionato.
Visualizza proprietà unite	Visualizzare le proprietà personalizzate nell'ordine in cui sono presenti nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi, la proprietà compare una volta nell'elenco in base alla sua prima occorrenza.

Utilizzo di proprietà personalizzate della rete

È possibile specificare informazioni relative a rete e sicurezza per componenti macchina diversi da vSphere e blueprint che non contengono NSX utilizzando proprietà personalizzate della rete a livello di componente macchina o blueprint.

I componenti **Rete e sicurezza** sono disponibili solo per l'uso con componenti macchina vSphere. I componenti macchina diversi da vSphere non contengono una scheda **Rete** o **Sicurezza**.

Per i componenti macchina di vSphere con NSX associato, utilizzare le impostazioni di rete, sicurezza e bilanciamento del carico nell'interfaccia utente. Per i componenti macchina senza la scheda **Rete** o **Sicurezza**, è possibile aggiungere proprietà personalizzate di rete e sicurezza, quali ad esempio `VirtualMachine.Network0.Name`, alla relativa scheda **Proprietà** nella tela di progettazione. Le proprietà di rete, sicurezza e bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

È possibile definire le proprietà personalizzate singolarmente o come parte di un gruppo di proprietà esistente utilizzando la scheda **Proprietà** durante la configurazione di un componente macchina nella tela di progettazione. Le proprietà personalizzate definite per un componente macchina si applicano alle macchine di quel tipo di cui si effettua il provisioning dal blueprint.

Per informazioni sulle proprietà personalizzate disponibili, vedere *Guida di riferimento alle proprietà personalizzate*.

Risoluzione dei problemi dei blueprint per cloni e cloni collegati

Quando si crea il blueprint di un clone o di un clone collegato, la macchina o i modelli sono mancanti. È impossibile eseguire il provisioning delle macchine utilizzando il blueprint di cloni condiviso per richiedere le macchine.

Problema

Quando si lavora con blueprint di cloni o cloni collegati si può verificare uno dei seguenti problemi:

- Quando si crea un blueprint di clone collegato, nell'elenco da clonare non compare alcuna macchina o la macchina che si desidera clonare non compare.
- Quando si crea un blueprint di cloni, nell'elenco dei modelli da clonare non compare alcun modello o il modello desiderato non viene visualizzato.
- Quando vengono richieste macchine utilizzando il blueprint di cloni condiviso, il provisioning termina con esito negativo.
- A causa delle tempistiche della raccolta dei dati, nel momento in cui gli utenti creano o modificano blueprint di cloni collegati, viene ancora visualizzato un modello che è stato rimosso.

Tenere presente che i cloni collegati non sono supportati quando viene eseguito il provisioning in SDSR. I cloni collegati vengono creati nello stesso archivio dati dell'elemento principale, ma non vengono ribilanciati tra gli archivi dati del cluster. In questi casi, l'archivio dati principale potrebbe infine riempirsi.

Causa

Le cause possibili dei problemi più frequenti ai blueprint di cloni e cloni collegati sono molteplici.

Per informazioni correlate sulle opzioni **Clona da** e **Clona da snapshot** con **Utilizza snapshot corrente** disponibili quando si creano blueprint, vedere [vSphereImpostazioni dei componenti macchina in vRealize Automation](#).

Tabella 3-29. Cause dei problemi più frequenti ai blueprint di cloni e cloni collegati

Problema	Causa	Soluzione
Macchine mancanti	È possibile creare blueprint di cloni collegati solo utilizzando macchine gestite come amministratore tenant o manager gruppo di business.	<p>Un utente del proprio tenant o gruppo di business deve richiedere una macchina vSphere. È possibile farlo da soli se si rivestono i ruoli appropriati.</p> <p>In questa finestra di dialogo è inoltre possibile visualizzare le macchine non gestite.</p> <p>È possibile che le macchine gestite siano state importate. Non esiste alcun requisito che richieda che le macchine sottoposte a provisioning da vRealize Automation siano visibili in questa finestra di dialogo.</p>
Modelli mancanti	La raccolta dei dati non è riuscita in un determinato endpoint oppure non sono disponibili endpoint per la piattaforma del componente.	<ul style="list-style-type: none"> ■ Se gli endpoint sono in cluster e contengono più risorse di elaborazione, verificare che l'amministratore di IaaS abbia aggiunto il cluster contenente i modelli al gruppo di strutture. ■ Per i nuovi modelli, verificare che il reparto IT abbia collocato i modelli nello stesso cluster incluso nel gruppo di strutture.
Provisioning non riuscito con un blueprint condiviso	Per i blueprint, non è disponibile una convalida che confermi l'esistenza del modello selezionato nella prenotazione utilizzata per il provisioning di una macchina dal blueprint di cloni condiviso.	Prendere in considerazione l'uso di permessi per limitare il blueprint agli utenti che hanno una prenotazione sulla risorsa di elaborazione in cui è presente il modello.

Tabella 3-29. Cause dei problemi più frequenti ai blueprint di cloni e cloni collegati (continua)

Problema	Causa	Soluzione
Provisioning non riuscito con un agente guest	La macchina virtuale potrebbe riavviarsi immediatamente dopo il completamento della personalizzazione del sistema operativo guest, ma prima che gli elementi di lavoro dell'agente guest siano completati, impedendo la riuscita del provisioning. È possibile utilizzare la proprietà personalizzata <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> per aumentare il ritardo.	Assicurarsi di aver aggiunto la proprietà personalizzata <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> . Il valore deve essere nel formato HH:MM:SS. Se il valore non è impostato, il valore predefinito è un minuto (00:01:00).
Il provisioning dei blueprint di cloni o di cloni collegati non riesce poiché non è possibile trovare il modello su cui è basato il clone.	Non è possibile eseguire il provisioning delle macchine da un blueprint clonato da un modello che non esiste più. vRealize Automation esegue periodicamente la raccolta dei dati, ogni 24 ore per impostazione predefinita. Se un modello viene rimosso, la modifica non viene applicata fino alla successiva raccolta dei dati, quindi è possibile creare un blueprint in base a un modello non esistente.	Ridefinire il blueprint utilizzando un modello esistente, quindi richiedere il provisioning. Come precauzione e laddove possibile, eseguire la raccolta dei dati prima di definire il blueprint di cloni o di cloni collegati.

Progettazione di blueprint con impostazioni NSX

Se è stata configurata l'integrazione di vRealize Automation con NSX for vSphere o NSX-T, è possibile utilizzare i componenti rete, sicurezza e bilanciamento del carico per configurare il blueprint per il provisioning delle macchine.

È inoltre possibile aggiungere le seguenti impostazioni di rete e sicurezza di NSX all'intero blueprint:

- **Zona di trasporto**
Contiene le reti utilizzate per la distribuzione di macchine fornite in provisioning.
- **Criterio di prenotazione della rete**
Gestisce le comunicazioni di rete per la distribuzione delle macchine fornite in provisioning.
- **Isolamento app**
Consente solo il traffico interno tra le macchine utilizzate nella distribuzione delle macchine fornite in provisioning.

Per ulteriori informazioni sull'integrazione di vRealize Automation e NSX, consultare l'articolo del blog [vRA and NSX - Intro to Network and Security Automation](#) e visualizzare il contenuto di anteprima della serie di corsi su [networking e sicurezza con vRealize Automation e NSX](#).

Le impostazioni di NSX sono applicabili solo ai tipi di componente macchina vSphere.

Nuovo blueprint e impostazioni della pagina delle proprietà del blueprint con NSX in vRealize Automation

È possibile specificare le impostazioni che si applicano all'intero blueprint vRealize Automation, incluse alcune impostazioni di NSX, utilizzando la pagina **Nuovo blueprint** quando si crea il blueprint. Dopo aver creato il blueprint, è possibile modificare le impostazioni nella pagina **Proprietà blueprint**.

Scheda Generale

Le impostazioni nella scheda Generale si applicano all'intero blueprint di vRealize Automation.

Tabella 3-30. Impostazioni della scheda **Generale**

Impostazione	Descrizione
Nome	Immettere il nome del blueprint.
Identificatore	Il campo dell'identificatore viene compilato automaticamente in base al nome immesso. È possibile modificare il campo, ma dopo aver salvato il blueprint il campo non potrà più essere modificato. Gli identificatori sono permanenti e univoci all'interno del tenant. È possibile utilizzarli per interagire in modo programmatico con i blueprint e creare binding di proprietà.
Descrizione	Testo che riepiloga il blueprint a vantaggio di altri architetti. Questa descrizione viene anche visualizzata per gli utenti nel modulo di richiesta.
Limite distribuzione	Specificare il numero massimo di distribuzioni che è possibile creare quando questo blueprint viene utilizzato per il provisioning delle macchine.
Giorni di lease: Minimo e Massimo	Immettere un valore minimo e massimo per consentire agli utenti di scegliere da un intervallo di lunghezze di lease. Al termine del lease, la distribuzione viene eliminata o archiviata. Se non si specifica un valore minimo o massimo, il lease viene impostato senza una scadenza. Immettere le informazioni sul lease per le macchine nel blueprint di vRealize Automation, non nell'applicazione dell'endpoint di origine. Se si specificano le informazioni sul lease in un'applicazione esterna, non vengono riconosciute in vRealize Automation.
Giorni di archiviazione	Invece di eliminare le distribuzioni immediatamente alla scadenza del lease, è possibile specificare un periodo di archiviazione temporanea. Specificare 0 per eliminare la distribuzione alla scadenza del suo lease. Il periodo di archiviazione inizia il giorno in cui scade il lease. Al termine del periodo di archiviazione, la distribuzione viene eliminata. Il valore predefinito è 0.
Propaga aggiornamenti alle distribuzioni esistenti	Gli intervalli minimo-massimo estesi per CPU, memoria o storage vengono inseriti nelle distribuzioni attive di cui è stato eseguito il provisioning dal blueprint. Il nuovo intervallo deve includere l'intero vecchio intervallo. Ad esempio, per un valore originale minimo di 32 e massimo di 128 (32, 128), una modifica come (16, 128) o (32, 256) o (2, 1000) può essere applicata dopo la riconfigurazione o la scalabilità orizzontale, mentre una modifica di (33, 512) o (4, 64) non può.

Scheda Impostazioni NSX

Se è stato configurato NSX, quando si crea o si modifica un blueprint è possibile specificare le impostazioni di NSX relative a zona di trasporto, criterio di prenotazione della rete e isolamento app. Queste impostazioni sono disponibili nella scheda **Impostazioni NSX** nelle pagine **Blueprint** e **Proprietà blueprint**.

Per informazioni sull'applicazione NSX, vedere la [documentazione di VMware NSX Data Center for vSphere](#) o la [documentazione di VMware NSX-T Data Center](#).

Tabella 3-31. Impostazioni della scheda **Impostazioni NSX**

Impostazione	Descrizione
Zona di trasporto	<p>Selezionare una zona di trasporto di NSX esistente per contenere la rete o le reti che possono essere utilizzate dalla distribuzione della macchina di cui è stato eseguito il provisioning.</p> <p>Una zona di trasporto definisce quali cluster possono rientrare nelle reti. Quando si esegue il provisioning di macchine, se è specificata una zona di trasporto in una prenotazione e in un blueprint, i valori della zona di trasporto devono coincidere. Sono disponibili solo le zone di trasporto applicabili al tenant corrente.</p> <p>Per i blueprint che contengono oggetti di rete e di sicurezza su richiesta di NSX for vSphere o NSX-T, è necessaria una zona di trasporto.</p> <p>Per ulteriori informazioni, vedere Applicazione di una zona di trasporto NSX a un blueprint.</p> <p>Specificare una zona di trasporto appropriata per una distribuzione di NSX for vSphere o NSX-T.</p>
Criteri di prenotazione della rete	<p>Per NSX for vSphere, selezionare un criterio di prenotazione della rete per stabilire dove posizionare il dispositivo edge o il DLR nella distribuzione.</p> <p>Quando vRealize Automation esegue il provisioning di una macchina con servizi di rete di instradamento o NAT, esegue il provisioning di un gateway instradato come router di rete. L'Edge o il gateway instradato è una macchina di gestione che consuma risorse di elaborazione. Gestisce inoltre le comunicazioni di rete per tutte le macchine nella distribuzione. La prenotazione utilizzata per eseguire il provisioning dell'Edge o del gateway instradato determina la rete esterna utilizzata per il NAT e gli indirizzi IP virtuali del bilanciamento del carico. È consigliabile utilizzare cluster di gestione separati per macchine di gestione quali gli Edge NSX.</p> <p>Per NSX-T, selezionare un criterio di prenotazione della rete che consente di determinare dove posizionare il router logico di livello 0 nella distribuzione del blueprint.</p> <p>Per ulteriori informazioni, vedere Applicazione di un criterio di prenotazione della rete di NSX a un blueprint.</p> <p>Specificare un criterio di prenotazione appropriato per una distribuzione di NSX for vSphere o NSX-T. I cluster distribuiti dal blueprint possono essere gestiti da NSX for vSphere o NSX-T.</p>
Isolamento app	<p>Selezionare la casella di controllo Isolamento app per utilizzare il criterio di protezione isolamento app configurato in NSX for vSphere. Il criterio di isolamento app viene applicato a tutti i componenti delle macchine vSphere nel blueprint. È possibile aggiungere tag e gruppi di sicurezza per permettere a vRealize Orchestrator di aprire la rete isolata e consentire percorsi di ingresso e uscita aggiuntivi dell'isolamento app.</p> <p>Per ulteriori informazioni, vedere Applicazione dell'isolamento app NSX a un blueprint.</p>

Scheda **Proprietà**

Le proprietà personalizzate aggiunte a livello del blueprint vengono applicate all'intero blueprint, inclusi tutti i componenti. Per informazioni sull'ordine di precedenza, vedere *Guida di riferimento alle proprietà personalizzate*.

Tabella 3-32. Impostazioni della scheda **Proprietà**

Scheda	Impostazione	Descrizione
Gruppi di proprietà		I gruppi di proprietà sono gruppi riutilizzabili che semplificano l'aggiunta di proprietà personalizzate ai blueprint.
	Aggiungi	<p>Aggiungere uno o più gruppi di proprietà esistenti e applicarli all'intero blueprint.</p> <p>Sono forniti i seguenti gruppi di proprietà correlati ai contenitori:</p> <ul style="list-style-type: none"> ■ Proprietà dell'host del contenitore con autenticazione mediante certificato ■ Proprietà dell'host del contenitore con autenticazione mediante utente/password
	Sposta su /Sposta giù	Controllano l'ordine di precedenza di ciascun gruppo di proprietà rispetto agli altri in base alle priorità desiderate. Il primo gruppo dell'elenco ha la priorità maggiore e le sue proprietà personalizzate hanno la precedenza rispetto a tutte le altre. È inoltre possibile scorrere per riordinare.
	Visualizza proprietà	Consente di visualizzare le proprietà personalizzate nel gruppo di proprietà selezionato.
	Visualizza proprietà unite	Se una proprietà personalizzata è inclusa in più di un gruppo di proprietà, la precedenza è assegnata al valore incluso nel gruppo di proprietà con la priorità più elevata.
Proprietà personalizzate		È possibile aggiungere singole proprietà personalizzate invece di gruppi di proprietà.
	Nuovo	Aggiungere una singola proprietà personalizzata e applicarla all'intero blueprint.
	Nome	Specificare il nome della proprietà. Per un elenco delle proprietà personalizzate e delle relative definizioni, vedere <i>Guida di riferimento alle proprietà personalizzate</i> .
	Valore	Immettere il valore della proprietà personalizzata.

Tabella 3-32. Impostazioni della scheda **Proprietà** (continua)

Scheda	Impostazione	Descrizione
	Codificato	Codificare il valore della proprietà, ad esempio se il valore è una password.
	Sovrascrivibile	L'utente del blueprint può sovrascrivere il valore della proprietà. Se si seleziona Mostra nella richiesta , gli utenti possono visualizzare e modificare i valori delle proprietà quando richiedono elementi del catalogo.
	Mostra nella richiesta	Il nome e il valore della proprietà sono visibili per gli utenti nel modulo di richiesta di provisioning. Selezionare Sovrascrivibile se si consente agli utenti di fornire un valore.

Applicazione di una zona di trasporto NSX a un blueprint

Gli amministratori di NSX possono creare zone di trasporto per controllare l'uso delle reti da parte dei cluster.

Una zona di trasporto controlla gli host che possono essere raggiunti da uno switch logico e può comprendere uno o più cluster di host, inclusi gli host presenti in più vCenter.

Per i blueprint contenenti una rete NAT su richiesta o una rete instradata su richiesta, specificare una zona di trasporto che includa le reti che devono essere utilizzate dalla distribuzione delle macchine con provisioning.

Per i blueprint che includono un endpoint NSX-T, è necessario specificare una zona di trasporto.

La zona di trasporto specificata per il blueprint deve corrispondere a quella specificata per la prenotazione utilizzata dal blueprint. Vedere [Applicazione di un criterio di prenotazione della rete di NSX a un blueprint](#).

- Se il blueprint non utilizza componenti su richiesta di NSX-T, il valore della zona di trasporto viene ignorato.
- NSX-T supporta più zone di trasporto sovrapposte e più zone di trasporto VLAN.
- Una zona di trasporto è necessaria per creare uno switch logico. Gli switch logici vengono creati all'interno delle zone di trasporto.
- Durante la creazione di un blueprint vengono espresse solo le zone di trasporto del tenant corrente. Le zone di trasporto diventano disponibili se vengono utilizzate da una prenotazione nel tenant corrente.

Applicazione di un criterio di prenotazione della rete di NSX a un blueprint

Durante il provisioning del blueprint, il criterio di prenotazione consente di raggruppare le prenotazioni che possono essere prese in considerazione per la distribuzione. In ogni prenotazione sono contenute informazioni di networking.

Se nel criterio di prenotazione è presente una zona di trasporto, quest'ultima deve corrispondere alla zona di trasporto specificata nel blueprint. Vedere [Applicazione di una zona di trasporto NSX a un blueprint](#).

È possibile applicare un criterio di prenotazione della rete a livello di blueprint utilizzando la pagina **Nuovo blueprint** o **Proprietà blueprint**.

Considerazioni su NSX for vSphere

Per NSX for vSphere, questo criterio di prenotazione consente di determinare il posizionamento dell'edge NSX o la selezione del router logico distribuito (DLR) associato alle reti su richiesta. Questo criterio è inoltre chiamato criterio di prenotazione del gateway instradato o criterio di prenotazione dell'edge.

Ad esempio, per NSX for vSphere, un profilo di rete NAT e il bilanciamento del carico consentono di abilitare vRealize Automation per la distribuzione di un gateway di servizi edge di NSX. Un profilo di rete instradato utilizza un router distribuito logico (DLR, Logical Distributed Router) di NSX for vSphere. Il DLR deve essere creato in NSX prima che possa essere utilizzato da vRealize Automation. vRealize Automation non può creare DLR. Dopo la raccolta dei dati, vRealize Automation può utilizzare il router DLR per il provisioning delle macchine virtuali.

NSX Edge fornisce servizi di instradamento e la connettività a reti esterne alla distribuzione di NSX. Il gateway NSX Edge connette subnet isolate a reti (uplink) condivise fornendo servizi gateway comuni, quali NAT e il routing dinamico. Le distribuzioni comuni di NSX Edge includono ambienti multi-tenant in cui NSX Edge crea limiti virtuali per ciascun tenant.

vRealize Automation esegue il provisioning di un gateway instradato, ad esempio un gateway di servizi Edge, per reti NAT e per bilanciamenti del carico. Per le reti instradate, vRealize Automation utilizza i router distribuiti esistenti.

La prenotazione utilizzata per eseguire il provisioning dell'edge o del gateway instradato determina i profili di rete NAT, privati o instradati disponibili e gli indirizzi IP virtuali del bilanciamento del carico.

Considerazioni su NSX-T

Per NSX-T, questo criterio di prenotazione consente di selezionare un router logico di livello 0 utilizzato per la distribuzione.

I router logici di livello 0 dispongono di porte downlink per la connessione a router logici di livello 1 e di porte uplink per la connessione a reti esterne. vRA connette un router logico di livello 1 a un router logico di livello 0 per l'accesso al router fisico di livello superiore e assegna un cluster edge a un router logico per eseguire i servizi NAT e di bilanciamento del carico.

Applicazione dell'isolamento app NSX a un blueprint

È possibile abilitare l'isolamento app per consentire soltanto il traffico interno tra i componenti di cui viene eseguito il provisioning dal blueprint.

Un criterio di isolamento app di NSX agisce come un firewall per bloccare tutto il traffico in ingresso e uscita da e verso le macchine fornite in provisioning nella distribuzione. Quando si specifica un criterio di protezione di isolamento app di NSX definito, le macchine di cui viene eseguito il provisioning dal blueprint possono comunicare tra loro ma non possono connettersi all'esterno del firewall.

Se viene specificata una regola di isolamento app e vengono specificate anche regole di sicurezza utilizzando gruppi di sicurezza inclusi nel blueprint, l'impostazione relativa all'isolamento app è la regola che viene elaborata per ultima durante la distribuzione del blueprint.

È possibile applicare l'isolamento app al livello di blueprint utilizzando la pagina **Nuovo blueprint** o **Proprietà blueprint**.

Considerazioni su NSX for vSphere

I componenti di cui è stato eseguito il provisioning vengono inseriti in un gruppo di sicurezza, che viene isolato tramite le regole del firewall. Per l'abilitazione è necessario configurare l'endpoint vSphere in modo che supporti l'isolamento app di NSX.

Quando si utilizza un criterio di isolamento app di NSX for vSphere, è consentito solo il traffico interno tra macchine fornite in provisioning dal blueprint. Quando si richiede il provisioning, viene creato un gruppo di sicurezza per le macchine da sottoporre a provisioning. In NSX for vSphere viene creato un criterio di isolamento app che viene applicato al gruppo di sicurezza. Le regole del firewall sono definite nel criterio di sicurezza per consentire solo il traffico interno tra i componenti nella distribuzione.

quando si esegue il provisioning con un blueprint che utilizza sia un bilanciamento del carico NSX for vSphere edge che un criterio di protezione di isolamento app di NSX for vSphere, il bilanciamento del carico fornito dinamicamente in provisioning non viene aggiunto al gruppo di sicurezza. Questo aspetto impedisce al bilanciamento del carico di comunicare con le macchine per le quali è deputato a gestire le connessioni. Dato che gli edge sono esclusi dal firewall distribuito NSX for vSphere, non possono essere aggiunti ai gruppi di sicurezza. Per garantire un corretto funzionamento del bilanciamento del carico, utilizzare un altro gruppo di sicurezza o criterio di protezione che permetta il bilanciamento del carico del traffico richiesto nelle macchine virtuali dei componenti.

Il criterio di isolamento app ha una precedenza inferiore rispetto ad altri criteri di protezione in NSX for vSphere. Ad esempio, se la distribuzione fornita in provisioning contiene una macchina componente Web e una macchina componente App, e la macchina componente Web ospita un servizio Web, il servizio deve consentire il traffico in ingresso sulle porte 80 e 443. In questo caso,

gli utenti devono creare un criterio di protezione Web in NSX for vSphere con regole firewall definite per consentire il traffico in ingresso su queste porte. In vRealize Automation, gli utenti devono applicare il criterio di protezione Web sul componente Web della distribuzione di macchine fornite in provisioning.

Nota Se un blueprint contiene un bilanciamento del carico ed è abilitato l'isolamento app, i VIP del bilanciamento del carico vengono aggiunti come set di IP al gruppo di sicurezza dell'isolamento app. Se un blueprint contiene un gruppo di sicurezza su richiesta associato a un livello macchina associato a un bilanciamento del carico, il gruppo di sicurezza su richiesta include il livello macchina, il set di IP e i VIP.

Se la macchina componente Web deve accedere alla macchina componente App utilizzando un bilanciamento del carico sulle porte 8080 e 8443, oltre alle regole firewall esistenti che consentono il traffico in ingresso alle porte 80 e 443 il criterio di protezione Web dovrebbe includere anche regole firewall per consentire il traffico in ingresso a queste porte.

Considerazioni su NSX-T

I componenti di cui è stato eseguito il provisioning vengono inseriti in un gruppo NS, che viene isolato tramite le regole del firewall. Per l'abilitazione è necessario configurare l'endpoint vSphere in modo che supporti l'isolamento app di NSX.

NSX-T supporta la creazione di una topologia di router logici di livello 2: il router logico di livello 0 è il router di livello superiore e il router logico di livello 1 è il router di livello inferiore. Questa struttura fornisce all'amministratore del provider e agli amministratori tenant il controllo completo dei propri servizi e criteri. In NSX-T gli amministratori controllano e configurano il routing e i servizi di livello 0, mentre gli amministratori tenant controllano e configurano il routing e i servizi di livello 1.

Configurazione delle impostazioni dei componenti rete e sicurezza in vRealize Automation

vRealize Automation supporta reti virtualizzate basate sulla piattaforma NSX. Sono inoltre supportate reti di Contenitori per vRealize Automation integrate.

Per integrare rete e sicurezza NSX con vRealize Automation, è necessario che un amministratore IaaS configuri gli endpoint vSphere e NSX. vRealize Automation supporta NSX for vSphere e NSX-T.

Per informazioni sulla preparazione esterna, vedere *Configurazione di vRealize Automation*.

È possibile creare profili di rete da utilizzare per definire le impostazioni di rete nelle prenotazioni e nel blueprint. I profili di rete esterna definiscono le reti fisiche esistenti. Profili di rete instradati e NAT su richiesta possono generare switch logici NSX e impostazioni di routing appropriate per un nuovo percorso di rete.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere e NSX-T. Per informazioni sulla configurazione di NSX, vedere *Administration Guide* nella [documentazione del prodotto NSX for vSphere](#) o nella [documentazione del prodotto NSX-T](#), a seconda dell'applicazione utilizzata.

Per i componenti macchina di vSphere con NSX associato, utilizzare le impostazioni di rete, sicurezza e bilanciamento del carico nell'interfaccia utente. Per i componenti macchina senza la scheda **Rete** o **Sicurezza**, è possibile aggiungere proprietà personalizzate di rete e sicurezza, quali ad esempio `VirtualMachine.Network0.Name`, alla relativa scheda **Proprietà** nella tela di progettazione. Le proprietà di rete, sicurezza e bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Se viene specificato un profilo di rete in una prenotazione e un blueprint, i valori del blueprint hanno la precedenza.

In base alla risorsa di elaborazione, è possibile selezionare una zona di trasporto che identifichi un endpoint vSphere. Una zona di trasporto definisce gli host e i cluster che possono essere associati agli switch logici creati all'interno della zona. Una zona di trasporto può abbracciare più cluster vSphere. Il blueprint e le prenotazioni utilizzate nel provisioning devono avere la stessa impostazione della zona di trasporto. Le zone di trasporto sono definite negli ambienti NSX.

È possibile configurare le impostazioni di sicurezza specificando le informazioni in una prenotazione, in un blueprint o in uno script dell'agente guest. Se le macchine richiedono un agente guest, aggiungere una regola di sicurezza alla prenotazione o al blueprint.

È inoltre possibile aggiungere un componente di rete Contenitori a un blueprint.

Per informazioni correlate alla configurazione di rete e sicurezza per NSX-T in vRealize Automation, vedere il blog VMware [Networking e sicurezza dell'applicazione con vRealize Automation e NSX-T](#).

Controllo dell'accesso al tenant per gli oggetti di sicurezza in vRealize Automation

È possibile controllare la disponibilità cross-tenancy degli oggetti di sicurezza di NSX in vRealize Automation.

Quando si crea un oggetto di sicurezza NSX, la sua disponibilità predefinita può essere globale, il che significa che l'oggetto è disponibile in tutti i tenant per cui l'endpoint associato ha una prenotazione, oppure nascosta per tutti gli utenti ad eccezione dell'amministratore.

La disponibilità degli oggetti di sicurezza in un tenant dipende dal fatto che l'endpoint associato disponga o meno di una prenotazione o di un criterio di prenotazione nel tenant.

NSX non include gruppi di sicurezza. Tuttavia, è possibile controllare la disponibilità di gruppi di sicurezza in vRealize Automation utilizzando la proprietà personalizzata `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects`.

Per impostazione predefinita, i nuovi oggetti di sicurezza sono disponibili per tutti i tenant per gli endpoint NSX associati in cui si dispone di una prenotazione. Se l'endpoint non ha alcuna prenotazione nel tenant attivo, gli oggetti di sicurezza non sono disponibili nel tenant attivo.

Se non si imposta la proprietà personalizzata

`VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` negli endpoint NSX, i nuovi oggetti di sicurezza vengono impostati su Globale per impostazione predefinita. Gli oggetti di sicurezza che esistevano prima di eseguire l'aggiornamento a questa versione di vRealize Automation vengono impostati su Globale indipendentemente dalla proprietà personalizzata.

Nota Quando si esegue l'aggiornamento a questa versione di vRealize Automation, i gruppi di sicurezza della versione precedente vengono impostati su Globale per impostazione predefinita. I gruppi di sicurezza e i tag di sicurezza esistenti sono disponibili in tutti i tenant in cui l'endpoint associato ha una prenotazione.

È possibile nascondere i nuovi gruppi di sicurezza per impostazione predefinita aggiungendo la proprietà personalizzata `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` all'endpoint NSX associato. Questa impostazione diventerà effettiva alla successiva raccolta dati nell'endpoint NSX e verrà applicata solo ai nuovi oggetti di sicurezza.

È inoltre possibile modificare l'impostazione del tenancy di un oggetto di sicurezza esistente a livello di programmazione. Ad esempio, se un gruppo di sicurezza è impostato su Globale, è possibile modificare la disponibilità del tenant di un oggetto di sicurezza utilizzando l'impostazione ID tenant dell'endpoint NSX associato nella REST API di vRealize Automation o in vRealize CloudClient. Le impostazioni ID tenant disponibili per l'endpoint NSX sono le seguenti:

- "`<global>`" - l'oggetto di sicurezza è disponibile per tutti i tenant. Questa è l'impostazione predefinita per gli oggetti di sicurezza esistenti dopo l'aggiornamento a questa versione e per tutti i nuovi oggetti di sicurezza creati.
- "`<unscoped>`" - l'oggetto di sicurezza non è disponibile per alcun tenant. Solo l'amministratore di sistema può accedere all'oggetto di sicurezza. Questa è un'impostazione ideale quando si definiscono oggetti di sicurezza che verranno assegnati a un tenant specifico.
- "`tenant_id_name`" - l'oggetto di sicurezza è disponibile solo per un singolo tenant denominato.

È possibile utilizzare la REST API di vRealize Automation o gli strumenti di vRealize CloudClient per assegnare a un tenant denominato il parametro ID tenant (*tenantId*) degli oggetti di sicurezza associati a un endpoint specifico.

Per informazioni sui comandi REST API di vRealize Automation, vedere *Riferimento API di vRealize Automation* nella sezione [Documentazione relativa all'API di vRealize Automation](#) per la versione vRealize Automation 7.x. Per ulteriori informazioni, consultare *Guida alla programmazione di vRealize Automation* nella sezione [Documentazione relativa all'API di vRealize Automation](#) per la versione vRealize Automation 7.x.

Per informazioni su vRealize CloudClient, vedere <https://code.vmware.com/web/dp/tool/cloudclient>.

Informazioni sulle topologie di distribuzione di NSX-T per i servizi di rete, la sicurezza e le configurazioni del bilanciamento del carico

È possibile stabilire e utilizzare varie tipologie di distribuzione in base alla configurazione della rete e della sicurezza di NSX-T e ai componenti di bilanciamento del carico nel blueprint di vRealize Automation.

Rete e sicurezza

■ Reti instradate

Se si associa un componente di rete instradata di NSX-T a un componente macchina di vSphere nel blueprint, viene eseguito il provisioning della seguente topologia in NSX-T:

- Viene creato un router di livello 1.
- Viene creato uno switch logico.
- Il router di livello 1 viene collegato allo switch logico.
- Le route instradate specifiche vengono indicate nel router di livello 1.

■ Reti NAT (IP statico)

Se una rete NAT NSX-T viene collegata a un componente macchina di vSphere nel blueprint, viene eseguito il provisioning della seguente topologia in NSX-T:

- Viene creato un router di livello 1.
- Viene creato uno switch logico.
- Il router di livello 1 viene collegato al cluster edge.
- Il router di livello 1 viene collegato a un router di livello 0. Il router di livello 0 viene selezionato dalla prenotazione.
- Il router di livello 1 viene collegato allo switch logico.
- Tutte le route NAT vengono indicate nel router di livello 1.
- Viene assegnato un indirizzo IP esterno a ciascuna rete NAT dal profilo di rete esterno che supporta il profilo di rete NAT su richiesta. Questo IP viene utilizzato per le regole SNAT e DNAT.

■ Reti NAT (DHCP)

Se una rete NAT NSX-T con il protocollo DHCP viene collegata a un componente macchina di vSphere nel blueprint, viene eseguito il provisioning della seguente topologia in NSX-T:

- Viene creato un router di livello 1.
- Viene creato uno switch logico.
- Il router di livello 1 viene collegato al cluster edge.
- Il router di livello 1 viene collegato a un router di livello 0. Il router di livello 0 viene selezionato dalla prenotazione.
- Il router di livello 1 viene collegato allo switch logico.
- Viene eseguito il provisioning di un server DHCP con un pool di IP.
- Tutte le route NAT vengono indicate nel router di livello 1.

■ Isolamento app

Se è necessario l'isolamento app per un blueprint con componenti NSX-T, viene eseguito il provisioning della topologia seguente in NSX-T:

Nota È possibile configurare l'isolamento app per il blueprint nella pagina Proprietà blueprint quando si crea o modifica il blueprint.

- Viene creato un componente NSGroup.
- Viene creata una sezione firewall, con le regole di isolamento del firewall.
- Le macchine nel blueprint vengono aggiunte al componente NSGroup di isolamento app mediante tag.
- Il VIP del bilanciamento del carico e l'indirizzo IP esterno per le reti NAT nel set di IP vengono aggiunti al componente NSGroup dell'isolamento app.

Per supportare i componenti NSGroup dell'isolamento app, è necessario connettere le macchine a reti opache.

■ Componenti NSGroup esistenti

Se si associa un componente NSGroup esistente a un componente macchina di vSphere nel blueprint, viene eseguito il provisioning della seguente topologia in NSX-T:

- Le macchine collegate a NSGroup vengono aggiunte a NSGroup in NSX-T utilizzando i tag come criterio di appartenenza.

Per supportare i componenti NSGroup esistenti, è necessario connettere le macchine a reti opache.

Bilanciamento del carico

Le seguenti topologie sono supportate per il bilanciamento del carico in una distribuzione di blueprint di NSX-T:

- One-arm in una rete su richiesta NAT.
- One-arm in una rete su richiesta instradata.
- One-arm in una rete esterna (esistente).
- Two-arm, uno nel NAT e uno nella rete esterna.
- Two-arm, uno nella rete instradata e uno nella rete esterna.

Se il bilanciamento del carico di NSX-T viene aggiunto al blueprint, nella distribuzione viene eseguito il provisioning della seguente topologia oltre alle topologie di rete:

- Per tutte le topologie, tranne dove il bilanciamento del carico è in una distribuzione one-arm in una rete esterna:
 - Viene creato un singolo servizio di bilanciamento del carico anche se sono presenti più componenti del bilanciamento del carico nel blueprint.
 - Il servizio di bilanciamento del carico viene collegato al router di livello 1 per la distribuzione. Il router di livello 1 viene creato su richiesta.

- Per tutte le topologie in cui il bilanciamento del carico è in una distribuzione one-arm in una rete esterna:
 - La rete esterna specificata nella prenotazione deve essere una rete opaca VC (switch logico NSX-T).
 - Il router di livello 1 deve essere presente e collegato alla rete esterna (switch logico NSX-T).
 - Se il router di livello 1 non esiste già, il server di bilanciamento del carico viene creato su richiesta e collegato al router di livello 1. In caso contrario, viene utilizzato un bilanciamento del carico già esistente.
- La route VIP viene annunciata, a meno che il VIP non si trovi in una rete privata NAT.
- Vengono creati uno o più server virtuali nel servizio di bilanciamento del carico.
Esistono limitazioni al numero di server virtuali per servizio di bilanciamento del carico, in base alle dimensioni del bilanciamento del carico.
- Per ogni server virtuale viene creato un profilo di applicazione del server virtuale.
- Per ogni server virtuale con opzioni di persistenza configurate viene creato un profilo di persistenza del server virtuale.
- Viene configurato un pool di iscrizione che contiene l'IP statico di ogni macchina nel pool di iscrizione.
- Viene creato un solo servizio di bilanciamento del carico indipendentemente dal numero di componenti nel blueprint.
- Viene creato e configurato un monitor di integrità per ogni pool di membri.

Per i server virtuali con supporto HTTPS, a differenza del bilanciamento del carico in NSX for vSphere, non è supportato il passthrough SSL nel bilanciamento del carico di NSX-T. vRealize Automation consente di configurare il server virtuale di bilanciamento del carico per interrompere SSL a livello del bilanciamento del carico e di utilizzare HTTP normale dal bilanciamento del carico ai membri del pool. Il nome del certificato SSL e il nome del profilo del client SSL, che devono essere entrambi presenti in NSX-T, devono essere specificati quando si configura un server virtuale con HTTPS. È possibile importare i certificati nel gestore di attendibilità di NSX-T.

Quando più componenti di NSX-T sono presenti nel blueprint, il router logico di livello 1 è condiviso tra tutti i componenti e viene configurato di conseguenza. L'ID del router logico di livello 1 esterno viene visualizzato nella vista Dettagli per ciascun componente nella pagina Distribuzioni di vRealize Automation.

Uso dei componenti di rete di NSX for vSphere in un blueprint vRealize Automation

È possibile aggiungere uno o più componenti rete NSX for vSphere alla tela di progettazione e configurare le loro impostazioni per i componenti macchina vSphere in un blueprint vRealize Automation.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere. Per informazioni sulla configurazione di NSX for vSphere, vedere *NSX Administration Guide* nella [documentazione del prodotto NSX for vSphere](#).

Aggiunta di un componente di rete esistente per NSX for vSphere

È possibile aggiungere un componente di rete di NSX for vSphere esistente alla tela di progettazione in preparazione per associare le sue impostazioni a uno o più componenti macchina vSphere nel blueprint.

È possibile utilizzare un componente rete esistente per aggiungere una rete NSX for vSphere alla tela di progettazione e configurare le sue impostazioni per l'uso con i componenti macchina vSphere e i componenti Software o XaaS che si riferiscono a vSphere.

Quando si associa un componente di rete esistente o un componente di rete su richiesta a un componente macchina, insieme a quest'ultimo vengono archiviate le informazioni sulla NIC. Le informazioni del profilo di rete specificato vengono memorizzate insieme al componente rete.

È possibile aggiungere più componenti di rete e sicurezza alla tela di progettazione.

Per i componenti macchina di vSphere con NSX associato, utilizzare le impostazioni di rete, sicurezza e bilanciamento del carico nell'interfaccia utente. Per i componenti macchina senza la scheda **Rete** o **Sicurezza**, è possibile aggiungere proprietà personalizzate di rete e sicurezza, quali ad esempio `VirtualMachine.Network0.Name`, alla relativa scheda **Proprietà** nella tela di progettazione. Le proprietà di rete, sicurezza e bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Durante la creazione di un blueprint vengono esposti solo i profili di rete applicabili al tenant corrente. In particolare, i profili di rete vengono resi disponibili se nel tenant corrente è presente almeno una prenotazione che ha almeno una rete assegnata al profilo.

Prerequisiti

- Creare e configurare le impostazioni di rete per NSX. Vedere l'elenco di controllo per la configurazione di NSX in *Configurazione di vRealize Automation* e la guida di amministrazione di *NSX for vSphere* nella [documentazione del prodotto NSX for vSphere](#).
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Creare un profilo di rete.
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **Rete esistente** nella tela di progettazione.

- 3 Fare clic nella casella di testo **Rete esistente** e selezionare un profilo di rete esistente.

I valori di descrizione, subnet mask e gateway vengono compilati in base al profilo di rete selezionato.

- 4 (Facoltativo) Fare clic sulla scheda **DNS/WINS**.

- 5 (Facoltativo) Specificare le impostazioni di DNS e WINS per il profilo di rete.

- DNS primario
- DNS secondario
- Suffisso DNS
- WINS preferito
- WINS alternativo

Non è possibile cambiare le impostazioni di DNS e WINS per una rete esistente.

- 6 (Facoltativo) Fare clic sulla scheda **Intervalli IP**.

Vengono visualizzati l'intervallo o gli intervalli di indirizzi IP specificati nel profilo di rete. È possibile cambiare l'ordine e la visualizzazione delle colonne. Per le reti NAT è possibile anche cambiare i valori dell'intervallo di indirizzi IP.

- 7 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Operazioni successive

È possibile aggiungere impostazioni di rete nella scheda **Rete** di un componente macchina vSphere.

Aggiunta di un componente di rete privato per NSX for vSphere in vRealize Automation

È possibile aggiungere un componente di rete di NSX for vSphere privato alla tela di progettazione per associare le sue impostazioni a uno o più componenti macchina vSphere nel blueprint vRealize Automation.

Durante la creazione di un blueprint, vengono esposti solo i profili di rete applicabili al tenant corrente.

Questa opzione di rete privata è disponibile solo per NSX for vSphere. Non è disponibile per NSX-T.

Prerequisiti

- Creare e configurare le impostazioni di rete per NSX. Vedere l'elenco di controllo per la configurazione di NSX in *Configurazione di vRealize Automation* e la guida di amministrazione di *NSX for vSphere* nella [documentazione del prodotto NSX for vSphere](#).

- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.

Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.

- Creare un profilo di rete.
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente della rete privata su richiesta nella tela di progettazione.
- 3 Per etichettare in modo univoco un componente nella tela di progettazione, immettere il nome del componente nella casella di testo **ID**.
- 4 Selezionare un profilo di rete esistente appropriato dal menu a discesa **Profilo di rete principale**.
- 5 (Facoltativo) Immettere una descrizione del componente nella casella di testo **Descrizione**.
- 6 (Facoltativo) Fare clic sulla scheda **DNS/WINS**.
- 7 (Facoltativo) Specificare le impostazioni di DNS e WINS per il profilo di rete.
 - DNS primario
 - DNS secondario
 - Suffisso DNS
 - WINS preferito
 - WINS alternativo

Non è possibile cambiare le impostazioni di DNS e WINS per una rete esistente.

- 8 Fare clic sulla scheda **Intervalli IP**.
 - a Immettere l'indirizzo IP iniziale nella casella di testo **Inizio intervallo IP**.
 - b Immettere l'indirizzo IP iniziale nella casella di testo **Inizio intervallo IP**.
- 9 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Creazione e utilizzo di regole NAT per NSX for vSphere

È possibile aggiungere regole NAT a un componente di rete NAT di tipo One-to-Many in un blueprint quando il componente di rete NAT è associato a un componente della macchina vSphere non di cluster o a un componente del bilanciamento del carico NSX for vSphere su richiesta.

È possibile definire regole NAT per qualsiasi protocollo supportato da NSX for vSphere oppure mappare una porta o un intervallo di porte dall'indirizzo IP esterno di un Edge a un indirizzo IP privato nel componente di rete NAT.

- Componente della macchina vSphere

È possibile creare regole NAT per un componente di rete NAT di tipo One-to-Many associato a un componente della macchina vSphere non di cluster.

Ad esempio, se due macchine sono associate a un componente di rete NAT di tipo One-to-Many nel blueprint, è possibile definire una regola NAT che consente alla porta 443 nell'IP esterno di connettersi alle macchine attraverso la porta 80 nella rete NAT mediante protocollo TCP.

- Componente del bilanciamento del carico NSX for vSphere

È possibile creare regole NAT per un componente di rete NAT di tipo One-to-Many associato alla rete VIP di un componente del bilanciamento del carico NSX for vSphere.

Ad esempio, se il componente della rete NAT viene associato a un componente del bilanciamento del carico che sta bilanciando il carico di tre macchine, è possibile definire una regola NAT che consente alla porta 90 nell'IP esterno di connettersi al VIP del bilanciamento del carico attraverso la porta 80 nella rete NAT mediante protocollo UDP.

È possibile creare un numero qualsiasi di regole NAT ed è possibile controllarne l'ordine di elaborazione.

I seguenti elementi non sono supportati per le regole NAT:

- NIC non incluse nella rete corrente
- NIC configurate in modo da ottenere indirizzi IP mediante DHCP
- Cluster di macchine

Per aggiungere regole NAT a un componente di una rete NAT in un blueprint, vedere [Aggiunta di un componente di rete instradata o NAT su richiesta in vRealize Automation](#).

Per informazioni correlate sull'utilizzo di regole NAT, consultare articoli pubblici quali ad esempio questo [post del blog di vmwarelab](#).

Aggiunta di un componente di rete instradata o NAT su richiesta in vRealize Automation

È possibile aggiungere un componente di rete NAT su richiesta NSX for vSphere o un componente di rete instradata su richiesta NSX for vSphere alla tela di progettazione in preparazione per associarne le impostazioni a uno o più componenti macchina vSphere nel blueprint vRealize Automation.

Quando si associa un componente di rete esistente o un componente di rete su richiesta a un componente macchina, insieme a quest'ultimo vengono archiviate le informazioni sulla NIC. Le informazioni del profilo di rete specificato vengono memorizzate insieme al componente rete.

È possibile aggiungere più componenti di rete e sicurezza alla tela di progettazione.

È possibile che in un blueprint singolo siano presenti più componenti di rete su richiesta. Tuttavia, tutti i profili di rete su richiesta utilizzati nel blueprint devono fare riferimento allo stesso profilo di rete esterna.

Per i componenti macchina di vSphere con NSX associato, utilizzare le impostazioni di rete, sicurezza e bilanciamento del carico nell'interfaccia utente. Per i componenti macchina senza la scheda **Rete** o **Sicurezza**, è possibile aggiungere proprietà personalizzate di rete e sicurezza, quali ad esempio `VirtualMachine.Network0.Name`, alla relativa scheda **Proprietà** nella tela di progettazione. Le proprietà di rete, sicurezza e bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Durante la creazione di un blueprint vengono esposti solo i profili di rete applicabili al tenant corrente. In particolare, i profili di rete vengono resi disponibili se nel tenant corrente è presente almeno una prenotazione al cui profilo è assegnata almeno una rete.

Prerequisiti

- Creare e configurare le impostazioni di rete per NSX for vSphere. Vedere *Configurazione di vRealize Automation* e la *guida di amministrazione di NSX* nella [documentazione del prodotto NSX for vSphere](#)
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Creare un profilo di rete su richiesta. Vedere [Creazione di un profilo di rete in vRealize Automation](#).
Ad esempio, se si sta aggiungendo un componente di rete NAT su richiesta, vedere [Creazione di un profilo di rete NAT per una rete su richiesta](#).
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.
- Se si desidera specificare regole NAT per un componente di rete NAT, è necessario utilizzare un profilo di rete NAT di tipo uno a molti. Vedere [Creazione di un profilo di rete NAT mediante l'endpoint IPAM fornito](#) o [Creazione di un profilo di rete NAT mediante un endpoint IPAM di terze parti in vRealize Automation](#). Per informazioni sulle regole NAT, vedere [Creazione e utilizzo di regole NAT per NSX for vSphere](#).

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente di rete NAT su richiesta o di rete instradata su richiesta nella tela di progettazione.

- 3 Per etichettare in modo univoco un componente nella tela di progettazione, immettere il nome del componente nella casella di testo **ID**.
- 4 Selezionare un profilo di rete appropriato dal menu a discesa **Profilo di rete principale**. Ad esempio, se si desidera aggiungere un componente di rete NAT, selezionare un profilo di rete NAT configurato per supportare le impostazioni di rete desiderate.

Se si desidera specificare regole NAT in un componente di rete NAT, è necessario utilizzare un profilo di rete padre configurato per NAT di tipo uno a molti.

A seconda del tipo di profilo selezionato, le impostazioni di rete seguenti vengono popolate in base alla selezione del profilo di rete. Eventuali modifiche a questi valori devono essere apportate nel profilo di rete:

- Nome del profilo di rete esterna
 - Tipo di NAT (NAT su richiesta)
 - Subnet mask
 - Subnet mask dell'intervallo (instradata su richiesta)
 - Subnet mask dell'intervallo (instradata su richiesta)
 - Indirizzo IP di base (instradata su richiesta)
- 5 (Facoltativo) Immettere una descrizione del componente nella casella di testo **Descrizione**.
 - 6 (Facoltativo) Fare clic sulla scheda **DNS/WINS**.
 - 7 (Facoltativo) Specificare le impostazioni di DNS e WINS per il profilo di rete.
 - DNS primario
 - DNS secondario
 - Suffisso DNS
 - WINS preferito
 - WINS alternativo

Non è possibile cambiare le impostazioni di DNS e WINS per una rete esistente.

- 8 Fare clic sulla scheda **Intervalli IP**.

Vengono visualizzati l'intervallo o gli intervalli di indirizzi IP specificati nel profilo di rete. È possibile cambiare l'ordine e la visualizzazione delle colonne. Per le reti NAT è possibile anche cambiare i valori dell'intervallo di indirizzi IP.

- a Immettere l'indirizzo IP iniziale nella casella di testo **Inizio intervallo IP**.
- b Immettere l'indirizzo IP iniziale nella casella di testo **Inizio intervallo IP**.

- 9 Se si utilizza una rete NAT basata su un profilo di rete NAT di tipo uno a molti che utilizza intervalli IP statici, è possibile utilizzare la scheda **Regole NAT** per aggiungere regole che consentono a un IP esterno di accedere a componenti nella rete NAT interna.

Per una rete NAT One-to-Many, è possibile definire regole NAT che possono essere configurate quando si aggiunge un componente di rete NAT al blueprint. È possibile modificare una regola NAT quando si modifica la rete NAT in una distribuzione.

Le opzioni disponibili per la selezione si basano sui componenti della macchina vSphere o del bilanciamento del carico NSX for vSphere associati al componente di rete NAT.

- **Nome:** immettere un nome di regola univoco.
- **Componente:** selezionare da un elenco di componenti di macchina o bilanciamento del carico vSphere associati a cui è associata la rete NAT.

Le regole NAT sono supportate solo per le macchine non in cluster. Se è stata specificata una dimensione di cluster maggiore di 1, non viene elencato alcun componente perché la configurazione non è supportata.

- **Porta di origine:** selezionare l'opzione Qualsiasi, immettere una porta o un intervallo di porte valido o specificare un binding di proprietà valido.
- **Porta di destinazione:** selezionare l'opzione Qualsiasi, immettere una porta o un intervallo di porte valido o specificare un binding di proprietà valido.
- **Protocollo:** immettere un qualsiasi protocollo valido supportato da NSX for vSphere o selezionare l'opzione TCP, UDP o Qualsiasi.
- **Descrizione:** immettere una breve descrizione della regola NAT.

- 10 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Operazioni successive

È possibile aggiungere impostazioni di rete nella scheda **Rete** di un componente macchina vSphere.

Uso dei componenti di rete di NSX-T in un blueprint

È possibile aggiungere uno o più componenti rete NSX-T alla tela di progettazione e configurare le loro impostazioni per i componenti macchina vSphere nel blueprint.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX-T. Per informazioni sulla configurazione di NSX-T, vedere *NSX-T Administration Guide* nella [documentazione del prodotto NSX-T](#).

Quando si distribuisce un blueprint che contiene un endpoint NSX-T, la distribuzione assegna un tag ai componenti NSX-T nella distribuzione. Il nome del tag e il nome della distribuzione corrispondono.

Per ulteriori informazioni sulle considerazioni relative a distribuzione e topologia specifiche di NSX-T, vedere [Informazioni sulle topologie di distribuzione di NSX-T per i servizi di rete, la sicurezza e le configurazioni del bilanciamento del carico](#).

Aggiunta di un componente di rete esistente per NSX-T

È possibile aggiungere un componente di rete di NSX-T esistente alla tela di progettazione in preparazione per associare le sue impostazioni a uno o più componenti macchina vSphere nel blueprint.

È possibile utilizzare un componente rete esistente per aggiungere una rete NSX-T alla tela di progettazione e configurare le sue impostazioni per l'uso con i componenti macchina vSphere e i componenti Software o XaaS che si riferiscono a vSphere.

Quando si associa un componente di rete esistente o un componente di rete su richiesta a un componente macchina, insieme a quest'ultimo vengono archiviate le informazioni sulla NIC. Le informazioni del profilo di rete specificato vengono memorizzate insieme al componente rete.

È possibile aggiungere più componenti di rete e sicurezza alla tela di progettazione.

Per i componenti macchina di vSphere con NSX associato, utilizzare le impostazioni di rete, sicurezza e bilanciamento del carico nell'interfaccia utente. Per i componenti macchina senza la scheda **Rete** o **Sicurezza**, è possibile aggiungere proprietà personalizzate di rete e sicurezza, quali ad esempio `VirtualMachine.Network0.Name`, alla relativa scheda **Proprietà** nella tela di progettazione. Le proprietà di rete, sicurezza e bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Durante la creazione di un blueprint vengono esposti solo i profili di rete applicabili al tenant corrente. In particolare, i profili di rete vengono resi disponibili se nel tenant corrente è presente almeno una prenotazione al cui profilo è assegnata almeno una rete.

Prerequisiti

- Creare e configurare le impostazioni di rete per NSX-T. Vedere *Configurazione di vRealize Automation* e la *guida di amministrazione di NSX-T* nella [documentazione del prodotto NSX-T](#).
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Creare un profilo di rete.
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.

- 2 Trascinare un componente **Rete esistente** nella tela di progettazione.
- 3 Fare clic nella casella di testo **Rete esistente** e selezionare un profilo di rete esistente.
I valori di descrizione, subnet mask e gateway vengono compilati in base al profilo di rete selezionato.

- 4 (Facoltativo) Fare clic sulla scheda **DNS/WINS**.

- 5 (Facoltativo) Specificare le impostazioni di DNS e WINS per il profilo di rete.

- DNS primario
- DNS secondario
- Suffisso DNS
- WINS preferito
- WINS alternativo

Non è possibile cambiare le impostazioni di DNS e WINS per una rete esistente.

- 6 (Facoltativo) Fare clic sulla scheda **Intervalli IP**.

Vengono visualizzati l'intervallo o gli intervalli di indirizzi IP specificati nel profilo di rete. È possibile cambiare l'ordine e la visualizzazione delle colonne. Per le reti NAT è possibile anche cambiare i valori dell'intervallo di indirizzi IP.

- 7 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Operazioni successive

È possibile aggiungere impostazioni di rete nella scheda **Rete** di un componente macchina vSphere.

Creazione e utilizzo di regole NAT per NSX-T

È possibile aggiungere regole NAT a un componente di rete NAT di tipo One-to-Many in un blueprint quando il componente di rete NAT è associato a un componente della macchina vSphere non di cluster.

È possibile definire regole NAT per qualsiasi protocollo supportato da NSX-T oppure mappare una porta o un intervallo di porte dall'indirizzo IP esterno di un Edge a un indirizzo IP privato nel componente di rete NAT.

È possibile creare regole NAT per un componente di rete NAT di tipo One-to-Many associato a un componente della macchina vSphere non di cluster. Ad esempio, se due macchine sono associate a un componente di rete NAT di tipo One-to-Many nel blueprint, è possibile definire una regola NAT che consente alla porta 443 nell'IP esterno di connettersi alle macchine attraverso la porta 80 nella rete NAT mediante protocollo TCP.

Le regole NAT non sono supportate per il bilanciamento del carico NSX-T o per NSX-T versione 2.2.

È possibile creare un numero qualsiasi di regole NAT ed è possibile controllarne l'ordine di elaborazione.

I seguenti elementi non sono supportati per le regole NAT:

- NIC non incluse nella rete corrente
- NIC configurate in modo da ottenere indirizzi IP mediante DHCP
- Cluster di macchine

Per aggiungere regole NAT a un componente di una rete NAT in un blueprint, vedere [Aggiunta di un componente di rete instradata NSX-T o NAT NSX-T su richiesta](#).

Aggiunta di un componente di rete instradata NSX-T o NAT NSX-T su richiesta

È possibile aggiungere un componente di rete NAT su richiesta NSX-T o un componente di rete instradata su richiesta NSX-T alla tela di progettazione in preparazione per associarne le impostazioni a uno o più componenti macchina vSphere nel blueprint.

Quando si associa un componente di rete esistente o un componente di rete su richiesta a un componente macchina, insieme a quest'ultimo vengono archiviate le informazioni sulla NIC. Le informazioni del profilo di rete specificato vengono memorizzate insieme al componente rete.

È possibile aggiungere più componenti di rete e sicurezza alla tela di progettazione.

È possibile che in un blueprint singolo siano presenti più componenti di rete su richiesta. Tuttavia, tutti i profili di rete su richiesta utilizzati nel blueprint devono fare riferimento allo stesso profilo di rete esterna.

Per NSX-T, non si possono sovrapporre gli intervalli di rete che vengono utilizzati da reti differenti nel Blueprint. Questa limitazione emerge quando si configurano reti router di livello 1 NSX-T.

Per i componenti macchina di vSphere con NSX associato, utilizzare le impostazioni di rete, sicurezza e bilanciamento del carico nell'interfaccia utente. Per i componenti macchina senza la scheda **Rete** o **Sicurezza**, è possibile aggiungere proprietà personalizzate di rete e sicurezza, quali ad esempio `VirtualMachine.Network0.Name`, alla relativa scheda **Proprietà** nella tela di progettazione. Le proprietà di rete, sicurezza e bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Durante la creazione di un blueprint vengono esposti solo i profili di rete applicabili al tenant corrente. In particolare, i profili di rete vengono resi disponibili se nel tenant corrente è presente almeno una prenotazione al cui profilo è assegnata almeno una rete.

Prerequisiti

- Creare e configurare le impostazioni di rete per NSX for vSphere. Vedere *Configurazione di vRealize Automation* e la *guida di amministrazione di NSX for vSphere* nella [documentazione del prodotto NSX-T](#).

- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.

Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.

- Creare un profilo di rete su richiesta. Vedere [Creazione di un profilo di rete in vRealize Automation](#).

Ad esempio, se si sta aggiungendo un componente di rete NAT su richiesta, vedere [Creazione di un profilo di rete NAT per una rete su richiesta](#).

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.
- Se si desidera specificare regole NAT per un componente di rete NAT, è necessario utilizzare un profilo di rete NAT di tipo uno a molti. Vedere [Creazione di un profilo di rete NAT mediante l'endpoint IPAM fornito](#) o [Creazione di un profilo di rete NAT mediante un endpoint IPAM di terze parti in vRealize Automation](#). Per informazioni sulle regole NAT, vedere [Creazione e utilizzo di regole NAT per NSX for vSphere](#).

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente di rete NAT su richiesta NSX-T o di rete instradata su richiesta NSX-T nella tela di progettazione.
- 3 Per etichettare in modo univoco un componente nella tela di progettazione, immettere il nome del componente nella casella di testo **ID**.
- 4 Selezionare un profilo di rete appropriato dal menu a discesa **Profilo di rete principale**. Ad esempio, se si desidera aggiungere un componente di rete NAT, selezionare un profilo di rete NAT configurato per supportare le impostazioni di rete desiderate.

Se si desidera specificare regole NAT in un componente di rete NAT, è necessario utilizzare un profilo di rete padre configurato per NAT di tipo uno a molti.

A seconda del tipo di profilo selezionato, le impostazioni di rete seguenti vengono popolate in base alla selezione del profilo di rete. Eventuali modifiche a questi valori devono essere apportate nel profilo di rete:

- Nome del profilo di rete esterna
 - Tipo di NAT (NAT su richiesta NSX-T)
 - Subnet mask
 - Subnet mask dell'intervallo (instradata su richiesta NSX-T)
 - Subnet mask dell'intervallo (instradata su richiesta NSX-T)
 - Indirizzo IP di base (instradata su richiesta NSX-T)
- 5 (Facoltativo) Immettere una descrizione del componente nella casella di testo **Descrizione**.
 - 6 (Facoltativo) Fare clic sulla scheda **DNS/WINS**.

7 (Facoltativo) Specificare le impostazioni di DNS e WINS per il profilo di rete.

- DNS primario
- DNS secondario
- Suffisso DNS
- WINS preferito
- WINS alternativo

Non è possibile cambiare le impostazioni di DNS e WINS per una rete esistente.

8 Fare clic sulla scheda **Intervalli IP**.

Vengono visualizzati l'intervallo o gli intervalli di indirizzi IP specificati nel profilo di rete. È possibile cambiare l'ordine e la visualizzazione delle colonne. Per le reti NAT è possibile anche cambiare i valori dell'intervallo di indirizzi IP.

- a Immettere l'indirizzo IP iniziale nella casella di testo **Inizio intervallo IP**.
- b Immettere l'indirizzo IP iniziale nella casella di testo **Inizio intervallo IP**.

9 Se si utilizza una rete NAT basata su un profilo di rete NAT di tipo uno a molti che utilizza intervalli IP statici, è possibile utilizzare la scheda **Regole NAT** per aggiungere regole che consentono a un IP esterno di accedere a componenti nella rete NAT interna.

Per una rete NAT One-to-Many, è possibile definire regole NAT che possono essere configurate quando si aggiunge un componente di rete NAT al blueprint. È possibile modificare una regola NAT quando si modifica la rete NAT in una distribuzione.

Le opzioni disponibili per la selezione si basano sui componenti della macchina vSphere associati al componente di rete NAT.

- **Nome:** immettere un nome di regola univoco.
- **Componente:** selezionare da un elenco di componenti di macchina o bilanciamento del carico vSphere associati a cui è associata la rete NAT.

Le regole NAT sono supportate solo per le macchine non in cluster. Se è stata specificata una dimensione di cluster maggiore di 1, non viene elencato alcun componente perché la configurazione non è supportata.

- **Porta di origine:** selezionare l'opzione Qualsiasi, immettere una porta o un intervallo di porte valido o specificare un binding di proprietà valido.
- **Porta di destinazione:** selezionare l'opzione Qualsiasi, immettere una porta o un intervallo di porte valido o specificare un binding di proprietà valido.
- **Protocollo:** immettere un qualsiasi protocollo valido supportato da NSX-T o selezionare l'opzione TCP, UDP o Qualsiasi.
- **Descrizione:** immettere una breve descrizione dello scopo della regola NAT.

10 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Operazioni successive

È possibile aggiungere impostazioni di rete nella scheda **Rete** di un componente macchina vSphere.

Uso dei componenti di bilanciamento del carico di NSX for vSphere in un blueprint

È possibile aggiungere uno o più componenti bilanciamento del carico di NSX for vSphere su richiesta alla tela di progettazione per configurare le impostazioni dei componenti macchina vSphere nel blueprint.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere e NSX-T. Per informazioni sulla configurazione di NSX, vedere *Administration Guide* nella [documentazione del prodotto NSX for vSphere](#) o nella [documentazione del prodotto NSX-T](#), a seconda dell'applicazione utilizzata.

Ai pool di bilanciamento del carico e alle impostazioni di rete VIP nel blueprint si applicano le seguenti regole.

- Se il profilo di rete del pool è NAT, il profilo di rete VIP può essere parte del profilo di rete NAT.
- Se il profilo di rete del pool è instradato, il profilo di rete VIP può trovarsi solo sulla stessa rete instradata.
- Se il profilo del pool è relativo a una rete esterna, il profilo di rete VIP può essere solo lo stesso profilo di rete esterna.

Ogni componente del bilanciamento del carico può includere più server virtuali, definiti anche servizi di bilanciamento del carico. Ogni server virtuale nel componente del bilanciamento del carico ha una porta e un protocollo. Ad esempio, è possibile eseguire il bilanciamento del carico di un servizio HTTP o HTTPS. Un bilanciamento del carico può eseguire il bilanciamento del carico in più servizi.

L'Edge NSX è il dispositivo di rete che contiene i server virtuali di bilanciamento del carico. È possibile disporre di più componenti di bilanciamento del carico in un blueprint, ma quando si effettua il provisioning della distribuzione, i server virtuali definiti in ciascun componente di bilanciamento del carico sono contenuti in un unico EdgeNSX.

Se un blueprint contiene un bilanciamento del carico ed è abilitato l'isolamento app, i VIP del bilanciamento del carico vengono aggiunti come set di IP al gruppo di sicurezza dell'isolamento app. Se un blueprint contiene un gruppo di sicurezza su richiesta associato a un livello macchina associato a un bilanciamento del carico, il gruppo di sicurezza su richiesta include il livello macchina, il set di IP e i VIP.

Le impostazioni del bilanciamento del carico in una distribuzione esistente possono essere riconfigurate in modo da aggiungere, modificare o rimuovere server virtuali.

Considerazioni sull'utilizzo di componenti di bilanciamento del carico aggiornati o migrati

Di seguito sono riportati diversi aspetti importanti da tenere in considerazione per operare con i componenti di bilanciamento del carico di NSX nella release di vRealize Automation target.

Queste informazioni si applicano ai componenti di bilanciamento del carico di NSX for vSphere che sono stati aggiornati o migrati a questa release di vRealize Automation.

- È necessario eseguire la raccolta dati di Inventario rete e sicurezza di NSX prima e dopo l'aggiornamento o la migrazione a questa release per evitare problemi quando si esegue l'azione di riconfigurazione del bilanciamento del carico. L'azione di riconfigurazione del bilanciamento del carico per le nuove distribuzioni non viene influenzata.

Per ulteriori informazioni, vedere *Aggiornamento da vRealize Automation 7.1 e versioni successive* e *Migrazione di vRealize Automation*.

- È possibile riconfigurare il bilanciamento del carico. Il permesso di catalogo richiesto è Riconfigura (bilanciamento del carico).
- Per le distribuzioni che sono state aggiornate o migrate da vRealize Automation 7.x a questa release di vRealize Automation, la riconfigurazione del bilanciamento del carico è limitata alle distribuzioni che contengono un singolo bilanciamento del carico.
- L'operazione di riconfigurazione del bilanciamento del carico non è supportata per le distribuzioni che sono state aggiornate o migrate da vRealize Automation 6.2.x a questa release di vRealize Automation.

Aggiunta di un componente bilanciamento del carico su richiesta

È possibile trascinare un componente di bilanciamento del carico su richiesta NSX nella tela di progettazione e configurarne le impostazioni per l'uso con componenti contenitore e componenti macchina vSphere nel blueprint.

Per informazioni correlate su come creare profili dell'applicazione NSX for vSphere per definire il comportamento di un determinato tipo di traffico di rete, consultare la *guida di amministrazione di NSX* nella [documentazione del prodotto NSX for vSphere](#).

Procedura

1 Definizione delle impostazioni del membro del bilanciamento del carico

È possibile definire un componente bilanciamento del carico NSX su richiesta per distribuire l'elaborazione delle attività tra macchine membro o macchine contenitore vSphere con provisioning effettuato in una rete.

2 Definizione delle impostazioni generali del server virtuale

È possibile definire un protocollo e una porta del server virtuale singolo per il bilanciamento del carico oppure aggiungere server virtuali aggiuntivi per personalizzare opzioni di bilanciamento del carico NSX aggiuntive.

3 Definizione delle impostazioni di distribuzione del server virtuale

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile specificare le informazioni sui membri di un pool quali la porta sulla quale tali membri ricevono il traffico, il tipo di protocollo che il bilanciamento del carico di NSX può utilizzare per accedere a tale porta, l'algoritmo utilizzato per il bilanciamento del carico e le impostazioni di persistenza.

4 Definizione delle impostazioni di controllo dell'integrità del server virtuale

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile specificare in che modo, o se, il bilanciamento del carico NSX deve eseguire i controlli di integrità sui membri del pool all'interno del server virtuale.

5 Definizione delle impostazioni avanzate del server virtuale

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile personalizzare il componente di bilanciamento del carico NSX per specificare impostazioni quali il numero di connessioni simultanee che un singolo membro del pool è in grado di riconoscere e il numero massimo di connessioni simultanee che il server virtuale è in grado di elaborare.

6 Definizione delle opzioni di registrazione del bilanciamento del carico

È possibile definire i tipi di azione di registrazione del bilanciamento del carico che vengono acquisiti e inclusi nei registri del bilanciamento del carico.

Definizione delle impostazioni del membro del bilanciamento del carico

È possibile definire un componente bilanciamento del carico NSX su richiesta per distribuire l'elaborazione delle attività tra macchine membro o macchine contenitore vSphere con provisioning effettuato in una rete.

Quando si aggiunge un componente del bilanciamento del carico a un blueprint nella tela di progettazione, è possibile scegliere un'opzione predefinita o personalizzata durante la creazione o la modifica delle definizioni del server virtuale nel componente del bilanciamento del carico. L'opzione predefinita consente di specificare il protocollo, la porta e la descrizione del server virtuale, oltre che di utilizzare i valori predefiniti per tutte le altre impostazioni. L'opzione personalizzata consente di definire ulteriori livelli di dettaglio.

Se il provisioning del bilanciamento del carico viene eseguito con una rete esterna, il VIP (rete VIP) e il pool di membri (rete di membri) devono trovarsi nella stessa rete esistente. Il provisioning non riesce se il VIP e il pool di membri non si trovano nella stessa rete esterna.

Prerequisiti

- Creare e configurare le impostazioni del bilanciamento del carico per NSX. Vedere *Configurazione di vRealize Automation* e la *guida di amministrazione di NSX*.
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Creare un profilo di rete.
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.
- Verificare che nel blueprint sia presente almeno un componente del contenitore o un componente della macchina vSphere.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **Bilanciamento del carico su richiesta** nella tela di progettazione.
- 3 Per etichettare in modo univoco un componente nella tela di progettazione, immettere il nome del componente nella casella di testo **ID**.
- 4 Selezionare un nome del componente del contenitore o del componente della macchina vSphere dal menu a discesa **Membro**.

L'elenco contiene solo i componenti del contenitore e i componenti della macchina vSphere nel blueprint attivo.

- 5 Selezionare la NIC di cui eseguire il bilanciamento del carico nel menu a discesa **Rete membro**.

L'elenco include le NIC definite per il membro macchina vSphere selezionato.

- 6 Selezionare una rete di indirizzi IP virtuali disponibile nel menu a discesa **Rete VIP**. Ad esempio, selezionare una rete esterna o NAT disponibile.

Un blueprint può includere più componenti di bilanciamento del carico NSX e di rete su richiesta NSX, ma tali componenti devono essere tutti associati alla stessa rete VIP.

- 7 (Facoltativo) Immettere un indirizzo IP valido per la NIC nella casella di testo **Indirizzo IP**.

L'impostazione predefinita è l'indirizzo IP statico associato alla rete VIP. È possibile specificare un altro indirizzo IP o un intervallo di indirizzi IP. Per impostazione predefinita, il successivo indirizzo IP disponibile viene allocato dalla rete VIP associata.

Lasciare il campo dell'indirizzo IP vuoto per consentire l'allocazione dell'indirizzo IP dalla rete VIP associata durante il provisioning.

Se si specifica un indirizzo IP per qualsiasi altro tipo di rete, è possibile eseguire il provisioning di una sola distribuzione. Nelle distribuzioni successive l'allocazione dell'indirizzo IP non riesce, perché è già utilizzato dalla prima distribuzione.

- 8 Per creare una definizione di server virtuale, fare clic su **Nuovo** e vedere [Definizione delle impostazioni generali del server virtuale](#).

Ciascun componente di bilanciamento del carico richiede almeno un server virtuale.

Per specificare le opzioni di registrazione, vedere [Definizione delle opzioni di registrazione del bilanciamento del carico](#).

Definizione delle impostazioni generali del server virtuale

È possibile definire un protocollo e una porta del server virtuale singolo per il bilanciamento del carico oppure aggiungere server virtuali aggiuntivi per personalizzare opzioni di bilanciamento del carico NSX aggiuntive.

È ad esempio possibile personalizzare il componente del bilanciamento del carico per definire impostazioni come protocollo e porta del controllo dell'integrità, algoritmo, persistenza e trasparenza.

Prerequisiti

[Definizione delle impostazioni del membro del bilanciamento del carico.](#)

Procedura

- 1 Fare clic sulla scheda **Generale** nella pagina **Nuovo server virtuale**.
- 2 Nel menu a discesa **Protocollo** selezionare il protocollo del traffico di rete da utilizzare per il bilanciamento del carico del server virtuale.

Le opzioni del protocollo sono HTTP, HTTPS, TCP e UDP.

- 3 Immettere un valore della porta nella casella di testo **Porta**.

Il protocollo selezionato determina l'impostazione della porta predefinita.

Protocollo	Porta predefinita
HTTP	80
HTTPS	443
TCP	8080
UDP	nessun valore predefinito

I protocolli HTTP, HTTPS e TCP possono condividere una porta con UDP. Ad esempio, se il servizio 1 utilizza TCP, HTTP o HTTPS sulla porta 80, il servizio 2 può utilizzare UDP sulla porta 80. Se il servizio 1 utilizza UDP sulla porta 80, il servizio 2 non può utilizzare UDP sulla porta 80.

- 4 (Facoltativo) Immettere una descrizione per il componente del server virtuale.
- 5 Selezionare una delle opzioni disponibili in **Impostazioni**.

■ Usa valore predefinito per tutte le altre impostazioni

Consente di accettare tutte le altre impostazioni predefinite. Fare clic su **OK** per completare la definizione del componente del bilanciamento del carico e continuare a lavorare nel blueprint.

È possibile visualizzare i valori predefiniti facendo clic su **Personalizza** ed esaminando le opzioni aggiuntive della scheda. Se le impostazioni predefinite sono accettabili, fare clic su **Usa valore predefinito per tutte le altre impostazioni** nella scheda **Generale**.

■ Personalizza

Consente di configurare il componente del bilanciamento del carico con impostazioni aggiuntive, ad esempio per definire un protocollo diverso per il monitoraggio dell'integrità o una porta diversa per il monitoraggio del traffico del membro.

Vengono visualizzate schede aggiuntive che consentono di aggiungere impostazioni personalizzate.

Se si seleziona l'opzione **Usa valore predefinito per tutte le altre impostazioni** e si fa clic su **OK**, il processo viene completato ed è possibile continuare a definire o modificare il blueprint nella tela di progettazione. Se si seleziona l'opzione **Personalizza**, continuare con il passaggio successivo.

- 6 Fare clic sulla scheda **Distribuzione** e vedere l'argomento [Definizione delle impostazioni di distribuzione del server virtuale](#) per continuare a definire il server virtuale nel componente del bilanciamento del carico NSX.

Definizione delle impostazioni di distribuzione del server virtuale

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile specificare le informazioni sui membri di un pool quali la porta sulla quale tali membri ricevono il traffico, il tipo di protocollo che il bilanciamento del carico di NSX può utilizzare per accedere a tale porta, l'algoritmo utilizzato per il bilanciamento del carico e le impostazioni di persistenza.

Un pool rappresenta un cluster di macchine in cui viene eseguito il bilanciamento del carico. Un membro del pool rappresenta una macchina in tale cluster.

Le impostazioni predefinite del protocollo del membro e della porta del membro corrispondono alle impostazioni del protocollo e della porta nella pagina **Generale**.

Il pool di macchine membro viene visualizzato nel valore dell'opzione **Membro** nell'interfaccia utente del componente del bilanciamento del carico blueprint. La voce **Membro** è impostata sul pool o sul cluster di macchine.

Prerequisiti

[Definizione delle impostazioni generali del server virtuale.](#)

Procedura

- 1 (Facoltativo) L'impostazione di **Protocollo membro** corrisponde al protocollo specificato nella scheda **Generale**. Questa impostazione definisce la modalità con cui il membro del pool riceve il traffico di rete.
- 2 (Facoltativo) Immettere un numero di porta nella casella di testo **Porta membro** per specificare la porta in cui il membro del pool riceve il traffico di rete.

Ad esempio, se la richiesta in entrata all'indirizzo IP virtuale (VIP) del bilanciamento del carico viene ricevuta tramite la porta 80, è possibile instradare la richiesta a un'altra porta, ad esempio la porta 8080, nei membri del pool.

3 (Facoltativo) Selezionare il metodo di bilanciamento dell'algoritmo per questo pool.

Le opzioni dell'algoritmo e i parametri dell'algoritmo per le opzioni che li richiedono vengono descritti nella tabella seguente.

Opzione	Descrizione e parametri dell'algoritmo
ROUND_ROBIN	<p>Ciascun server viene utilizzato a turno in base al peso assegnato.</p> <p>Se il bilanciamento del carico è stato creato in vRealize Automation, il peso è lo stesso per tutti i membri.</p> <p>Si tratta dell'algoritmo più uniforme ed equo quando il tempo di elaborazione del server rimane distribuito in modo omogeneo.</p> <p>I parametri dell'algoritmo sono disattivati per questa opzione.</p>
IP-HASH	<p>Seleziona un server in base a un hash dell'indirizzo IP di origine e al peso totale di tutti i server in esecuzione.</p> <p>I parametri dell'algoritmo sono disattivati per questa opzione.</p>
LEASTCONN	<p>Distribuisce richieste client a più server in base al numero di connessioni già presenti nel server.</p> <p>Le nuove connessioni vengono inviate al server con il numero minore di connessioni.</p> <p>I parametri dell'algoritmo sono disattivati per questa opzione.</p>
URI	<p>Nella parte sinistra dell'URI (prima del punto di domanda) viene applicato un hash e tale parte viene divisa per il peso totale dei server in esecuzione.</p> <p>Il risultato indica il server che riceverà la richiesta. Ciò assicura che un URI venga sempre indirizzato allo stesso server purché nessun altro server diventi attivo o inattivo.</p> <p>Il parametro dell'algoritmo dell'URI ha due opzioni, ovvero <code>uriLength=<len></code> e <code>uriDepth=<dep></code>. Immettere i parametri di lunghezza e profondità in righe separate nella casella di testo Parametri algoritmo.</p> <p>I parametri di lunghezza e profondità sono seguiti da un numero intero positivo. Queste opzioni possono bilanciare i server solo in base alla parte iniziale dell'URI.</p> <p>Il parametro di lunghezza indica che l'algoritmo deve prendere in considerazione solo i caratteri definiti all'inizio dell'URI per calcolare l'hash. L'intervallo del parametro di lunghezza deve essere $1 \leq \text{len} < 256$.</p> <p>Il parametro di profondità indica la profondità di directory massima da utilizzare per calcolare l'hash. Viene conteggiato un livello per ciascuna barra presente nella richiesta. L'intervallo del parametro di profondità deve essere $1 \leq \text{dep} < 10$.</p> <p>Se vengono specificati entrambi i parametri, la valutazione termina quando viene raggiunto uno dei parametri.</p>

Opzione	Descrizione e parametri dell'algoritmo
HTTPHEADER	<p>In ciascuna richiesta HTTP viene cercato il nome dell'intestazione HTTP.</p> <p>Nel nome dell'intestazione tra parentesi non viene fatta distinzione tra maiuscole e minuscole, in modo simile alla funzione ACL 'hdr()'.</p> <p>Il parametro dell'algoritmo HTTPHEADER ha un'unica opzione, ovvero <code>headerName=<name></code>. Ad esempio, è possibile utilizzare host come parametro dell'algoritmo HTTPHEADER.</p> <p>Se l'intestazione è assente o non contiene alcun valore, viene applicato l'algoritmo round robin.</p>
URL	<p>Nella stringa di query di ciascuna richiesta HTTP GET viene cercato il parametro dell'URL specificato nell'argomento.</p> <p>Il parametro dell'algoritmo dell'URL ha un'unica opzione, ovvero <code>urlParam=<url></code>.</p> <p>Se il parametro è seguito da un segno di uguale = e da un valore, al valore viene applicato un hash e tale valore viene diviso per il peso totale dei server in esecuzione. Il risultato indica il server che riceverà la richiesta. Questo processo viene utilizzato per tenere traccia degli identificatori utente nelle richieste e assicurare che lo stesso ID utente venga sempre inviato allo stesso server purché nessun altro server diventi attivo o inattivo.</p> <p>Se non viene trovato alcun valore o parametro, viene applicato un algoritmo round robin.</p>

4 (Facoltativo) Selezionare il metodo di persistenza per questo pool.

La persistenza tiene traccia dei dati della sessione e ne effettua l'archiviazione, come nel caso del membro del pool specifico che ha gestito la richiesta di un client. Con la persistenza, le richieste del client vengono indirizzate allo stesso membro del pool per la durata di una sessione o durante le sessioni successive.

Protocollo	Metodo di persistenza supportato
HTTP	Nessuno, Cookie, IP di origine
HTTPS	Nessuno, IP di origine e ID sessione SSL
TCP	Nessuno, IP di origine, MSRPD
UDP	Nessuno, IP di origine

- Selezionare **Cookie** per inserire un cookie univoco allo scopo di identificare la sessione la prima volta che un client accede al sito. Al cookie verrà fatto riferimento nelle richieste successive per la persistenza della connessione al server appropriato.
- Selezionare **IP di origine** per tenere traccia delle sessioni in base all'indirizzo IP di origine. Quando un client richiede una connessione a un server virtuale che supporta la persistenza dell'affinità dell'indirizzo di origine, il bilanciamento del carico verifica se tale client si è già connesso in precedenza. In caso affermativo, restituisce il client allo stesso membro del pool.
- Selezionare l'**ID sessione SSL** e il modello di traffico HTTPS passthrough SSL.
 - Passthrough SSL - Client -> HTTPS-> LB (passthrough SSL) -> HTTPS -> server

- Client - HTTP-> LB -> HTTP -> server

Nota vRealize Automation attualmente supporta solo passthrough SSL. Viene utilizzato il metodo passthrough SSL indipendentemente dall'opzione selezionata.

- Selezionare **MSRDP** per mantenere le sessioni persistenti tra i client e i server Windows in cui è in esecuzione il servizio Microsoft Remote Desktop Protocol (RDP). Lo scenario consigliato per abilitare la persistenza di MSRDP consiste nel creare un pool di bilanciamento del carico composto da membri che eseguono il server Windows supportato, in cui tutti i membri appartengono a un cluster Windows e partecipano a una directory di sessione Windows.
 - Selezionare **Nessuno** per fare in modo che le azioni della sessione non vengano archiviate per il richiamo successivo.
- 5 Se si utilizza un'impostazione di persistenza Cookie, immettere il nome del cookie.
- 6 (Facoltativo) Selezionare la modalità di inserimento del cookie dal menu a discesa **Modalità**.

Opzione	Descrizione
Inserisci	NSX Edge invia un cookie. Se il server invia uno o più cookie, il client riceve un ulteriore cookie (i cookie del server + il cookie di NSX Edge). Se il server non invia alcun cookie, il client riceve il cookie di NSX Edge.
Prefisso	Il server invia un cookie. Utilizzare questa opzione se il client non supporta più di un cookie. Se si dispone di un'applicazione proprietaria che utilizza un client proprietario che supporta un solo cookie, il server Web invia un cookie ma NSX Edge inserisce (come prefisso) le informazioni del proprio cookie nel valore del cookie del server.
Sessione app	Il server non invia alcun cookie. Invia invece le informazioni della sessione utente come URL. Ad esempio, http://mysite.com/admin/UpdateUserServlet;jsessionId=X000X0XXX0XXXX, dove jsessionId rappresenta le informazioni della sessione utente e viene utilizzato per la persistenza.

- 7 (Facoltativo) Immettere l'ora di scadenza della persistenza per il cookie in secondi.
Ad esempio, per un bilanciamento del carico L7 con un IP di origine TCP, se non vengono effettuate nuove connessioni TCP per l'ora di scadenza specificata si verifica un timeout della voce di persistenza, anche se le connessioni esistenti sono ancora attive.
- 8 (Facoltativo) Fare clic sulla scheda **Controllo di integrità** e vedere l'argomento [Definizione delle impostazioni di controllo dell'integrità del server virtuale](#) per continuare a definire il server virtuale nel componente del bilanciamento del carico NSX.

Definizione delle impostazioni di controllo dell'integrità del server virtuale

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile specificare in che modo, o se, il bilanciamento del carico NSX deve eseguire i controlli di integrità sui membri del pool all'interno del server virtuale.

Le impostazioni predefinite del protocollo e della porta del controllo dell'integrità corrispondono alle impostazioni del protocollo e della porta nella scheda **Generale**.

Per informazioni correlate, vedere *Create a Service Monitor* nella documentazione di prodotto relativa a NSX all'indirizzo https://www.vmware.com/support/pubs/nsx_pubs.html. Tenere presente che nella documentazione relativa a NSX il membro del server virtuale viene definito membro del pool.

Prerequisiti

[Definizione delle impostazioni generali del server virtuale.](#)

Procedura

- 1 (Facoltativo) Selezionare un protocollo del controllo dell'integrità nel menu a discesa **Protocollo controllo di integrità** per specificare la modalità di accesso al membro del pool quando il bilanciamento del carico è in ascolto per determinare l'integrità del membro del pool.

Le opzioni del protocollo sono **HTTP**, **HTTPS**, **TCP**, **ICMP**, **UDP** e **Nessuno**.

È anche possibile accettare il protocollo predefinito specificato nella scheda Generale.

- 2 (Facoltativo) Immettere un valore nella casella **Porta controllo di integrità** per specificare la porta di ascolto del bilanciamento del carico per il monitoraggio dell'integrità del membro del server virtuale o del pool.

Tenere presente che nella documentazione relativa a NSX il membro del server virtuale viene definito membro del pool.

I protocolli HTTP, HTTPS e TCP possono condividere una porta con UDP. Ad esempio, se il servizio 1 utilizza TCP, HTTP o HTTPS sulla porta 80, il servizio 2 può utilizzare UDP sulla porta 80. Se il servizio 1 utilizza UDP sulla porta 80, il servizio 2 non può utilizzare UDP sulla porta 80.

- 3 Immettere il valore di **Intervallo**, in secondi, per l'esecuzione del ping di un server.
- 4 Immettere il valore di **Timeout** massimo, in secondi, entro il quale è necessario ricevere una risposta dal server virtuale.
- 5 Immettere un valore nel campo **Numero massimo tentativi** per specificare il numero massimo di tentativi di ping da eseguire prima di dichiarare inattivo il server.

- 6 Specificare ulteriori impostazioni del controllo di integrità in base al **Protocollo controllo di integrità** selezionato.
 - a Immettere il **Metodo** da utilizzare per rilevare lo stato del server. Le opzioni sono GET, OPTIONS e POST.
 - b Immettere l'**URL** da utilizzare per rilevare lo stato del server. Si tratta dell'URL utilizzato per le opzioni di metodo GET e POST (include "/" per impostazione predefinita).
 - c Nella casella di testo **Invia** immettere la stringa da inviare al server dopo aver stabilito una connessione.

Nella casella di testo **Invia** immettere la stringa da inviare al server dopo aver stabilito una connessione.
 - d Nella casella di testo **Ricevi** immettere la stringa che si prevede di ricevere dal server.

Il server viene considerato attivo solo quando la stringa ricevuta corrisponde a questa definizione.

La stringa può essere un'intestazione oppure trovarsi nel corpo della risposta.
- 7 Fare clic sulla scheda **Avanzate** e vedere l'argomento [Definizione delle impostazioni avanzate del server virtuale](#) per continuare a definire il server virtuale nel componente del bilanciamento del carico NSX.

Per specificare le opzioni di registrazione, vedere [Definizione delle opzioni di registrazione del bilanciamento del carico](#).

Definizione delle impostazioni avanzate del server virtuale

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile personalizzare il componente di bilanciamento del carico NSX per specificare impostazioni quali il numero di connessioni simultanee che un singolo membro del pool è in grado di riconoscere e il numero massimo di connessioni simultanee che il server virtuale è in grado di elaborare.

Prerequisiti

[Definizione delle impostazioni generali del server virtuale.](#)

Procedura

- 1 Immettere un valore nella casella di testo **Limite connessione** per specificare il numero massimo di connessioni simultanee in NSX che il server virtuale è in grado di elaborare.

Questa impostazione considera il numero di tutte le connessioni del membro.

Immettere il valore 0 per non specificare alcun limite.
- 2 Immettere un valore nella casella di testo **Limite frequenza di connessione** per specificare il numero massimo di richieste di connessione in entrata in NSX che è possibile accettare al secondo.

Questa impostazione considera il numero di tutte le connessioni del membro.

Immettere il valore 0 per non specificare alcun limite.

- 3 (Facoltativo) Selezionare la casella di controllo **Attiva accelerazione** per fare in modo che ciascun IP virtuale (VIP) utilizzi il bilanciamento del carico L4 più veloce anziché il bilanciamento del carico L7.
- 4 (Facoltativo) Selezionare la casella di controllo **Trasparente** per consentire ai membri del pool del bilanciamento del carico di visualizzare l'indirizzo IP delle macchine che richiamano il bilanciamento del carico.

Se la casella di controllo non è selezionata, i membri del pool del bilanciamento del carico visualizzano l'indirizzo IP di origine del traffico come un indirizzo IP interno del bilanciamento del carico.

- 5 Immettere un valore nella casella di testo **Numero massimo connessioni** per specificare il numero massimo di connessioni simultanee che un singolo membro del pool è in grado di riconoscere.

Se il numero di richieste in entrata supera questo valore, le richieste vengono aggiunte alla coda e quindi elaborate in base all'ordine di ricezione man mano che le connessioni sono disponibili.

Immettere il valore 0 per non specificare alcun valore massimo.

- 6 Immettere un valore nella casella di testo **Numero minimo connessioni** per specificare il numero minimo di connessioni simultanee che un singolo membro del pool deve sempre accettare.

Immettere il valore 0 per non specificare alcun valore minimo.

- 7 Fare clic su **OK** per completare la definizione del server virtuale.
- 8 Per specificare le opzioni di registrazione, vedere [Definizione delle opzioni di registrazione del bilanciamento del carico](#), altrimenti fare clic su **Salva** o **Fine**.

Definizione delle opzioni di registrazione del bilanciamento del carico

È possibile definire i tipi di azione di registrazione del bilanciamento del carico che vengono acquisiti e inclusi nei registri del bilanciamento del carico.

Dopo o durante la definizione di un componente del bilanciamento del carico, è possibile specificare un livello di registrazione per la raccolta dei registri del traffico del bilanciamento del carico. I livelli di registrazione definiti per un componente qualsiasi del bilanciamento del carico nel blueprint vengono applicati a tutti i bilanciamenti del carico definiti nel blueprint.

I livelli di registrazione includono le opzioni Debug, Informazioni, Avviso, Errore e Critico. Le opzioni Debug e Informazioni registrano le richieste degli utenti, mentre le opzioni Avviso, Errore e Critico non registrano le richieste degli utenti.

Per ulteriori informazioni sulla registrazione del bilanciamento del carico NSX, vedere la *NSX Administration Guide*.

Prerequisiti

[Definizione delle impostazioni del membro del bilanciamento del carico.](#)

Procedura

- 1 Selezionare la scheda **Globale** nel componente del bilanciamento del carico nella tela di progettazione.

- 2 Selezionare una o più opzioni di registrazione dal menu a discesa **Livello di registrazione**.

Selezionare un livello di registrazione per raccogliere i registri del traffico del bilanciamento del carico. L'impostazione viene applicata a tutti i componenti del bilanciamento del carico NSX nel blueprint.

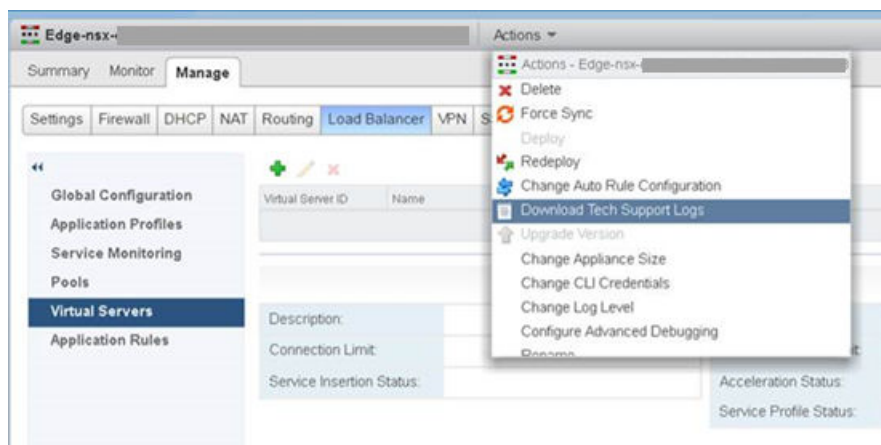
Le impostazioni di registrazione vengono definite nel client Web di vSphere.

- Nessuno
- Informazioni
- Emergenza
- Avviso
- Critico
- Errore
- Avviso
- Notifica
- Debug

- 3 Fare clic su **Salva**.

Risultati

È possibile visualizzare e scaricare i registri nel client Web vSphere utilizzando il menu **Azioni** per NSX Edge, come descritto in *Download Tech Support Logs for NSX Edge* nella documentazione del prodotto NSX all'indirizzo https://www.vmware.com/support/pubs/nsx_pubs.html.



Uso dei componenti del bilanciamento del carico di NSX-T in un blueprint

È possibile aggiungere uno o più componenti bilanciamento del carico di NSX-T su richiesta alla tela di progettazione per configurare le impostazioni dei componenti macchina vSphere nel blueprint.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere e NSX-T. Per informazioni sulla configurazione di NSX, vedere *Administration Guide* nella [documentazione del prodotto NSX for vSphere](#) o nella [documentazione del prodotto NSX-T](#), a seconda dell'applicazione utilizzata.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX-T. Per informazioni sulla configurazione di NSX-T, vedere *NSX-T Administration Guide* nella [documentazione del prodotto NSX-T](#).

Ai pool di bilanciamento del carico e alle impostazioni di rete VIP nel blueprint si applicano le seguenti regole.

- Se il profilo di rete del pool è NAT, il profilo di rete VIP può essere parte del profilo di rete NAT.
- Se il profilo di rete del pool è instradato, il profilo di rete VIP può trovarsi solo sulla stessa rete instradata o sulla stessa rete esterna.
- Se il profilo del pool è relativo a una rete esterna, il profilo di rete VIP può essere solo lo stesso profilo di rete esterna.

Ogni componente del bilanciamento del carico può includere più server virtuali, definiti anche servizi di bilanciamento del carico. Ogni server virtuale nel componente del bilanciamento del carico ha una porta e un protocollo. Ad esempio, è possibile eseguire il bilanciamento del carico di un servizio HTTP o HTTPS. Un bilanciamento del carico può eseguire il bilanciamento del carico in più servizi.

Il bilanciamento del carico NSX è il servizio che contiene i server virtuali di bilanciamento del carico.

Se un blueprint contiene un bilanciamento del carico ed è abilitato l'isolamento app, i VIP del bilanciamento del carico vengono aggiunti come set di IP al gruppo di sicurezza dell'isolamento app. Se un blueprint contiene un gruppo di sicurezza su richiesta associato a un livello macchina associato a un bilanciamento del carico, il gruppo di sicurezza su richiesta include il livello macchina, il set di IP e i VIP.

Per ulteriori informazioni sulle considerazioni relative a distribuzione e topologia specifiche di NSX-T, vedere [Informazioni sulle topologie di distribuzione di NSX-T per i servizi di rete, la sicurezza e le configurazioni del bilanciamento del carico](#).

Aggiunta di un bilanciamento del carico NSX-T su richiesta

È possibile trascinare un componente di bilanciamento del carico su richiesta NSX-T nella tela di progettazione e configurarne le impostazioni per l'uso con componenti contenitore e componenti macchina vSphere nel blueprint.

Il bilanciamento del carico di NSX-T distribuisce equamente le richieste di servizio in entrata tra più server. In questo modo, la distribuzione del carico avviene in modo trasparente per gli utenti. Il bilanciamento del carico consente di ottenere un utilizzo ottimale delle risorse, ottimizzando la velocità, riducendo al minimo i tempi di risposta ed evitando i sovraccarichi.

È possibile mappare un indirizzo IP virtuale ad un set di server pool per il bilanciamento del carico. Il bilanciamento del carico accetta richieste TCP, UDP, HTTP o HTTPS sull'indirizzo IP virtuale e sceglie il membro del pool da utilizzare. Un bilanciamento del carico è collegato ad un router logico di livello 1.

A seconda delle esigenze dell'ambiente in uso, è possibile scalare le prestazioni del bilanciamento del carico aumentando il numero di server virtuali e dei membri pool esistenti per gestire carichi di traffico di rete elevati.

Per informazioni sulla creazione di bilanciamenti del carico di NSX-T per definire il comportamento del traffico di rete, vedere *Bilanciamento del carico logico* e *Configurazione di componenti del bilanciamento del carico* nella guida di amministrazione di NSX-T nella [documentazione del prodotto NSX-T](#).

Procedura

1 Definizione delle impostazioni del membro del bilanciamento del carico NSX-T

È possibile definire un componente bilanciamento del carico NSX-T su richiesta per distribuire l'elaborazione delle attività tra macchine membro o macchine contenitore vSphere con provisioning effettuato in una rete.

2 Definizione delle impostazioni generali del server virtuale per NSX-T

È possibile definire un protocollo e una porta del server virtuale singolo per il bilanciamento del carico oppure aggiungere server virtuali aggiuntivi per personalizzare opzioni di bilanciamento del carico NSX-T aggiuntive.

3 Definizione delle impostazioni di distribuzione del server virtuale per NSX-T

Selezionando l'opzione **Personalizza** quando si definisce un server virtuale, è possibile specificare le informazioni sui membri di un pool quali la porta sulla quale tali membri ricevono il traffico, il tipo di protocollo che il bilanciamento del carico di NSX-T può utilizzare per accedere a tale porta, l'algoritmo utilizzato per il bilanciamento del carico e le impostazioni di persistenza.

4 Definizione delle impostazioni di controllo dell'integrità del server virtuale per NSX-T

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile specificare in che modo, o se, il bilanciamento del carico NSX-T deve eseguire i controlli di integrità sui membri del pool all'interno del server virtuale.

5 Definizione delle impostazioni avanzate del server virtuale per NSX-T

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile personalizzare il componente di bilanciamento del carico NSX-T per specificare impostazioni quali il numero di connessioni simultanee che un singolo membro del pool è in grado di riconoscere e il numero massimo di connessioni simultanee che il server virtuale è in grado di elaborare.

6 Definizione delle opzioni di registrazione del bilanciamento del carico NSX-T

È possibile definire i tipi di azione di registrazione del bilanciamento del carico che vengono acquisiti e inclusi nei registri del bilanciamento del carico.

Definizione delle impostazioni del membro del bilanciamento del carico NSX-T

È possibile definire un componente bilanciamento del carico NSX-T su richiesta per distribuire l'elaborazione delle attività tra macchine membro o macchine contenitore vSphere con provisioning effettuato in una rete.

Quando si aggiunge un componente del bilanciamento del carico a un blueprint nella tela di progettazione, è possibile scegliere un'opzione predefinita o personalizzata durante la creazione o la modifica delle definizioni del server virtuale nel componente del bilanciamento del carico. L'opzione predefinita consente di specificare il protocollo, la porta e la descrizione del server virtuale, oltre che di utilizzare i valori predefiniti per tutte le altre impostazioni. L'opzione personalizzata consente di definire ulteriori livelli di dettaglio.

Se il provisioning del bilanciamento del carico viene eseguito con una rete esterna, il VIP (rete VIP) e il pool di membri (rete di membri) devono trovarsi nella stessa rete esistente. Il provisioning non riesce se il VIP e il pool di membri non si trovano nella stessa rete esterna.

Prerequisiti

- Creare e configurare le impostazioni del bilanciamento del carico per NSX. Vedere [Elenco di controllo per la preparazione della configurazione di rete e sicurezza di NSX](#).
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Creare un profilo di rete. Vedere [Creazione di un profilo di rete in vRealize Automation](#).
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.
- Verificare che nel blueprint sia presente almeno un componente del contenitore o un componente della macchina vSphere.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **Bilanciamento del carico su richiesta NSX-T** nella tela di progettazione.
- 3 Per etichettare in modo univoco un componente nella tela di progettazione, immettere il nome del componente nella casella di testo **ID**.
- 4 Selezionare un nome del componente del contenitore o del componente della macchina vSphere dal menu a discesa **Membro**.

L'elenco contiene solo i componenti del contenitore e i componenti della macchina vSphere nel blueprint attivo.

- 5 Selezionare la NIC di cui eseguire il bilanciamento del carico nel menu a discesa **Rete membro**.

L'elenco include le NIC definite per il membro macchina vSphere selezionato.

- 6 Selezionare una rete di indirizzi IP virtuali disponibile nel menu a discesa **Rete VIP**. Ad esempio, selezionare una rete esterna o NAT disponibile.

Un blueprint può includere più componenti di bilanciamento del carico NSX e di rete su richiesta NSX, ma tali componenti devono essere tutti associati alla stessa rete VIP.

- 7 (Facoltativo) Immettere un indirizzo IP valido per la NIC nella casella di testo **Indirizzo IP**.

L'impostazione predefinita è l'indirizzo IP statico associato alla rete VIP. È possibile specificare un altro indirizzo IP o un intervallo di indirizzi IP. Per impostazione predefinita, il successivo indirizzo IP disponibile viene allocato dalla rete VIP associata.

Lasciare il campo dell'indirizzo IP vuoto per consentire l'allocazione dell'indirizzo IP dalla rete VIP associata durante il provisioning.

Se si specifica un indirizzo IP per qualsiasi altro tipo di rete, è possibile eseguire il provisioning di una sola distribuzione. Nelle distribuzioni successive l'allocazione dell'indirizzo IP non riesce, perché è già utilizzato dalla prima distribuzione.

- 8 Per creare una definizione di server virtuale, fare clic su **Nuovo** e vedere [Definizione delle impostazioni generali del server virtuale per NSX-T](#).

Ciascun componente di bilanciamento del carico richiede almeno un server virtuale.

Per specificare le opzioni di registrazione, vedere [Definizione delle opzioni di registrazione del bilanciamento del carico NSX-T](#).

Definizione delle impostazioni generali del server virtuale per NSX-T

È possibile definire un protocollo e una porta del server virtuale singolo per il bilanciamento del carico oppure aggiungere server virtuali aggiuntivi per personalizzare opzioni di bilanciamento del carico NSX-T aggiuntive.

È ad esempio possibile personalizzare il componente del bilanciamento del carico per definire impostazioni come protocollo e porta del controllo dell'integrità, algoritmo, persistenza e trasparenza.

Prerequisiti

[Definizione delle impostazioni del membro del bilanciamento del carico NSX-T](#).

Procedura

- 1 Fare clic sulla scheda **Generale** nella pagina **Server virtuale**.
- 2 Nel menu a discesa **Protocollo** selezionare il protocollo del traffico di rete da utilizzare per il bilanciamento del carico del server virtuale.

Le opzioni del protocollo sono HTTP, HTTPS, TCP e UDP.

I bilanciamenti del carico NSX-T non supportano la modalità passthrough SSL ma utilizzano la modalità di terminazione SSL. Se si specifica HTTPS, è necessario fornire le seguenti informazioni aggiuntive, che devono essere già presenti nel manager NSX-T:

- Nome del certificato nell'inventario dei certificati NSX-T. Il bilanciamento del carico presenta questo certificato ai client.
- Nome del profilo SSL client.

3 Immettere un valore della porta nella casella di testo **Porta**.

Il protocollo selezionato determina l'impostazione della porta predefinita.

Protocollo	Porta predefinita
HTTP	80
HTTPS	443
TCP	8080
UDP	nessun valore predefinito

I protocolli HTTP, HTTPS e TCP possono condividere una porta con UDP. Ad esempio, se il servizio 1 utilizza TCP, HTTP o HTTPS sulla porta 80, il servizio 2 può utilizzare UDP sulla porta 80. Se il servizio 1 utilizza UDP sulla porta 80, il servizio 2 non può utilizzare UDP sulla porta 80.

- 4** (Facoltativo) Immettere una descrizione per il componente del server virtuale.
- 5** Fare clic sulla scheda **Distribuzione** e vedere l'argomento [Definizione delle impostazioni di distribuzione del server virtuale per NSX-T](#) per continuare a definire il server virtuale nel componente del bilanciamento del carico NSX-T.

Definizione delle impostazioni di distribuzione del server virtuale per NSX-T

Selezionando l'opzione **Personalizza** quando si definisce un server virtuale, è possibile specificare le informazioni sui membri di un pool quali la porta sulla quale tali membri ricevono il traffico, il tipo di protocollo che il bilanciamento del carico di NSX-T può utilizzare per accedere a tale porta, l'algoritmo utilizzato per il bilanciamento del carico e le impostazioni di persistenza.

Un pool rappresenta un cluster di macchine in cui viene eseguito il bilanciamento del carico. Un membro del pool rappresenta una macchina in tale cluster.

Le impostazioni predefinite del protocollo del membro e della porta del membro corrispondono alle impostazioni del protocollo e della porta nella pagina **Generale**.

Il pool di macchine membro viene visualizzato nel valore dell'opzione **Membro** nell'interfaccia utente del componente del bilanciamento del carico blueprint. La voce **Membro** è impostata sul pool o sul cluster di macchine.

Prerequisiti

[Definizione delle impostazioni del membro del bilanciamento del carico NSX-T.](#)

Procedura

- 1 (Facoltativo) L'impostazione di **Protocollo membro** corrisponde al protocollo specificato nella scheda **Generale**. Questa impostazione definisce la modalità con cui il membro del pool riceve il traffico di rete.
- 2 (Facoltativo) Immettere un numero di porta nella casella di testo **Porta membro** per specificare la porta in cui il membro del pool riceve il traffico di rete.

Ad esempio, se la richiesta in entrata all'indirizzo IP virtuale (VIP) del bilanciamento del carico viene ricevuta tramite la porta 80, è possibile instradare la richiesta a un'altra porta, ad esempio la porta 8080, nei membri del pool.

- 3 (Facoltativo) Selezionare il metodo di bilanciamento dell'algoritmo per questo pool.

Le opzioni dell'algoritmo e i parametri dell'algoritmo per le opzioni che li richiedono vengono descritti nella tabella seguente.

Per le informazioni correlate, vedere *Aggiunta di un pool di server per il bilanciamento del carico* nella [documentazione del prodotto NSX-T](#).

Opzione	Descrizione e parametri dell'algoritmo
ROUND_ROBIN	Le richieste del client in entrata vengono assegnate una alla volta ad un elenco di server disponibili in grado di gestirle. Questa opzione consente di ignorare il peso dei membri del pool di server anche se configurato.
WEIGHTED ROUND ROBIN	A ciascun server viene assegnato un valore relativo al peso che indica le prestazioni di tale server rispetto ad altri server inclusi nel pool. Il valore determina il numero di richieste del client inviate ad un server rispetto ad altri server inclusi nel pool. Questo algoritmo di bilanciamento del carico consente di distribuire equamente il carico tra le risorse server disponibili.
IP-HASH	Seleziona un server in base a un hash dell'indirizzo IP di origine e al peso totale di tutti i server in esecuzione.
LEASTCONN	Distribuisce le richieste del client in più server in base al numero di connessioni già presenti sul server. Le nuove connessioni vengono inviate al server con il numero minore di connessioni. Questa opzione consente di ignorare il peso dei membri del pool di server anche se configurato.
WEIGHTED LEASTCONN	A ciascun server viene assegnato un valore relativo al peso che indica le prestazioni di tale server rispetto ad altri server inclusi nel pool. Il valore determina il numero di richieste del client inviate ad un server rispetto ad altri server inclusi nel pool. Questo algoritmo di bilanciamento del carico consente di utilizzare il valore relativo al peso per distribuire equamente il carico tra le risorse server disponibili. Per impostazione predefinita, il valore del peso è pari a 1 se tale valore non è configurato e l'avvio lento è abilitato.

4 (Facoltativo) Selezionare il metodo di persistenza per questo pool.

La persistenza tiene traccia dei dati della sessione e ne effettua l'archiviazione, come nel caso del membro del pool specifico che ha gestito la richiesta di un client. Con la persistenza, le richieste del client vengono indirizzate allo stesso membro del pool per la durata di una sessione o durante le sessioni successive. Per ulteriori informazioni sui metodi di persistenza, vedere *Configurazione dei profili permanenti* nella [documentazione del prodotto NSX-T](#).

- Selezionare **Nessuno** per fare in modo che le azioni della sessione non vengano archiviate per il richiamo successivo.
- Selezionare **Cookie** per inserire un cookie univoco allo scopo di identificare la sessione la prima volta che un client accede al sito. Al cookie verrà fatto riferimento nelle richieste successive per la persistenza della connessione al server appropriato.
- Selezionare **IP di origine** per tenere traccia delle sessioni in base all'indirizzo IP di origine. Quando un client richiede una connessione a un server virtuale che supporta la persistenza dell'affinità dell'indirizzo di origine, il bilanciamento del carico verifica se tale client si è già connesso in precedenza. In caso affermativo, restituisce il client allo stesso membro del pool.

5 Se si utilizza la persistenza dei cookie, immettere il nome del cookie.

6 (Facoltativo) Selezionare la modalità di inserimento del cookie dal menu a discesa **Modalità**.

Opzione	Descrizione
Inserisci	Creare un cookie univoco per identificare la sessione.
Prefisso	Aggiunge il cookie esistente.
Riscrivi	Sovrascrive il cookie esistente.

7 (Facoltativo) Immettere l'ora di scadenza della persistenza per il cookie in secondi.

Ad esempio, per un bilanciamento del carico L7 con un IP di origine TCP, se non vengono effettuate nuove connessioni TCP per l'ora di scadenza specificata si verifica un timeout della voce di persistenza, anche se le connessioni esistenti sono ancora attive.

8 (Facoltativo) Fare clic sulla scheda **Controllo di integrità** e vedere l'argomento [Definizione delle impostazioni di controllo dell'integrità del server virtuale per NSX-T](#) per continuare a definire il server virtuale nel componente del bilanciamento del carico NSX-T.

Definizione delle impostazioni di controllo dell'integrità del server virtuale per NSX-T

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile specificare in che modo, o se, il bilanciamento del carico NSX-T deve eseguire i controlli di integrità sui membri del pool all'interno del server virtuale.

Le impostazioni predefinite del protocollo e della porta del controllo dell'integrità corrispondono alle impostazioni del protocollo e della porta nella scheda **Generale**.

Per informazioni correlate, vedere la [documentazione di prodotto NSX-T](#). Tenere presente che nella documentazione relativa a NSX-T il membro del server virtuale viene definito membro del pool.

Prerequisiti

[Definizione delle impostazioni di distribuzione del server virtuale per NSX-T.](#)

Procedura

- 1 (Facoltativo) Selezionare un protocollo del controllo dell'integrità nel menu a discesa **Protocollo controllo di integrità** per specificare la modalità di accesso al membro del pool quando il bilanciamento del carico è in ascolto per determinare l'integrità del membro del pool.

Le opzioni del protocollo sono **Nessuno, HTTP, HTTPS, TCP, ICMP e UDP**.

È anche possibile accettare il protocollo predefinito specificato nella scheda Generale.

- 2 (Facoltativo) Immettere un valore nella casella **Porta controllo di integrità** per specificare la porta di ascolto del bilanciamento del carico per il monitoraggio dell'integrità del membro del server virtuale o del pool.

Tenere presente che nella documentazione relativa a NSX il membro del server virtuale viene definito membro del pool.

I protocolli HTTP, HTTPS e TCP possono condividere una porta con UDP. Ad esempio, se il servizio 1 utilizza TCP, HTTP o HTTPS sulla porta 80, il servizio 2 può utilizzare UDP sulla porta 80. Se il servizio 1 utilizza UDP sulla porta 80, il servizio 2 non può utilizzare UDP sulla porta 80.

- 3 Immettere il valore di **Intervallo**, in secondi, per l'esecuzione del ping di un server.
- 4 Immettere il valore di **Timeout** massimo, in secondi, entro il quale è necessario ricevere una risposta dal server virtuale.
- 5 Immettere un valore nel campo **Numero massimo tentativi** per specificare il numero massimo di tentativi di ping da eseguire prima di dichiarare inattivo il server.
- 6 Se è stato specificato un protocollo HTTP o HTTPS, immettere il **Metodo** da utilizzare per rilevare lo stato del server.
- 7 Se disponibile, immettere l'**URL** da utilizzare per rilevare lo stato del server. Si tratta dell'URL utilizzato per le opzioni di metodo GET e POST (include "/" per impostazione predefinita).
- 8 Se disponibili, immettere le stringhe di invio e ricezione nelle caselle di testo **Invia** e **Ricevi**.

Nella casella di testo **Invia** immettere la stringa da inviare al server dopo aver stabilito una connessione.

Nella casella di testo **Ricevi** immettere la stringa che si prevede di ricevere dal server. Il server viene considerato attivo solo quando la stringa ricevuta corrisponde a questa definizione.

- 9 Fare clic sulla scheda **Avanzate** e vedere l'argomento [Definizione delle impostazioni avanzate del server virtuale per NSX-T](#) per continuare a definire il server virtuale nel componente del bilanciamento del carico NSX-T.

Per specificare le opzioni di registrazione, vedere [Definizione delle opzioni di registrazione del bilanciamento del carico NSX-T](#).

Definizione delle impostazioni avanzate del server virtuale per NSX-T

Selezionando l'opzione **Personalizza** nella scheda **Generale**, è possibile personalizzare il componente di bilanciamento del carico NSX-T per specificare impostazioni quali il numero di connessioni simultanee che un singolo membro del pool è in grado di riconoscere e il numero massimo di connessioni simultanee che il server virtuale è in grado di elaborare.

Prerequisiti

[Definizione delle impostazioni generali del server virtuale per NSX-T](#).

Procedura

- 1 Immettere un valore nella casella di testo **Limite connessione** per specificare il numero massimo di connessioni simultanee in NSX-T che il server virtuale è in grado di elaborare.

Questa impostazione considera il numero di tutte le connessioni del membro.

Immettere il valore 0 per non specificare alcun limite.
- 2 Immettere un valore nella casella di testo **Limite frequenza di connessione** per specificare il numero massimo di richieste di connessione in entrata in NSX-T che è possibile accettare al secondo.

Questa impostazione considera il numero di tutte le connessioni del membro.

Immettere il valore 0 per non specificare alcun limite.
- 3 (Facoltativo) Selezionare la casella di controllo **Trasparente** per consentire ai membri del pool del bilanciamento del carico di visualizzare l'indirizzo IP delle macchine che richiamano il bilanciamento del carico.

Se la casella di controllo non è selezionata, i membri del pool del bilanciamento del carico visualizzano l'indirizzo IP di origine del traffico come un indirizzo IP interno del bilanciamento del carico.
- 4 Immettere un valore nella casella di testo **Numero massimo connessioni** per specificare il numero massimo di connessioni simultanee che un singolo membro del pool è in grado di riconoscere.

Se il numero di richieste in entrata supera questo valore, le richieste vengono aggiunte alla coda e quindi elaborate in base all'ordine di ricezione man mano che le connessioni sono disponibili.

Immettere il valore 0 per non specificare alcun valore massimo.
- 5 Fare clic su **OK** per completare la definizione del server virtuale.

- 6 Per specificare le opzioni di registrazione, vedere [Definizione delle opzioni di registrazione del bilanciamento del carico NSX-T](#), altrimenti fare clic su **Salva** o **Fine**.

Definizione delle opzioni di registrazione del bilanciamento del carico NSX-T

È possibile definire i tipi di azione di registrazione del bilanciamento del carico che vengono acquisiti e inclusi nei registri del bilanciamento del carico.

È possibile specificare un livello di registrazione per raccogliere i registri del traffico del bilanciamento del carico. I livelli di registrazione definiti per un componente qualsiasi del bilanciamento del carico NSX-T nel blueprint vengono applicati a tutti i bilanciamenti del carico definiti nel blueprint.

I livelli di registrazione includono le opzioni Debug, Informazioni, Avviso, Errore e Critico. Le opzioni Debug e Informazioni registrano le richieste degli utenti, mentre le opzioni Avviso, Errore e Critico non registrano le richieste degli utenti.

Per ulteriori informazioni sulla registrazione del bilanciamento del carico di NSX-T, vedere la *guida di amministrazione di NSX-T* nella [documentazione del prodotto NSX-T](#).

Prerequisiti

[Definizione delle impostazioni del membro del bilanciamento del carico NSX-T](#)

Procedura

- 1 Selezionare la scheda **Globale** nel componente del bilanciamento del carico nella tela di progettazione.
- 2 Selezionare una o più opzioni di registrazione dal menu a discesa **Livello di registrazione**.

Le impostazioni di registrazione vengono definite nel client Web di vSphere.

- Nessuno
- Emergenza
- Avviso
- Critico
- Errore
- Avviso
- Informazioni
- Debug

- 3 Selezionare un bilanciamento del carico piccolo, medio o grande.
- 4 Fare clic su **Salva**, quindi su **Fine**.

Uso dei componenti di sicurezza di NSX for vSphere in un blueprint

È possibile aggiungere componenti sicurezza di NSX for vSphere alla tela di progettazione per rendere le loro impostazioni configurate disponibili per uno o più componenti macchina di vSphere nel blueprint.

Gruppi di sicurezza, tag di sicurezza e criteri di protezione sono configurati all'esterno di vRealize Automation nell'applicazione NSX.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere e NSX-T. Per informazioni sulla configurazione di NSX, vedere *Administration Guide* nella [documentazione del prodotto NSX for vSphere](#) o nella [documentazione del prodotto NSX-T](#), a seconda dell'applicazione utilizzata.

È possibile aggiungere controlli di sicurezza ai blueprint configurando criteri di protezione e gruppi e tag di sicurezza per la risorsa di elaborazione vSphere in NSX. Dopo aver eseguito la raccolta dati, le configurazioni di sicurezza sono disponibili per essere selezionate in vRealize Automation.

Per una strategia di sicurezza di NSX for vSphere di esempio, consultare questo post del blog su [vRealize e NSX](#).

Gruppi di sicurezza esistenti e su richiesta per NSX for vSphere

Un gruppo di sicurezza è una raccolta di asset o di oggetti di raggruppamento provenienti dall'inventario di vSphere e mappata a un set di criteri di protezione, ad esempio regole firewall distribuite e integrazioni di servizi di sicurezza di terze parti, quali antivirus e rilevamento delle intrusioni. La funzione di raggruppamento consente di creare contenitori personalizzati a cui è possibile assegnare risorse, come ad esempio macchine virtuali e schede di rete, per garantire la protezione firewall distribuita. Dopo aver definito un gruppo, è possibile aggiungere il gruppo come origine o destinazione a una regola firewall per ottenere la protezione.

È possibile aggiungere gruppi di sicurezza vSphere esistenti o su richiesta a un blueprint, oltre ai gruppi di sicurezza specificati nella prenotazione.

È possibile creare uno o più gruppi di sicurezza su richiesta. È possibile selezionare uno o più criteri di sicurezza da configurare in un gruppo di sicurezza.

Un criterio di protezione è un insieme di servizi di analisi di endpoint, firewall e rete che possono essere applicati a un gruppo di sicurezza. È possibile aggiungere criteri di protezione a una macchina virtuale vSphere utilizzando un gruppo di sicurezza su richiesta in un blueprint. Non è possibile aggiungere un criterio di protezione direttamente in una prenotazione. Dopo la raccolta dati, in un blueprint è possibile selezionare i criteri di protezione definiti in NSX for vSphere per una risorsa di elaborazione.

I gruppi di sicurezza sono gestiti nella risorsa di origine. Per informazioni sulla gestione dei gruppi di sicurezza per i vari tipi di risorse, vedere la documentazione di NSX for vSphere.

Nota Quando è abilitato l'isolamento app, viene creato un criterio di protezione separato. L'isolamento app utilizza un firewall logico per bloccare tutto il traffico in ingresso e uscita da e verso le applicazioni nel blueprint. Le macchine componenti di cui viene eseguito il provisioning e che contengono un criterio di isolamento app possono comunicare tra loro ma non possono connettersi all'esterno del firewall, a meno che non vengano aggiunti al blueprint altri gruppi di sicurezza con criteri di protezione che consentono l'accesso.

Se un blueprint contiene un bilanciamento del carico ed è abilitato l'isolamento app, i VIP del bilanciamento del carico vengono aggiunti come set di IP al gruppo di sicurezza dell'isolamento app. Se un blueprint contiene un gruppo di sicurezza su richiesta associato a un livello macchina associato a un bilanciamento del carico, il gruppo di sicurezza su richiesta include il livello macchina, il set di IP e i VIP.

Tag di sicurezza esistenti per NSX for vSphere

È possibile aggiungere componenti tag di sicurezza esistenti per NSX for vSphere. Un tag di sicurezza è un oggetto qualificatore o una voce di categorizzazione utilizzabile come meccanismo di raggruppamento. È possibile definire i criteri che devono essere rispettati da un oggetto per poter essere aggiunto al gruppo di sicurezza creato. Ciò rende possibile l'inclusione di macchine tramite la definizione di criteri di filtro con una serie di parametri supportati, che permettono di articolare le ricerche in base ai criteri desiderati. Ad esempio, è possibile aggiungere a un gruppo di sicurezza tutte le macchine che hanno un tag di sicurezza specifico.

Aggiunta di un componente del gruppo di sicurezza esistente per NSX for vSphere

È possibile aggiungere un componente del gruppo di sicurezza di NSX for vSphere alla tela di progettazione in preparazione per associare le sue impostazioni a uno o più componenti macchina di vSphere nel blueprint.

È possibile utilizzare un componente gruppo di sicurezza esistente per aggiungere un gruppo di sicurezza NSX alla tela di progettazione e configurare le sue impostazioni per l'uso con i componenti macchina vSphere e i componenti Software o XaaS che si riferiscono a vSphere.

Per impostazione predefinita, durante la creazione di un blueprint vengono esposti i gruppi di sicurezza applicabili al tenant corrente. In particolare, i gruppi di sicurezza vengono resi disponibili se l'endpoint associato ha una prenotazione nel tenant corrente. Per ulteriori informazioni sul controllo dell'accesso tenancy, vedere [Controllo dell'accesso al tenant per gli oggetti di sicurezza in vRealize Automation](#).

Prerequisiti

- Creare e configurare gruppi di sicurezza per NSX. Vedere l'elenco di controllo per la configurazione di NSX in *Configurazione di vRealize Automation* e la guida di amministrazione di NSX for vSphere nella [documentazione del prodotto NSX for vSphere](#).
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.

Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.

- Esaminare i concetti relativi al componente di sicurezza. Vedere [Uso dei componenti di sicurezza di NSX for vSphere in un blueprint](#).
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **Gruppo di sicurezza esistente** nella tela di progettazione.
- 3 Selezionare un gruppo di sicurezza esistente dal menu a discesa **Gruppo di sicurezza**.
- 4 Fare clic su **OK**.
- 5 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Risultati

È possibile aggiungere impostazioni di sicurezza nella scheda **Sicurezza** di un componente macchina vSphere.

Aggiunta di un componente tag di sicurezza esistente per NSX for vSphere

È possibile aggiungere un componente tag di sicurezza esistente di NSX for vSphere alla tela di progettazione del blueprint in preparazione per associare le sue impostazioni a uno o più componenti vSphere nel blueprint.

È possibile utilizzare un componente tag di sicurezza per aggiungere un tag di sicurezza esistente di vSphere alla tela di progettazione e configurare le sue impostazioni per l'uso con i componenti macchina vSphere e i componenti Software che si riferiscono a vSphere.

Per impostazione predefinita, durante la creazione di un blueprint vengono esposti i gruppi di sicurezza applicabili al tenant corrente. In particolare, i tag di sicurezza vengono resi disponibili se l'endpoint associato ha una prenotazione nel tenant corrente. Per ulteriori informazioni sul controllo dell'accesso tenancy, vedere [Controllo dell'accesso al tenant per gli oggetti di sicurezza in vRealize Automation](#).

È possibile aggiungere più componenti di rete e sicurezza alla tela di progettazione.

Per ulteriori informazioni, vedere [Uso dei componenti di sicurezza di NSX for vSphere in un blueprint](#).

Prerequisiti

- Creare e configurare tag di sicurezza per NSX. Vedere l'elenco di controllo per la configurazione di NSX in *Configurazione di vRealize Automation* e la guida di amministrazione di *NSX for vSphere* nella [documentazione del prodotto NSX for vSphere](#).
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **Tag di sicurezza esistente** nella tela di progettazione.
- 3 Fare clic nella casella di testo **Tag di sicurezza** e selezionare un tag di sicurezza esistente.
- 4 Fare clic su **OK**.
- 5 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Risultati

È possibile aggiungere impostazioni di sicurezza nella scheda **Sicurezza** di un componente macchina vSphere.

Aggiunta di un componente gruppo di sicurezza su richiesta

È possibile aggiungere un componente gruppo di sicurezza NSX su richiesta alla tela di progettazione in preparazione all'associazione delle sue impostazioni a uno o più componenti macchina vSphere o ad altri tipi di componenti disponibili nel blueprint.

Quando si crea un gruppo di sicurezza su richiesta, è necessario aggiungere criteri di protezione per creare il gruppo. I criteri di protezione possono essere esposti a livello globale o nascosti per impostazione predefinita. I criteri sono visibili solo nei tenant per cui l'endpoint NSX associato ha una prenotazione in tali tenant.

Per impostazione predefinita, durante la creazione di un blueprint vengono esposti i gruppi di sicurezza applicabili al tenant corrente. In particolare, i gruppi di sicurezza vengono resi disponibili se l'endpoint associato ha una prenotazione nel tenant corrente. Per ulteriori informazioni sul controllo dell'accesso tenancy, vedere [Controllo dell'accesso al tenant per gli oggetti di sicurezza in vRealize Automation](#).

Prerequisiti

- Creare e configurare un criterio di sicurezza in NSX. Vedere la *guida di amministrazione di NSX*.
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Esaminare i concetti relativi al componente di sicurezza. Vedere [Uso dei componenti di sicurezza di NSX for vSphere in un blueprint](#).
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **Gruppo di sicurezza su richiesta** nella tela di progettazione.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Aggiungere uno o più criteri di protezione facendo clic sull'icona **Aggiungi** nell'area **Criteri di protezione** e selezionando i criteri di protezione disponibili.
- 5 Fare clic su **OK**.
- 6 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Risultati

È possibile aggiungere impostazioni di sicurezza nella scheda **Sicurezza** di un componente macchina vSphere.

Uso dei componenti di sicurezza di NSX-T in un blueprint

È possibile aggiungere un componente di sicurezza di rete di NSX-T alle tele di progettazione per rendere le relative impostazioni configurate disponibili per uno o più componenti macchina di vSphere associati nel blueprint.

Un gruppo NS esistente di NSX-T consente di assegnare risorse, ad esempio macchine virtuali e schede di rete, per la protezione firewall distribuita.

È possibile aggiungere controlli di sicurezza ai blueprint configurando gruppi NS per la risorsa di elaborazione vSphere in NSX-T. Dopo aver eseguito la raccolta dati, le configurazioni di sicurezza sono disponibili per essere selezionate in vRealize Automation. È possibile aggiungere un componente gruppo NS esistente di NSX-T al blueprint come origine o destinazione di una regola firewall.

I gruppi di sicurezza NSX-T NS sono gestiti all'esterno di vRealize Automation nell'applicazione NSX-T. Per informazioni sulla gestione dei gruppi NS, vedere la documentazione del prodotto NSX-T.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere e NSX-T. Per informazioni sulla configurazione di NSX, vedere *Administration Guide* nella [documentazione del prodotto NSX for vSphere](#) o nella [documentazione del prodotto NSX-T](#), a seconda dell'applicazione utilizzata.

Quando si distribuisce un blueprint che contiene un endpoint NSX-T, la distribuzione assegna un tag ai componenti NSX-T nella distribuzione. Il nome del tag e il nome della distribuzione corrispondono.

Quando è abilitato l'isolamento dell'app, viene creata una nuova sezione firewall con le regole per una distribuzione. L'isolamento app utilizza un firewall logico per bloccare tutto il traffico in ingresso e uscita da e verso le applicazioni nel blueprint. Le macchine componenti di cui viene eseguito il provisioning e che contengono un criterio di isolamento app possono comunicare tra loro ma non possono connettersi all'esterno del firewall, a meno che non vengano aggiunti al blueprint altri gruppi NS con regole di protezione che consentono l'accesso.

Se un blueprint contiene un bilanciamento del carico ed è abilitato l'isolamento app, i VIP del bilanciamento del carico vengono aggiunti come set di IP al gruppo di sicurezza dell'isolamento app. Se un blueprint contiene un gruppo di sicurezza su richiesta associato a un livello macchina associato a un bilanciamento del carico, il gruppo di sicurezza su richiesta include il livello macchina, il set di IP e i VIP.

Per NSX-T, l'isolamento app è l'unico gruppo NS su richiesta creato. Contiene un set di IP che include VIP di bilanciamento del carico e IP esterni di rete uno a molti NAT.

Per ulteriori informazioni sulle considerazioni relative a distribuzione e topologia specifiche di NSX-T, vedere [Informazioni sulle topologie di distribuzione di NSX-T per i servizi di rete, la sicurezza e le configurazioni del bilanciamento del carico](#).

Aggiunta di un componente NSGroup di NSX-T

È possibile aggiungere un componente NSGroup esistente di NSX-T alla tela di progettazione e configurare le relative impostazioni per l'utilizzo con componenti macchina vSphere e con gli altri componenti associati, ad esempio componenti software e di rete.

Un componente NSGroup di NSX-T può contenere una combinazione di set di indirizzi IP, set di indirizzi MAC, porte logiche, switch logici e altri componenti NSGroup. È possibile specificare componenti NSGroup come origini e destinazioni nelle regole del firewall. Per ulteriori informazioni sulle caratteristiche di NSGroup, vedere *Creazione di un componente NSGroup* in *NSX-T Administration Guide* nella [documentazione del prodotto NSX-T](#).

Nota La sicurezza di NSGroup viene applicata alle macchine virtuali connesse alle reti nascoste gestite da NSX-T. Se una macchina virtuale è connessa a un dvPortGroup di vSphere la micro-segmentazione non è disponibile per tale rete.

Per impostazione predefinita, quando si crea o si modifica un blueprint vengono esposti i componenti NSGroup applicabili al tenant corrente. I gruppi di sicurezza vengono resi disponibili se l'endpoint associato ha una prenotazione nel tenant corrente. Per ulteriori informazioni sul controllo dell'accesso tenancy, vedere [Controllo dell'accesso al tenant per gli oggetti di sicurezza in vRealize Automation](#).

Prerequisiti

- Creare e configurare un componente NSGroup in NSX-T. Vedere [Elenco di controllo per la preparazione della configurazione di rete e sicurezza di NSX](#).
- Verificare che l'inventario di NSX sia stato eseguito in modo corretto per il cluster.
Per utilizzare le configurazioni di NSX in vRealize Automation, è necessario eseguire la raccolta dati.
- Esaminare i concetti relativi al componente di sicurezza. Vedere [Uso dei componenti di sicurezza di NSX-T in un blueprint](#).
- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **NSGroup di NSX-T** nella tela di progettazione.
- 3 Selezionare un componente NSGroup dal menu a discesa.
- 4 Se richiesto, immettere un endpoint associato.
- 5 Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Risultati

È possibile aggiungere impostazioni di sicurezza nella scheda **Sicurezza** di un componente macchina vSphere.

Associazione di componenti di rete e sicurezza

Quando si trascinano componenti di rete e sicurezza in una tela di progettazione, le loro impostazioni diventano disponibili per la configurazione dei componenti macchina nel blueprint. Una volta definite le impostazioni di rete e sicurezza per la macchina, è possibile eventualmente associare le impostazioni da un componente bilanciamento del carico.

Dopo aver aggiunto un componente di rete o sicurezza NSX nella tela di progettazione e averne definito le impostazioni disponibili, è possibile aprire le schede di rete e sicurezza di un componente macchina vSphere nella tela e configurarne le impostazioni.

È possibile trascinare un componente di rete NAT su richiesta sulla tela di progettazione e associarlo a un componente macchina vSphere o a un componente di bilanciamento del carico NSX nel blueprint.

Le impostazioni dei componenti di rete e sicurezza aggiunte al blueprint derivano dalla configurazione di NSX for vSphere e NSX-T. Per informazioni sulla configurazione di NSX, vedere *Administration Guide* nella [documentazione del prodotto NSX for vSphere](#) o nella [documentazione del prodotto NSX-T](#), a seconda dell'applicazione utilizzata.

Nota Se un blueprint contiene un bilanciamento del carico ed è abilitato l'isolamento app, i VIP del bilanciamento del carico vengono aggiunti come set di IP al gruppo di sicurezza dell'isolamento app. Se un blueprint contiene un gruppo di sicurezza su richiesta associato a un livello macchina associato a un bilanciamento del carico, il gruppo di sicurezza su richiesta include il livello macchina, il set di IP e i VIP.

Per informazioni sull'uso delle regole NAT per consentire a una porta TCP o UDP di eseguire la mappatura da un indirizzo IP esterno di un Edge (porta di origine) a un indirizzo IP privato nel componente di rete NAT (porta di destinazione), vedere [Creazione e utilizzo di regole NAT per NSX for vSphere](#) o [Creazione e utilizzo di regole NAT per NSX-T](#).

Per ulteriori informazioni sulle considerazioni relative a distribuzione e topologia specifiche di NSX-T, vedere [Informazioni sulle topologie di distribuzione di NSX-T per i servizi di rete, la sicurezza e le configurazioni del bilanciamento del carico](#).

Configurazione di un blueprint per il provisioning da un OVF

È possibile utilizzare un OVF per definire le proprietà della macchina vSphere e le impostazioni hardware che in genere vengono definite nelle pagine di configurazione del blueprint in vRealize Automation o tramite programmazione utilizzando le API REST di vRealize Automation o vRealize CloudClient.

È inoltre possibile importare le impostazioni da un OVF per definire un set di valori per il profilo di un componente immagine. I blueprint parametrizzati utilizzano i tipi di profili componente immagine e dimensione.

OVF è uno standard open source per la creazione di pacchetti e la distribuzione di applicazioni software per macchine virtuali.

Il provisioning di OVF è simile alla clonazione, ad eccezione del fatto che la macchina di origine è un modello OVF ospitato su un server o un sito Web anziché un modello di macchina virtuale ospitato in vCenter.

Un file OVF viene in genere utilizzato per descrivere una singola macchina virtuale o appliance virtuale. Il file può contenere informazioni sul formato di un file di immagine del disco virtuale e una descrizione dell'hardware virtuale da emulare per eseguire il sistema operativo o l'applicazione contenuti nell'immagine del disco. Un file OVA è un pacchetto di appliance virtuale che contiene i file utilizzati per descrivere una macchina virtuale, tra cui un file descrittore OVF, file manifesto e di certificato facoltativi e altri file correlati.

L'opzione di provisioning `ImportOvfWorkflow` è disponibile in un componente macchina vSphere quando si definisce un blueprint. È disponibile inoltre quando si definisce un set di valori per il profilo di un componente immagine nel dizionario di proprietà.

È possibile aggiungere impostazioni di configurazione del blueprint in un OVF per descrivere i seguenti tipi di informazioni:

- Allocazioni minime di CPU, memoria e storage.
- Proprietà personalizzate configurabili dall'utente.
- Impostazioni del profilo del componente per la parametrizzazione del blueprint.

I file OVF e OVA con più macchine non sono supportati.

Considerazioni essenziali includono le seguenti istruzioni:

- I file OVF e i pacchetti OVA sono supportati.
- È supportata l'autenticazione di base mediante nome utente e password per il server HTTP in cui si trova il file OVF o OVA ospitato. L'URL specificato viene convalidato nel blueprint.
- I dati dei file OVF e OVA non sono raccolti da vCenter Server.
- Sono supportate le sottoscrizioni EBS.
- Quando si importano impostazioni OVF configurabili dall'utente nel blueprint, è possibile definire proprietà personalizzate.
- È possibile aggiungere, modificare o rimuovere impostazioni ottenute da un'importazione OVF quando si richiede il provisioning di una macchina vSphere.
- È possibile aggiungere, modificare o rimuovere le impostazioni durante la riconfigurazione della macchina.

Definizione delle impostazioni del blueprint per un componente vSphere utilizzando un OVF

È possibile importare le impostazioni da un OVF per semplificare il processo di configurazione delle impostazioni del componente della macchina vSphere in un blueprint di vRealize Automation.

Questa procedura presuppone che l'utente disponga di una conoscenza di base del processo di creazione del blueprint di vRealize Automation.

Prerequisiti

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Soddisfare i prerequisiti rimanenti specificati in [Configurazione del blueprint di una macchina](#).

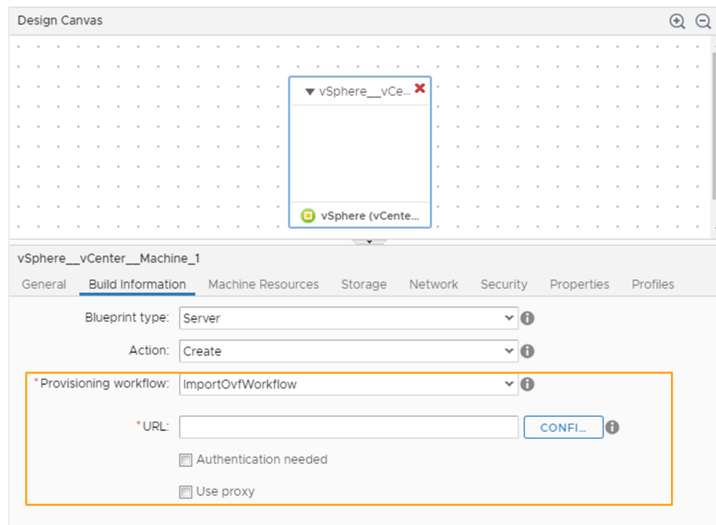
Procedura

- 1 Scegliere **Progettazione > Blueprint**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere un nome una descrizione per il blueprint e fare clic su **OK**.

- 4 Fare clic su **Tipi di macchine** nell'area Categorie e trascinare un componente **Macchina vSphere (vCenter)** nella tela di progettazione.
- 5 Fare clic sulla scheda **Informazioni build** e specificare le seguenti opzioni:

- **Tipo di blueprint:** Server
- **Azione:** Crea
- **Workflow di provisioning:** ImportOvfWorkflow

L'impostazione ImportOvfWorkflow consente di rendere disponibile l'opzione **URL**.



- 6 Specificare la posizione del file OVF.
 - Immettere il percorso dell'URL dell'OVF nel formato `https://server/folder/name.ovf` o `name.oVa`.
Se si abilita l'autenticazione nel server che ospita il file OVF, immettere le credenziali dell'utente di cui eseguire l'autenticazione.
 - Se il file OVF è ospitato su un sito Web ed è stato creato un endpoint Proxy da utilizzare nell'accesso al sito Web, scegliere **Usa proxy** e selezionare l'endpoint Proxy disponibile.

- 7 Fare clic su **Configura**.

Nota Se viene visualizzato un messaggio di errore di autenticazione, significa che il server su cui è ospitato l'OVF richiede le credenziali di autenticazione. In questo caso, selezionare la casella di controllo **Autenticazione necessaria**, immettere le credenziali specificando **Nome utente** e **Password** richieste per l'autenticazione nel server HTTP in cui si trova l'OVF e fare nuovamente clic su **Configura**.

L'opzione Configura apre una procedura guidata nella quale vengono visualizzate tutte le proprietà configurabili dall'utente e i valori importabili dall'OVF come proprietà personalizzate. Se non sono disponibili proprietà configurabili da importare, il riquadro è vuoto.

- a Utilizzare la procedura guidata per accettare i valori predefiniti da importare o modificare i valori per il blueprint prima dell'importazione.
- b Fare clic su **OK** per importare le proprietà e i valori.

Tutte le proprietà configurabili dall'utente contenute nel modello OVF vengono importate nel blueprint come proprietà personalizzate di vRealize Automation modificabili, precedute da `VMware.Ovf`, mentre altre vengono importate come proprietà nascoste non destinate alla modifica dopo l'importazione.

- 8** Fare clic sulla scheda **Risorse macchina** per visualizzare i risultati dell'importazione di OVF riportati nelle voci dei valori minimi per le opzioni **CPU**, **Memoria (MB)** e **Storage (GB)**.

È possibile modificare qualsiasi di questi valori dopo l'importazione.

- 9** Fare clic sulla scheda **Storage** per visualizzare i risultati dell'importazione di OVF.
- 10** Fare clic su **Proprietà > Proprietà personalizzate** per visualizzare i risultati dell'importazione di OVF.
- 11** Fare clic su **Salva**.

Operazioni successive

Continuare a definire le impostazioni del blueprint o fare clic su **Fine**.

Definizione di un set di valori dell'immagine per un profilo componente mediante un OVF

È possibile importare impostazioni da un OVF per creare uno o più set di valori per un profilo componente immagine da utilizzare in un blueprint di vRealize Automation parametrizzato.

Dopo aver importato le definizioni dei set di valori per il profilo componente Image, è possibile aggiungere uno o più set di valori al profilo componente per un componente macchina vSphere in un blueprint. Quando un utente richiede un elemento del catalogo, può selezionare un elemento Image disponibile ed effettuare la distribuzione utilizzando i parametri definiti nel set di valori dell'immagine.

Quando si importa il file OVF, le proprietà e i valori configurabili dall'utente presenti nell'OVF non vengono importati come proprietà personalizzate nel set di valori. Se si desidera utilizzare le nuove proprietà personalizzate dell'OVF importato in relazione al set di valori dell'immagine, è necessario definire manualmente le nuove proprietà personalizzate nel componente macchina vSphere o nel blueprint complessivo. Le proprietà personalizzate create nel blueprint parametrizzato devono essere applicabili al set di valori per ogni immagine del profilo componente.

Nota Le proprietà personalizzate dell'OVF per vRealize Automation non sono applicabili alle proprietà personalizzate dell'OVF per vSphere. È consigliabile creare un set di valori dell'immagine per vRealize Automation e un set di valori dell'immagine per vSphere.

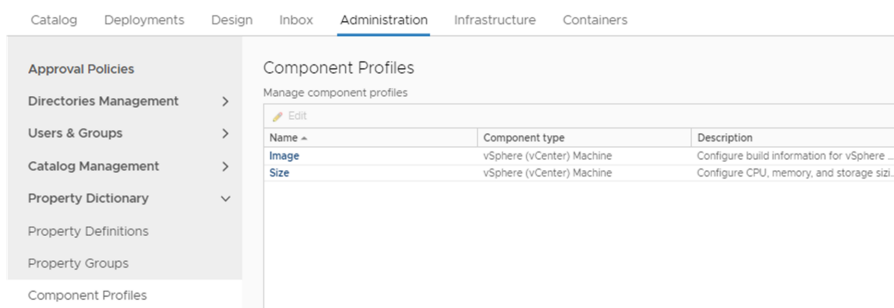
Per ulteriori informazioni sull'utilizzo dei profili componente per la parametrizzazione del blueprint, vedere [Aspetti da conoscere e utilizzo della parametrizzazione dei blueprint](#).

Prerequisiti

- Accedere a vRealize Automation come amministratore con diritti di accesso di **amministratore tenant** e **amministratore IaaS**.

Procedura

- 1 Selezionare **Amministrazione > Dizionario proprietà > Profili componente**.



- 2 Fare clic su **Immagine** nella colonna Nome.

Vengono visualizzate le informazioni relative alla proprietà del componente immagine fornita.

- 3 Fare clic sulla scheda **Set di valori**.

- 4 Per definire un nuovo set di valori, fare clic su **Nuovo** e configurare le impostazioni di Image.

- a Inserire un valore nel campo **Nome visualizzato** da accordare al delimitatore ValueSet, ad esempio **ProdOVF**.
- b Accettare il valore predefinito presente nella casella di testo **Nome** o inserire un nome personalizzato.
- c Inserire una descrizione, come ad esempio **Impostazioni build per scenario di clonazione A** nella casella di testo **Descrizione**.

- d Selezionare **Attivo** o **Inattivo** nel menu a discesa **Stato**.

Selezionare **Attivo** per consentire la visibilità del set di valori nel modulo di richiesta di provisioning del catalogo.

- e Selezionare l'azione **Crea**.

- f Selezionare **Server** o **Desktop** come tipo di blueprint.

- g Selezionare il workflow di provisioning **ImportOvfWorkflow**.

- h Immettere il percorso dell'URL dell'OVF nel formato `https://server/folder/name.ovf` o `name.ova`.

- i Se si abilita l'autenticazione nel server che ospita il file OVF, immettere le credenziali dell'utente di cui eseguire l'autenticazione.

- j Se il file OVF è ospitato su un sito Web ed è stato creato un endpoint Proxy da utilizzare per l'accesso al sito Web, scegliere **Usa proxy** e selezionare l'endpoint Proxy disponibile.

5 Fare clic su **Salva**.

6 Terminata la definizione delle impostazioni, fare clic su **Fine**.

Operazioni successive

Dopo aver creato l'immagine e importato il file OVF per definire il set di valori dell'immagine, è possibile aggiungere l'immagine a un componente macchina vSphere in un blueprint.

Uso dei componenti di un contenitore nei blueprint

È possibile configurare e utilizzare i componenti di un contenitore nel blueprint.

Dopo che l'amministratore dei contenitori ha creato le definizioni dei contenitori in Contenitori per vRealize Automation, un architetto di contenitori può aggiungere e configurare i componenti del contenitore per i blueprint di vRealize Automation nella tela di progettazione.

Impostazioni per i componenti contenitore

È possibile configurare le impostazioni e le opzioni dei blueprint per un Contenitori per vRealize Automation componente contenitore nella vRealize Automation tela di progettazione.

Scheda **Generale**

Configurare le impostazioni generali per il componente contenitore del blueprint nella tela di progettazione.

Tabella 3-33. Impostazioni della scheda Generale

Impostazione	Descrizione
Nome	Inserire un nome per il componente contenitore nel blueprint.
Descrizione	Testo che riepiloga il componente contenitore a vantaggio di altri architetti.

Tabella 3-33. Impostazioni della scheda **Generale** (continua)

Impostazione	Descrizione
Immagine	Consente di specificare il nome completo d'un'immagine in un registro gestito, come un registro privato o un registro del servizio Docker Hub (ad esempio registry.hub.docker.com/library/python).
Comandi	Inserire un comando appropriato all'immagine specificata, ad esempio python app.py. Il comando verrà eseguito nel momento in cui viene avviata la procedura di provisioning dei contenitori.
Collegamenti	I collegamenti rappresentano un altro modo di collegare i contenitori a un singolo host o fra più host. Specificare uno o più servizi a cui collegare il contenitore, ad esempio redis o datadog.

Scheda **Rete**

Configurare le impostazioni generali per il componente contenitore del blueprint nella tela di progettazione.

È possibile collegare un contenitore a una rete. La rete viene rappresentata come componente rete di contenitore nella tela di progettazione. Le informazioni sulle reti disponibili sono indicate nella pagina Rete del modulo del componente contenitore.

Tabella 3-34. Impostazioni della scheda **Rete**

Impostazione	Descrizione
Reti	Consente di specificare le reti esistenti definite per l'immagine selezionata e È inoltre possibile creare una nuova rete. Quando si aggiunge un componente contenitore di rete al modulo di progettazione, le reti specificate in questo campo verranno elencate come opzioni selezionabili.
Binding di porta	Consente di specificare i binding di porta per la rete selezionata. I binding di porta sono formati da host protocollo, porta host e porta del contenitore.
Pubblica tutte le porte	Selezionare questa casella di controllo per rendere visibili le porte utilizzate nell'immagine del contenitore a tutti gli utenti.
Nome host	Consente di specificare il nome host del contenitore. Se non viene specificato un nome, viene automaticamente inserito il nome del componente contenitore nel blueprint.
Modalità di rete	Consente di specificare lo stack di rete del contenitore. Se non viene specificato un valore, il contenitore viene configurato nella modalità di collegamento con bridging.

Scheda **Storage**

Configurare le impostazioni di storage per il componente contenitore del blueprint nella tela di progettazione.

Tabella 3-35. Impostazioni della scheda **Storage**

Impostazioni	Descrizione
Volumi	Consente di specificare i volumi di storage mappati dall'host da utilizzare con il contenitore.
Volumi da	Consente di specificare i volumi di storage da ereditare da un altro contenitore.
Directory di lavoro	Consente di specificare la directory da cui eseguire i comandi.

Scheda **Criterio**

Configurare le impostazioni relative ai criteri, ad esempio il criterio di distribuzione e i vincoli di affinità per il componente contenitore del blueprint nella tela di progettazione.

Tabella 3-36. Impostazioni della scheda **Criterio**

Impostazioni	Descrizione
Criterio di distribuzione	Consente di specificare un criterio di distribuzione per impostare le preferenze per il set di host da utilizzare per la distribuzione del contenitore. È possibile associare i criteri di distribuzione a definizioni di host, criteri e contenitori, così da poter definire le preferenze in merito a host, criteri e quote al momento della distribuzione del contenitore. È possibile aggiungere un criterio di distribuzione mediante la scheda Contenitori in vRealize Automation.
Dimensioni cluster	Consente di specificare il numero di istanze da generare come cluster a partire dal contenitore.
Criterio di riavvio	Specificare un criterio di riavvio per definire come viene riavviato un contenitore all'uscita.
N. massimo di riavvii	Se è stato selezionato In caso di errore come criterio di riavvio, è possibile specificare il numero massimo di riavvii.
Condivisioni CPU	Consente di specificare il numero di quote di CPU allocate per la risorsa con provisioning effettuato.
Limite di memoria	Consente di specificare un numero compreso fra 0 e la memoria disponibile nella zona di posizionamento. Questo valore rappresenta la memoria totale disponibile per le risorse in questo posizionamento. 0 indica che non sono presenti limiti.

Tabella 3-36. Impostazioni della scheda **Criterio** (continua)

Impostazioni	Descrizione
Swap memoria	Limite della memoria totale.
Vincoli di affinità	<p>Indica le regole per il provisioning dei contenitori sugli stessi host o in altri.</p> <ul style="list-style-type: none"> ■ Tipo di affinità In caso di anti-affinità, i contenitori vengono posizionati su host diversi, altrimenti si trovano sullo stesso host. ■ Servizio Il nome del servizio disponibile sul menu a discesa corrisponde al nome del componente contenitore specificato nel campo Nome della scheda Generale. ■ Vincolo Se è presente un vincolo fisso, il provisioning non può essere eseguito se è impossibile rispettare il vincolo. Se è presente un vincolo flessibile, il provisioning viene eseguito anche se risulta impossibile rispettare il vincolo.

Scheda Ambiente

Configurare le impostazioni relative all'ambiente, ad esempio il binding di proprietà per il contenitore del blueprint nella tela di progettazione.

Tabella 3-37. Impostazioni della scheda **Ambiente**

Impostazione	Descrizione
Nome	Il nome della variabile.
Binding	<p>Esegue il binding della variabile a un'altra proprietà che è una parte del modello. Quando si seleziona il binding, si deve immettere un valore nella sintassi <code>_resource~TemplateComponent~TemplateComponentProperty</code>.</p>
Valore	Il valore della variabile di ambiente o, se è stato selezionato il binding, il valore della proprietà di cui eseguire il binding.

Scheda Proprietà

Configurare proprietà singole o gruppi di proprietà personalizzate per il componente contenitore del blueprint nella tela di progettazione.

Se si seleziona la scheda **Gruppi di proprietà** e si fa clic su **Aggiungi**, saranno disponibili le seguenti opzioni:

- Proprietà dell'host del contenitore con autenticazione mediante certificato
- Proprietà dell'host del contenitore con autenticazione mediante utente/password

Se sono stati definiti gruppi di proprietà aggiuntivi, verranno anch'essi inclusi nell'elenco.

Se si seleziona la scheda **Proprietà personalizzate** e si fa clic su **Aggiungi**, è possibile aggiungere proprietà personalizzate individuali al componente contenitore.

Tabella 3-38. Impostazioni della scheda **Proprietà per **Proprietà personalizzate****

Impostazione	Descrizione
Nome	Consente di specificare il nome di una proprietà personalizzata o di selezionare una proprietà personalizzata disponibile dal menu a discesa.
Valore	Consente di specificare o di modificare un valore da associare al nome della proprietà personalizzata.
Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.
Sovrascrivibile	È possibile specificare che il valore di una proprietà può essere sovrascritto dalla persona successiva che utilizza tale proprietà. Si tratta in genere di un altro architetto, ma se si seleziona Mostra nella richiesta , gli utenti business saranno in grado di visualizzare e modificare i valori della proprietà al momento di richiedere gli elementi del catalogo.
Mostra nella richiesta	Se si desidera consentire agli utenti finali di visualizzare il nome e il valore della proprietà, si può scegliere di visualizzare la proprietà nel modulo della richiesta di provisioning di una macchina. Per consentire agli utenti di fornire un valore, è inoltre necessario selezionare Sovrascrivibile .

Scheda **Configurazione integrità**

Consente di specificare la modalità di configurazione dei controlli di stato per la componente contenitore del blueprint nella tela di progettazione.

Tabella 3-39. Impostazioni della scheda **Configurazione integrità**

Impostazione Modalità	Descrizione
Nessuno	Valore predefinito. Non sono stati configurati controlli di stato.
HTTP	<p>Se si seleziona HTTP, è necessario specificare un'API a cui accedere nonché un metodo e una versione HTTP da utilizzare. L'API è relativa. Non è necessario inserire l'indirizzo del contenitore. È inoltre possibile specificare un periodo di timeout per il funzionamento e impostare una soglia di integrità.</p> <p>Ad esempio, una soglia di integrità pari a 2 indica che, affinché il contenitore venga considerato integro, devono essere portate a termine correttamente due chiamate consecutive con stato RUNNING . Ad esempio, una soglia di non integrità pari a 2 indica che, affinché il contenitore venga considerato non integro, non devono andare a buon fine due chiamate, che devono presentare lo stato ERROR. Per gli stati intermedi fra la soglia di integrità e di non integrità, lo stato del contenitore è DEGRADED.</p>
Connessione TCP	Se si seleziona Connessione TCP , sarà necessario inserire solo una porta per il contenitore. Il controllo dello stato tenta di stabilire una connessione TCP con il contenitore mediante la porta specificata. È inoltre possibile specificare un valore di timeout per il funzionamento e impostare una soglia di integrità o di non integrità con HTTP.
Comando	Se si seleziona Comando , è necessario inserire un comando da eseguire sul contenitore. L'esito del controllo di stato è determinato dall'esito del comando.
Ignora controllo di integrità durante il provisioning	Deselezionare questa opzione per forzare il controllo dell'integrità durante il provisioning. Quando si forza il controllo dell'integrità, il provisioning del contenitore non viene considerato completato finché non viene eseguito un controllo dell'integrità con esito positivo.
Distribuisce automaticamente	Ridistribuzione automatica di contenitori quando si trovano nello stato ERRORE.

Scheda **Configurazione registrazione**

Specificare la modalità di registrazione nonché le opzioni di registrazione facoltative per il componente contenitore del blueprint nella tela di progettazione.

Tabella 3-40. Impostazioni scheda **Configurazione registrazione**

Impostazione	Descrizione
Driver	Selezionare un formato di registrazione dal menu a discesa.
Opzioni	Consente di specificare le opzioni relative ai driver mediante un formato per il nome e il valore appropriato al formato di registrazione.

Utilizzo di proprietà di contenitori e gruppi di proprietà in un blueprint

È possibile aggiungere gruppi di proprietà predefiniti a un componente di contenitori in un blueprint di vRealize Automation. Quando si esegue il provisioning di macchine con un blueprint che contiene tali proprietà, la macchina sottoposta a provisioning viene registrata come macchina host Docker Container.

Contenitori per vRealize Automation fornisce i seguenti due gruppi di proprietà personalizzate specifiche dei contenitori. Quando si aggiunge un componente di contenitori a un blueprint, è possibile aggiungere tali gruppi di proprietà al contenitore per registrare le macchine sottoposte a provisioning come host di contenitori.

- Proprietà dell'host del contenitore con autenticazione mediante certificato
- Proprietà dell'host del contenitore con autenticazione mediante utente/password

Tali gruppi di proprietà sono visibili in vRealize Automation quando si seleziona **Amministrazione > Dizionario proprietà > Gruppi di proprietà**.

Poiché i gruppi di proprietà sono condivisi da tutti i tenant, se si opera in ambiente multi-tenant, si consiglia di clonare e personalizzare le proprietà. Assegnando nomi univoci ai gruppi di proprietà e alle proprietà nei gruppi, è possibile modificarli per definire valori personalizzati da utilizzare in un tenant specifico.

Le proprietà più comunemente utilizzate sono `Container.Auth.PublicKey` e `Container.Auth.PrivateKey` in cui l'amministratore contenitori fornisce il certificato client per l'autenticazione con l'host dei contenitori.

Tabella 3-41. Proprietà personalizzate di Contenitori

Proprietà	Descrizione
<code>containers.ipam.driver</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica il driver IPAM da utilizzare quando si aggiunge un componente di rete di Contenitori a un blueprint. I valori supportati dipendono dai driver installati nell'ambiente host del contenitore in cui vengono utilizzati. Ad esempio, un valore supportato potrebbe essere <code>infoblox</code> o <code>calico</code> , a seconda dei plug-in IPAM installati nell'host del contenitore.
<code>containers.network.driver</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica il driver di rete da utilizzare quando si aggiunge un componente di rete di Contenitori a un blueprint. I valori supportati dipendono dai driver installati nell'ambiente host del contenitore in cui vengono utilizzati. Per impostazione predefinita, i driver di rete forniti con Docker includono <code>bridge</code> , <code>overlay</code> e <code>macvlan</code> , mentre i driver di rete forniti con VCH (Virtual Container Host) includono il driver <code>bridge</code> . È possibile che siano disponibili anche driver di rete di terze parti, ad esempio <code>weave</code> e <code>calico</code> , a seconda dei plug-in di rete installati nell'host del contenitore.
<code>Container</code>	Riservata all'utilizzo esclusivo con i contenitori. Il valore predefinito è <code>App.Docker</code> . Questo valore è obbligatorio. Non modificare questa proprietà.
<code>Container.Auth.User</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica il nome utente utilizzato per la connessione all'host di Contenitori.
<code>Container.Auth.Password</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica la password associata al nome utente o la password chiave pubblica o privata da utilizzare. Per la proprietà sono supportati valori codificati.
<code>Container.Auth.PublicKey</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica la chiave pubblica utilizzata per la connessione all'host di Contenitori.
<code>Container.Auth.PrivateKey</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica la chiave privata utilizzata per la connessione all'host di Contenitori. Per la proprietà sono supportati valori codificati.
<code>Container.Connection.Protocol</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica il protocollo di comunicazione. Il valore predefinito è <code>API</code> . Questo valore è obbligatorio. Non modificare questa proprietà.
<code>Container.Connection.Scheme</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica lo schema di comunicazione. Il valore predefinito è <code>https</code> .
<code>Container.Connection.Port</code>	Riservata all'utilizzo esclusivo con i contenitori. Specifica la porta di connessione di Contenitori. Il valore predefinito è <code>2376</code> .

Tabella 3-41. Proprietà personalizzate di Contenitori (continua)

Proprietà	Descrizione
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.MachineActivated	Riservata all'utilizzo esclusivo con i contenitori. Specifica la proprietà del gestore degli eventi utilizzata per esporre tutte le proprietà di Contenitori. La proprietà è utilizzata per la registrazione di un host di cui si è eseguito il provisioning. Il valore predefinito è Container*. Questo valore è obbligatorio. Non modificare questa proprietà.
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.Disposing	Riservata all'utilizzo esclusivo con i contenitori. Specifica la proprietà del gestore degli eventi utilizzata per esporre tutte le proprietà di Contenitori elencate sopra. La proprietà è utilizzata per l'annullamento della registrazione di un host di cui si è eseguito il provisioning. Il valore predefinito è Container*. Questo valore è obbligatorio. Non modificare questa proprietà.

Utilizzo di componenti di rete di Contenitori nella tela di progettazione

È possibile aggiungere uno o più componenti di rete di Contenitori alla tela di progettazione e configurare le relative impostazioni per i componenti della macchina vSphere nel blueprint.

È possibile aggiungere `containers.ipam.driver` e `containers.network.driver` al componente durante l'aggiunta al blueprint.

Aggiunta di un componente rete del contenitore

È possibile aggiungere informazioni sulla rete del contenitore a un blueprint di vRealize Automation che contiene componenti del contenitore.

È possibile configurare i contenitori in Contenitori per vRealize Automation utilizzando la scheda vRealize Automation **Contenitori** e quindi aggiungerli, con le relative impostazioni di rete, come componenti in un blueprint utilizzando le opzioni disponibili nella scheda vRealize Automation **Progettazione**.

Prerequisiti

- Accedere a vRealize Automation come **architetto contenitore**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Per visualizzare l'elenco dei componenti di rete e sicurezza disponibili, fare clic su **Rete e sicurezza** nella sezione Categorie.
- 2 Trascinare un componente **Rete contenitore** nella tela di progettazione.
- 3 Per etichettare in modo univoco un componente nella tela di progettazione, immettere il nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione del componente nella casella di testo **Descrizione**.

- 5 (Facoltativo) Se non si desidera specificare impostazioni IPAM esterne, selezionare la casella di controllo **Esterno**.

Se si seleziona la casella di controllo **Esterno**, la scheda **Configurazione IPAM** viene rimossa.

- 6 Fare clic sulla scheda **Configurazione IPAM** per immettere una nuova subnet, un nuovo intervallo IP e un nuovo gateway per la rete specificata in un componente del contenitore del blueprint o per modificarne i valori esistenti.

La configurazione IPAM è applicabile alle nuove reti create mediante vRealize Automation e non a quelle create in precedenza mediante Docker o un'altra applicazione contenitore supportata. Queste impostazioni non vengono convalidate e il provisioning non riesce se le impostazioni si sovrappongono a quelle di altre reti. Ad esempio, la subnet e il gateway devono essere univoci all'interno dell'host del contenitore.

- 7 Fare clic sulla scheda **Proprietà** per specificare le proprietà personalizzate del componente.

Se si seleziona la scheda **Gruppi di proprietà** e si fa clic su **Aggiungi**, saranno disponibili le seguenti opzioni:

- Proprietà dell'host del contenitore con autenticazione mediante certificato
- Proprietà dell'host del contenitore con autenticazione mediante utente/password

Se sono stati definiti gruppi di proprietà aggiuntivi, verranno anch'essi inclusi nell'elenco.

Se si seleziona la scheda **Proprietà personalizzate** e si fa clic su **Aggiungi**, è possibile aggiungere proprietà personalizzate individuali al componente contenitore.

Tabella 3-42. Impostazioni della scheda **Proprietà** per Proprietà personalizzate

Impostazione	Descrizione
Nome	Consente di specificare il nome di una proprietà personalizzata o di selezionare una proprietà personalizzata disponibile dal menu a discesa.
Valore	Consente di specificare o di modificare un valore da associare al nome della proprietà personalizzata.
Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.
Sovrascrivibile	È possibile specificare che il valore di una proprietà può essere sovrascritto dalla persona successiva che utilizza tale proprietà. Si tratta in genere di un altro architetto, ma se si seleziona Mostra nella richiesta , gli utenti business saranno in grado di visualizzare e modificare i valori della proprietà al momento di richiedere gli elementi del catalogo.
Mostra nella richiesta	Se si desidera consentire agli utenti finali di visualizzare il nome e il valore della proprietà, si può scegliere di visualizzare la proprietà nel modulo della richiesta di provisioning di una macchina. Per consentire agli utenti di fornire un valore, è inoltre necessario selezionare Sovrascrivibile .

- 8** Per salvare il blueprint come bozza o continuare la configurazione del blueprint, fare clic su **Salva** o su **Fine**.

Operazioni successive

È possibile aggiungere impostazioni di rete contenitore nella scheda **Rete** di un componente contenitore.

Applicazione di modelli di contenitori per l'utilizzo nei blueprint

È possibile creare un modello di contenitori disponibile per l'utilizzo in un blueprint di vRealize Automation.

Un modello di contenitori può includere più contenitori. Quando si applica un modello composto da più contenitori a vRealize Automation, il modello viene creato come blueprint con più componenti in vRealize Automation.

Le proprietà specifiche del contenitore aggiunte al modello di contenitori vengono riconosciute nel blueprint di vRealize Automation. Vedere [Utilizzo di proprietà di contenitori e gruppi di proprietà in un blueprint](#).

Quando si richiede il provisioning di un blueprint pubblicato nel catalogo di vRealize Automation, si esegue il provisioning dell'applicazione del contenitore di origine per tale blueprint.

È possibile aggiungere altri componenti al blueprint di vRealize Automation, inclusi i seguenti tipi di componenti:

- Tipi di macchine
- Componenti software
- Altri blueprint
- Componenti di rete e sicurezza di NSX
- Componenti di XaaS
- Componenti personalizzati

È possibile applicare un modello da Contenitori a vRealize Automation. Le modifiche apportate al blueprint di vRealize Automation non hanno effetto sul modello di Contenitori.

È possibile apportare modifiche successive nel modello di Contenitori e applicare di nuovo per sovrascrivere il blueprint in vRealize Automation. L'applicazione del modello a vRealize Automation comporta la sovrascrittura del blueprint, e le eventuali modifiche apportate al blueprint in vRealize Automation tra le applicazioni andranno perse. Per evitare di perdere le modifiche al blueprint, utilizzare vRealize CloudClient per clonare un nuovo blueprint o per esportare il blueprint.

Provisioning di un host o Docker Container da un blueprint

È possibile creare e utilizzare i blueprint di vRealize Automation per eseguire il provisioning di macchine come host Docker Container registrati.

Per registrare una macchina sottoposta a provisioning come host di contenitori, è necessario che soddisfi i seguenti requisiti:

- La macchina viene sottoposta a provisioning da un blueprint che contiene proprietà personalizzate specifiche di Contenitori.

Le proprietà personalizzate specifiche del contenitore sono fornite in due gruppi di proprietà. Vedere [Utilizzo di proprietà di contenitori e gruppi di proprietà in un blueprint](#).

Per informazioni sull'utilizzo di proprietà personalizzate e gruppi di proprietà in vRealize Automation, vedere *Guida di riferimento alle proprietà personalizzate*.

- La macchina è accessibile sulla rete.

Ad esempio, la macchina deve avere un indirizzo IP valido ed essere accesa.

È possibile definire un blueprint di vRealize Automation in modo che contenga proprietà personalizzate specifiche che designano un macchina come contenitore quando sottoposta a provisioning utilizzando il blueprint.

Quando una macchina con le proprietà del blueprint necessarie viene sottoposta correttamente e provisioning, viene registrata in Contenitori e riceve eventi e azioni da vRealize Automation.

Creazione di blueprint di Microsoft Azure e incorporazione di azioni risorse

Gli amministratori del cloud o dell'infrastruttura possono creare blueprint di macchine virtuali di Microsoft Azure che gli amministratori dei gruppi di business possono a loro volta utilizzare come base per la creazione di macchine di cui eseguire il provisioning per i clienti. Anche gli amministratori di DevOps possono creare blueprint di macchine di Azure o possono utilizzare blueprint di macchine Azure esistenti durante la creazione di blueprint compositi.

■ [Creazione di un blueprint per Microsoft Azure](#)

È possibile creare blueprint di macchine virtuali Microsoft Azure che forniscano accesso alle risorse delle macchine virtuali Azure.

■ [Creazione di azioni di risorse personalizzate Azure](#)

È possibile creare e utilizzare le azioni di risorse personalizzate per controllare le macchine virtuali Azure.

Creazione di un blueprint per Microsoft Azure

È possibile creare blueprint di macchine virtuali Microsoft Azure che forniscano accesso alle risorse delle macchine virtuali Azure.

Un modello di macchina Azure viene visualizzato nella categoria **Tipi di macchine** nella pagina Modifica blueprint di vRealize Automation. È possibile utilizzare questo modello di macchina virtuale come base di un blueprint Azure come descritto nella seguente procedura. Dopo aver creato un blueprint Azure, è possibile pubblicarlo e distribuirlo come progettato oppure è possibile utilizzarlo congiuntamente alle risorse Azure personalizzate o con altri blueprint per creare un blueprint composito.

Dopo aver creato e pubblicato il blueprint, gli utenti con i privilegi appropriati possono richiedere ed effettuare il provisioning di un'istanza di Azure tramite il Catalogo dei servizi di vRealize Automation.

Si tenga presente che i blueprint Azure definiscono i requisiti della macchina virtuale. vRealize Automation utilizza tali requisiti per selezionare la prenotazione più appropriata per la distribuzione.

Per informazioni sulle schede Impostazioni NSX e Proprietà della finestra di dialogo Nuovo blueprint, vedere *Configurazione di vRealize Automation*.

Per creare contemporaneamente due macchine virtuali da una sola distribuzione, è necessario creare due nomi di interfaccia di rete e due nomi di macchina virtuale.

Nota Evitare di effettuare il provisioning di una distribuzione sia su Azure che su vSphere utilizzando lo stesso prefisso di denominazione, poiché questo può causare la duplicazione di nomi in Azure e vSphere e questo potrebbe causare problemi ad alcuni utenti.

Prerequisiti

- Ottenere un ID di sottoscrizione Azure valido e le informazioni correlate, incluso il gruppo di risorse, l'account di storage e le informazioni della rete virtuale che potrebbero essere necessarie per la creazione di un blueprint.
- Configurare un endpoint Azure per creare una connessione ad Azure da utilizzare con la distribuzione di vRealize Automation.
- Configurare le prenotazioni Azure come opportuno per i gruppi di business.

Procedura

1 Scegliere **Progettazione > Blueprint**.

2 Fare clic sull'icona **Nuovo** (+).

3 Specificare il nome del blueprint nella casella di testo **Nome**.

Il nome immesso compila anche la casella di testo **ID**. Nella maggior parte dei casi è possibile ignorare le schede **Impostazioni NSX** e **Proprietà**.

4 Fare clic su **OK**.

5 Fare clic su **Tipi di macchine** nel menu Categorie.

6 Trascinare il modello della macchina virtuale **Azure Machine** nella Tela di progettazione.

Se è stata creata una risorsa Azure personalizzata da utilizzare come base di un blueprint, è possibile selezionare tale risorsa dalla categoria assegnata nell'elenco Categorie.

- 7 Immettere le informazioni necessarie per la macchina virtuale Azure nelle caselle di testo nelle pagine con schede situate nella parte centrale in basso nella tela di progettazione visualizzata quando si trascina il modello della macchina Azure nella tela di progettazione.

Le selezioni disponibili per le caselle di testo e gli altri parametri di tutte queste schede sono determinate principalmente dall'endpoint di Azure configurato come base per i blueprint.

Per la maggior parte dei parametri, quando si fa clic sulla casella di testo accanto al nome del parametro, si apre un nuovo riquadro nella parte destra della pagina. In questo riquadro, è possibile immettere valori di parametri nella casella di testo **Valore** e indicare se è **Obbligatorio**. Nota: in alcuni casi è inoltre possibile immettere un **Valore minimo** e un **Valore massimo**. Fare clic su **Applica** nel riquadro destro per compilare la casella di testo iniziale.

Figura 3-1. Menu destro del blueprint Azure

The screenshot shows the 'Azure_Machine_1' configuration window with the 'Machine Resources' tab active. Under 'Resource Group', the 'Use Existing' radio button is selected, and the 'Resource Group Name' is 'RG1-vAficionado'. Under 'Availability Set', the 'None' radio button is selected. On the right side, the 'Required' dropdown is set to 'No', and the 'Value' field contains 'RG1-vAficionado'. Orange boxes highlight the 'Use Existing' button, the 'Resource Group Name' field, the 'None' button, and the 'Value' field.

Per la maggior parte dei parametri è inoltre disponibile un pulsante **Opzioni avanzate**. Queste opzioni consentono di specificare la lunghezza dei parametri nonché di nascondere i parametri agli utenti finali.

Nota È necessario popolare i parametri richiesti su ogni scheda per poter procedere con la configurazione del blueprint. Se si desidera lasciare un campo vuoto, è possibile tornare indietro ed eliminare la voce prima di salvare.

Scheda	Descrizione	Parametri importanti
Generale	Selezionare le informazioni di connessione di base per la macchina virtuale Azure, ad esempio l'endpoint da utilizzare.	<p>ID - Identifica la macchina virtuale Azure in corso di creazione. Se il nome viene modificato, viene aggiornata automaticamente anche l'immagine della macchina virtuale Azure nella tela di progettazione.</p> <p>Descrizione - Identifica la macchina virtuale in corso di creazione e se è richiesta o meno.</p> <p>Istanze - Questa selezione consente di creare una macchina virtuale scalabile. Utilizzare i campi Minimo e Massimo per identificare il numero di istanze Azure che è possibile generare da questa macchina.</p> <p>Usa password di autenticazione - Selezionare Sì per utilizzare l'autenticazione tramite password oppure No per utilizzare SSH.</p> <p>Nome utente amministratore - Lasciare vuoto questo campo, potrà essere assegnato dall'utente che esegue il provisioning della macchina.</p> <p>Password amministratore - Lasciare vuoto questo campo, la password potrà essere inserita dall'utente che esegue il provisioning della macchina.</p>
Informazioni build	Consente di configurare le informazioni sulla macchina virtuale in corso di creazione.	<p>Posizione - Selezionare la località geografica in cui verrà distribuita tale macchina virtuale.</p> <p>Prefisso macchina - Selezionare il pulsante di opzione per indicare se si desidera utilizzare il prefisso della macchina dal gruppo di business associato o creare un prefisso personalizzato. Se si desidera utilizzare un prefisso personalizzato, immetterlo nella casella di testo Prefisso macchina personalizzato.</p> <p>Tipo di immagine della macchina virtuale - Scegliere il pulsante di opzione appropriato per l'immagine di una macchina virtuale di tipo Personalizzato o Stock. Viene creata una macchina virtuale personalizzata dalla distribuzione classica di Azure, offrendo un numero maggiore di opzioni di configurazione correlate a servizi cloud, account di storage e set di disponibilità.</p> <p>Immagine della macchina virtuale - Identificare l'immagine della macchina virtuale Azure su cui è basato il blueprint.</p> <ul style="list-style-type: none"> ■ Per un'immagine di macchina virtuale di tipo stock, l'URN dell'immagine della macchina deve corrispondere al seguente formato: (autore):(offerta):(sku): (versione). ■ Per un disco gestito, l'immagine della macchina URN deve corrispondere al seguente formato: (ResourceGroupName):(CustomImageName) ■ Per un'immagine di macchina virtuale personalizzata, l'URN dell'immagine della macchina deve corrispondere al seguente formato: <code>https://storageaccount.blob.core.windows.net/container/image.vhd</code> <p>È inoltre necessario compilare la casella di testo Tipo d'immagine sistema operativo (Windows o Linux) per le immagini personalizzate</p>

Scheda	Descrizione	Parametri importanti
		<p>Utente amministratore - Digitare il nome dell'amministratore designato configurato per le macchine virtuali basate su questo blueprint. In alternativa, può essere lasciato vuoto e immesso nel modulo di richiesta.</p> <p>Autenticazione - Selezionare il pulsante di opzione appropriato per indicare se le macchine virtuali basate su questo blueprint richiedono una password o l'autenticazione SSH.</p> <p>Password amministratore - La password dell'amministratore dell'istanza della macchina virtuale.</p> <p>Serie - Definisce la dimensione generale di un'istanza di macchina virtuale. Per ulteriori informazioni sulle serie, consultare la documentazione di Azure in https://azure.microsoft.com/it-it/documentation/articles/virtual-machines-windows-sizes/.</p> <p>Dimensione - Definisce la dimensione dell'istanza di macchina virtuale specifica in una serie. La dimensione è correlata alla Serie selezionata. Se è presente una connessione valida a un'istanza di Azure, le dimensioni disponibili vengono popolate dinamicamente in base alla sottoscrizione, nonché alla posizione e alle serie selezionate. Per ulteriori informazioni sulle dimensioni, consultare la documentazione di Azure.</p> <p>Dettagli dimensione istanza - Informazioni opzionali sulla serie e sulla dimensione dell'istanza di macchina virtuale.</p>

Scheda	Descrizione	Parametri importanti
Risorse macchina	<p>Organizzare le risorse della macchina virtuale in bucket. Un gruppo di risorse è un costrutto organizzativo che raggruppa le risorse della macchina virtuale, quali siti web, account, database e reti.</p> <p>Un Set di disponibilità è un meccanismo che consente di gestire due o più macchine virtuali per supportare la ridondanza. Vedere https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/ per ulteriori informazioni sui Set di disponibilità di Azure.</p> <hr/> <p>Nota Se si configura un blueprint con il numero massimo di istanze Azure impostato su un valore maggiore di 1, si consiglia di utilizzare il gruppo di risorse e il set di disponibilità esistenti anziché crearne di nuovi. L'utilizzo di nuovi gruppi di risorse o di nuovi set di disponibilità in più istanze nella stessa distribuzione causerà errori e altri problemi se associati con bilanciamenti del carico.</p>	<p>Creare o riutilizzare il gruppo di risorse - Selezionare il pulsante di opzione appropriato per indicare se si desidera utilizzare il gruppo di risorse Azure esistente o crearne uno nuovo. È possibile trovare il nome del gruppo di risorse esistente nella pagina Gruppi di risorse del portale di Azure. Se si sceglie di creare un nuovo gruppo di risorse, nella casella di testo Gruppo di risorse viene visualizzato automaticamente un nome appropriato per il nuovo gruppo.</p> <p>Creare o riutilizzare il set di disponibilità - Selezionare il pulsante di opzione appropriato in base alle operazioni che si desidera eseguire. Se si seleziona Crea nuovo, nella casella di testo vengono visualizzate le informazioni sul nuovo set di disponibilità.</p>

Scheda	Descrizione	Parametri importanti
Storage	Consente di scegliere un disco gestito Azure o un account di storage per questo blueprint. Con il disco gestito, Azure gestisce la maggior parte della configurazione e della manutenzione correlata allo storage. Un account di archiviazione fornisce l'accesso ai diversi tipi di storage di Azure, come Archivio BLOB di Azure, Tabella coda e Archiviazione file. Per la maggior parte dei blueprint, è possibile accettare i valori predefiniti.	<p>Tipo di storage: selezionare se si desidera fornire un disco gestito o un account di storage gestito manualmente.</p> <ul style="list-style-type: none"> ■ Se è stato selezionato Disco gestito, selezionare se si desidera utilizzare un disco premium o standard nella casella di testo Tipo di disco della macchina virtuale. È possibile ignorare le caselle di selezione rimanenti. ■ Se si seleziona Account di storage, immettere il nome dell'account di storage per la macchina virtuale nella casella Account di storage sul disco del sistema operativo. Il disco del sistema operativo della macchina virtuale Azure viene distribuito in questo account di storage. È possibile trovare le informazioni sul gruppo di archiviazione nel portale di Azure. È possibile disporre di uno o più account di storage. <hr/> <p>Nota I nomi di account di archiviazione che contengono trattini bassi o altri caratteri speciali possono causare errori.</p> <hr/> <p>Abilita diagnostica all'avvio: selezionare questa casella di controllo se si utilizzano dati di diagnostica con l'istanza Azure.</p> <p>Numero di dischi dati: selezionare il numero appropriato di dischi di storage di dati utilizzati nella macchina virtuale. È possibile specificare fino a quattro dischi. Tali dischi vengono aggiunti al disco del sistema operativo come specificato nella casella di testo Account di storage.</p> <p>N. disco di storage</p> <ul style="list-style-type: none"> ■ Nome disco - Identifica il nome assegnato al disco. ■ Tipo di disco - Tipo di dispositivo di storage. ■ Dimensione del disco - Dimensione del disco. ■ Replica - Metodo di ridondanza utilizzato per il backup del disco. ■ Cache host - Indica se le letture/scritture vengono memorizzate in cache per aumentare le prestazioni.

Scheda	Descrizione	Parametri importanti
Rete	<p>Consente di selezionare il servizio di rete per il blueprint della macchina virtuale. Per la maggior parte dei blueprint, è possibile accettare i valori predefiniti e l'utente immetterà le informazioni di rete appropriate durante la distribuzione.</p> <hr/> <p>Nota È possibile creare una sola macchina virtuale per interfaccia, tuttavia ciascuna macchina virtuale può disporre di un massimo di quattro interfacce.</p> <hr/>	<p>Fare clic sulla tabella per aprire una finestra di dialogo a destra, che contiene a sua volta un'altra tabella modificabile con i seguenti campi.</p> <ul style="list-style-type: none"> ■ Nome bilanciamento del carico - Il bilanciamento del carico utilizzato con l'istanza Azure. ■ Numero di interfacce di rete - Selezionare il numero di interfacce di rete utilizzate con l'istanza Azure. Il numero di interfacce di rete deve essere supportato dalla dimensione della macchina virtuale come selezionato nella scheda Storage. ■ Interfaccia di rete - Selezionare l'interfaccia di rete appropriata per il blueprint della macchina virtuale. Se si immette una rete esistente, è possibile ignorare tutte le altre schede relative alla rete. Se si immette un nome di interfaccia di rete inesistente, viene creata una nuova interfaccia con il nome specificato ed è possibile utilizzare tutte le altre schede relative all'interfaccia per configurarla. ■ Prefisso nome NIC - Il prefisso della scheda dell'interfaccia di rete. ■ Tipo di indirizzo IP - Indicare se la macchina virtuale utilizza un indirizzo IP statico o dinamico. ■ Configurazione di rete - Immettere la configurazione di rete appropriata. I profili di rete sono supportati. Sono disponibili due opzioni: Specifica reti Azure e Usa profilo di rete, e i campi successivi cambiano in base all'opzione selezionata. <ul style="list-style-type: none"> ■ Le seguenti opzioni sono disponibili se si seleziona Specifica reti Azure. Se tali caselle di testo sono lasciate vuote, i costrutti di rete predefiniti vengono utilizzati in base alle informazioni specificate nella prenotazione pertinente. <ul style="list-style-type: none"> ■ Nome vNet - Nome della rete virtuale ■ Nome subnet - Il nome di dominio della subnet di Azure. <hr/> <p>Nota È possibile impostare l'indirizzo IP pubblico per Azure durante le operazioni Gruppo 2.</p> <ul style="list-style-type: none"> ■ Se si seleziona Usa profilo di rete, la configurazione di rete viene scollegata dai costrutti Azure sottostanti e viene associata al profilo di rete di vRealize Automation. <ul style="list-style-type: none"> ■ Se la casella di testo Profilo di rete viene lasciata vuota, la coppia di vNet e subnet Azure predefinita viene risolta in base alle prenotazioni pertinenti in cui è specificato un profilo di rete. ■ Se si immette un profilo di rete, la vNet e la subnet Azure vengono risolte in base alla prenotazione corrispondente. <hr/>
Proprietà	<p>Consente di aggiungere proprietà personalizzate al blueprint. Le proprietà personalizzate aggiunte in</p>	<p>Per aggiungere proprietà personalizzate esistono due opzioni rappresentate da due schede nella finestra di dialogo Proprietà.</p>

Scheda	Descrizione	Parametri importanti
	questa scheda possono essere sovrascritte da proprietà assegnate in un momento successivo nella catena delle precedenze. Per ulteriori informazioni sull'ordine di precedenza delle proprietà personalizzate, vedere <i>Guida di riferimento alle proprietà personalizzate</i> .	<ul style="list-style-type: none"> ■ Gruppi di proprietà: si tratta di gruppi riutilizzabili che semplificano il processo di aggiunta di proprietà personalizzate. Per la selezione di gruppi di proprietà sono disponibili quattro opzioni: <ul style="list-style-type: none"> ■ Aggiungi: consente di aggiungere al blueprint un gruppo di proprietà disponibile. ■ Sposta su/Sposta giù: consente di controllare la precedenza dei gruppi di proprietà. Il primo gruppo ha la priorità più elevata e le sue proprietà personalizzate hanno la precedenza rispetto a tutte le altre. ■ Visualizza proprietà: consente di visualizzare le proprietà personalizzate all'interno del gruppo selezionato. ■ Visualizza proprietà unite: se una proprietà personalizzata è inclusa in più gruppi di proprietà, il valore nel gruppo di proprietà con la priorità più elevata ha la precedenza. La visualizzazione delle proprietà unite semplifica l'assegnazione della priorità ai gruppi di proprietà. ■ Proprietà personalizzate: utilizzare questa scheda per aggiungere singole proprietà personalizzate. <ul style="list-style-type: none"> ■ Nuovo: consente di aggiungere al blueprint una singola proprietà personalizzata. ■ Nome: immettere un nome per la proprietà. Per un elenco delle proprietà personalizzate e delle relative definizioni, vedere <i>Guida di riferimento alle proprietà personalizzate</i>. ■ Valore: immettere un valore per la proprietà personalizzata. ■ Codificato: consente di codificare la proprietà. ■ Sovrascrivibile: consente di specificare che il valore della proprietà può essere sovrascritto dall'utente successivo. Si tratta in genere di un altro architetto, ma se si seleziona Mostra nella richiesta, gli utenti business possono visualizzare e modificare i valori delle proprietà quando richiedono elementi del catalogo. ■ Mostra nella richiesta: se si desidera che gli utenti finali visualizzino il nome e il valore della proprietà, è possibile scegliere di visualizzare la proprietà nel modulo di richiesta del provisioning della macchina. Per consentire agli utenti di fornire un valore, è inoltre necessario selezionare Sovrascrivibile.

- 8 Fare clic su **Fine** per salvare la configurazione del blueprint e tornare alla pagina Blueprint principale.

Operazioni successive

Se sono state configurate proprietà personalizzate nella prenotazione di Azure per supportare un tunnel VPN, è possibile aggiungere componenti software ai blueprint Azure.

- 1 Selezionare **Componenti software** nel menu Categorie. I componenti software configurati nei blueprint Azure compaiono nel riquadro sottostante.
- 2 Selezionare Macchina virtuale Azure nei valori a discesa del contenitore.
- 3 Selezionare il componente software desiderato e trascinarlo nella macchina virtuale Azure nella tela di progettazione.
- 4 In caso di proprietà richieste per il componente software, inserirle nelle caselle di testo dei parametri corrispondenti sotto alla tela di progettazione.
- 5 Fare clic su **Salva**.

Se si desidera pubblicare il blueprint, selezionarlo nella pagina Blueprint principale e fare clic su **Pubblica**. Un blueprint pubblicato è disponibile nella pagina Elemento del catalogo. Inoltre, un manager di gruppi di business (o una figura equivalente) può utilizzare questo blueprint pubblicato come base di un blueprint composito.

Creazione di azioni di risorse personalizzate Azure

È possibile creare e utilizzare le azioni di risorse personalizzate per controllare le macchine virtuali Azure.

L'implementazione Azure vRealize Automation viene fornita con due azioni di risorsa personalizzata appena installata:

- Avvio di una macchina virtuale
- Arresto di una macchina virtuale

Inoltre è possibile creare le azioni di risorse personalizzate utilizzando i workflow che sono accessibili attraverso la libreria vRealize Orchestrator, disponibile nell'interfaccia vRealize Automation.

È possibile interoperare con le azioni risorsa Azure come con qualsiasi altra azione risorsa XaaS in vRealize Automation. Per ulteriori informazioni sulle azioni risorsa di XaaS, vedere *Creazione di blueprint e azioni risorsa di XaaS* e *Integrazione di vRealize Orchestrator in vRealize Automation* in *Configurazione di vRealize Automation*.

Prerequisiti

Configurare un endpoint Azure valido per la propria distribuzione di vRealize Automation.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic su **Nuovo**.
- 3 Passare a **Orchestrator > Libreria > Azure** nella libreria dei workflow di vRealize Orchestrator.

- 4 Selezionare la cartella e il workflow desiderati.
- 5 Configurare l'azione per le proprie esigenze come si farebbe con qualsiasi altra azione risorsa di XaaS.

Aggiunta di funzionalità di gestione della configurazione ai blueprint vSphere

È possibile aggiungere componenti di gestione della configurazione ai blueprint vSphere per supportare la gestione della configurazione delle macchine virtuali vSphere.

vRealize Automation supporta l'aggiunta di funzionalità di gestione della configurazione di Puppet e Ansible nei blueprint vSphere.

La gestione della configurazione basata su Puppet in genere utilizza regole e ambienti per definire e gestire la configurazione del software in base all'applicazione Puppet Enterprise. Tenere presente che il significato di ruolo e ambiente in Puppet è diverso dal significato IT più generico.

La gestione della configurazione basata su Ansible si basa su modelli di lavoro definiti in un'implementazione Ansible Tower. È possibile scegliere e riordinare più modelli. È possibile eseguire questi modelli dopo la distribuzione di una macchina e prima che venga eliminata da vRealize Automation.

Un endpoint stabilisce una connessione con una distribuzione enterprise Puppet o Ansible esistente. Quando viene creato l'endpoint, vRealize Automation recupera le informazioni appropriate dalle distribuzioni specificate. È possibile specificare scenari di binding precoce o tardivo quando si configura un blueprint di una macchina virtuale abilitata a Puppet o Ansible.

Nota Attualmente, i componenti Ansible e Puppet sono supportati solo su blueprint e macchine virtuali vSphere.

Aggiunta di un componente Puppet a un Blueprint vSphere

È possibile aggiungere un componente di gestione della configurazione Puppet a un Blueprint vSphere per facilitare la gestione applicata di macchine virtuali vSphere utilizzando un Master Puppet.

L'aggiunta di un componente Puppet a un Blueprint vSphere aggiunge un agente Puppet a macchine virtuali create da quel Blueprint.

Quando vengono creati Blueprint vSphere abilitati al Puppet, è necessario scegliere se creare una configurazione di binding precedente o successiva.

Con il binding precedente, gli utenti definiscono le impostazioni dell'ambiente e del ruolo del Puppet per tutte le macchine virtuali basate su un Blueprint particolare quando il componente Puppet viene aggiunto al Blueprint. Queste impostazioni rimangono statiche durante la vita del blueprint. Per il binding successivo sono disponibili varie opzioni.

- Lasciare vuote le caselle di testo **Ambiente Puppet** e **Ruolo Puppet** nel blueprint: gli utenti forniranno queste impostazioni al momento della richiesta.

- Specificare un **Ambiente Puppet** e lasciare vuota la casella **Ruolo puppet**. Gli utenti devono specificare il ruolo al momento della richiesta.

Prerequisiti

Creare un Blueprint vSphere appropriato. Vedere [vSphereImpostazioni dei componenti macchina in vRealize Automation](#) per ulteriori informazioni.

Procedura

- 1 Scegliere **Progettazione > Blueprint**.
- 2 Selezionare **Gestione configurazione** dal menu Categorie nella pagina Progettazione per Blueprint.
- 3 Selezionare il componente Puppet e trascinarlo nel componente vSphere nella Tela di progettazione.
- 4 Immettere un **ID** e una **Descrizione** per il componente Puppet nella scheda Generale nella parte inferiore della pagina.
L'ID e la descrizione sono arbitrari.
- 5 Fare clic sulla scheda Server.
- 6 Fare clic sull'elenco a discesa e selezionare il Master Puppet appropriato per il Blueprint.
- 7 Selezionare l'**Ambiente Puppet** e il **Ruolo Puppet** se si desidera utilizzare il binding precedente per questo componente.

Per configurare il binding precedente, selezionare un ambiente e un ruolo Puppet. Se si desidera creare un componente con binding successivo, selezionare un **Ambiente Puppet** o lasciare vuote le caselle di testo **Ambiente Puppet** e **Ruolo Puppet** e selezionare le caselle di testo denominate **Impostato in modulo di richiesta**.

Nota Le caselle di testo denominate **Impostato in modulo di richiesta** sono collegate. Ovvero, se ne viene selezionata una, l'altra viene selezionata automaticamente.

- 8 Fare clic su **Fine** per salvare la configurazione del componente Puppet e tornare alla pagina di progettazione Blueprint principale.

Aggiunta di un componente Ansible a un blueprint di vSphere

È possibile aggiungere un componente di gestione della configurazione Ansible a un blueprint di vSphere per facilitare la gestione applicata di macchine virtuali di vSphere utilizzando Ansible Tower.

L'aggiunta di un componente Ansible a un blueprint di vSphere consente ad Ansible Tower di comunicare con le risorse distribuite per eseguire i comandi.

Prerequisiti

Creare un Blueprint vSphere appropriato. Vedere [vSphereImpostazioni dei componenti macchina in vRealize Automation](#) per ulteriori informazioni.

Procedura

- 1 Scegliere **Progettazione > Blueprint**.
 - 2 Selezionare **Gestione configurazione** dal menu Categorie nella pagina Progettazione per Blueprint.
 - 3 Selezionare il componente Ansible e trascinarlo nel componente vSphere nella tela di progettazione.
 - 4 Immettere un **ID** e una **Descrizione** per il componente Ansible nella scheda Generale nella parte inferiore della pagina.
L'ID e la descrizione sono arbitrari.
 - 5 Fare clic sulla scheda Dettagli e immettere le informazioni appropriate su progetto, modello e Ansible Tower.
 - a Selezionare un'istanza di **Ansible Tower** e un'**Organizzazione** appropriate che utilizzeranno questo componente.
 - b Configurare il binding anticipato o tardivo per il componente Ansible.
 - Se si desidera utilizzare il binding anticipato per questo componente, selezionare **Progetto** e **Modello di processo** appropriati. Selezionare un modello appropriato da eseguire quando la macchina viene eliminata nella casella di testo **Annulla provisioning modello di processo**. Lasciare vuote le caselle di controllo **Impostato in modulo di richiesta**. Selezionare anche un ruolo e un ambiente Ansible appropriati.
 - Se si desidera creare un componente con binding tardivo, è possibile scegliere le caselle di controllo **Impostato in modulo di richiesta**, anziché impostare i valori per le caselle **Progetto**, **Modello di processo** e **Annulla provisioning modello di processo**.
-
- Nota** Le caselle di testo denominate **Impostato in modulo di richiesta** sono collegate. Quando se ne seleziona una, vengono selezionate automaticamente anche quelle sotto. Ciò accade perché il campo **Progetto** agisce come filtro per i modelli di processo. Se si specifica un progetto, l'elenco di modelli di processo viene filtrato automaticamente in base al progetto. Di conseguenza, se si sceglie **Impostato in modulo di richiesta** per un progetto, vengono selezionati automaticamente i due campi seguenti.
-
- 6 Fare clic su **Fine** per salvare la configurazione del componente Ansible e tornare alla pagina di progettazione del blueprint principale.

Aggiunta del supporto delle connessioni RDP ai blueprint di macchine Windows

Per consentire agli amministratori del catalogo di autorizzare gli utenti all'azione Connessione con RDP per i Blueprint Windows, aggiungere proprietà personalizzate RDP al Blueprint e fare riferimento al file RDP preparato dall'amministratore del sistema.

Nota se l'amministratore di struttura crea un gruppo di proprietà che contiene le proprietà personalizzate richieste e lo include nel blueprint, non è necessario aggiungere singolarmente le proprietà personalizzate al blueprint.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **manager del gruppo di business**.
- Ottenere il nome del file RDP personalizzato creato allo scopo dall'amministratore di sistema. Vedere [Creazione di un file RDP personalizzato per il supporto di connessioni RDP per le macchine di cui è stato eseguito il provisioning](#).
- Creare almeno un blueprint di macchina Windows.

Procedura

- 1 Scegliere **Progettazione > Blueprint**.
- 2 Selezionare il blueprint da aggiornare e fare clic su **Modifica**.
- 3 Selezionare il componente macchina sulla tela per modificarne i dettagli.
- 4 Fare clic sulla scheda **Proprietà**.
- 5 Fare clic sulla scheda **Proprietà personalizzate**.

6 Configurare le impostazioni RDP.

- a Fare clic su **Nuova proprietà**.
- b Specificare i nomi delle proprietà personalizzate RDP nella casella di testo **Nome** e i valori corrispondenti nella casella di testo **Valore**.

Opzione	Descrizione e valore
VirtualMachine.Rdp.File	Specifica un file RDP da cui ottenere le impostazioni, ad esempio <code>My_RDP_Settings.rdp</code> . Il file deve risiedere nella sottodirectory <code>Website\Rdp</code> della directory d'installazione di vRealize Automation.
VirtualMachine.Rdp.SettingN	Specifica le impostazioni di RDP da utilizzare all'apertura di un collegamento RDP alla macchina. <i>N</i> è un numero unico utilizzato per distinguere un'impostazione RDP da un'altra. Ad esempio, per specificare il livello di autenticazione RDP in modo che non siano impostati requisiti di autenticazione, definire la proprietà personalizzata <code>VirtualMachine.Rdp.Setting1</code> e impostare il valore al livello di autenticazione <code>level:3</code> . Per informazioni sulle impostazioni di RDP disponibili e sulla loro sintassi corretta, consultare la documentazione di RDP di Microsoft Windows, ad esempio la sezione relativa alle impostazioni di RDP per i servizi Desktop remoto di Windows Server .
VirtualMachine.Admin.NameCompletion	Specifica il nome di dominio da includere nel nome di dominio completo della macchina che i file RDP o SSH generano per le opzioni dell'interfaccia utente Connessione con RDP o Connessione con SSH . Ad esempio, impostare il valore su <code>myCompany.com</code> per generare il nome di dominio completo <code>my-machine-name.myCompany.com</code> nel file RDP o SSH.

- c Fare clic su **Salva**.

7 Selezionare la riga Blueprint e fare clic su **Pubblica**.

Risultati

Gli amministratori di catalogo possono autorizzare gli utenti all'azione **Connessione con RDP** per le macchine con provisioning eseguito dal Blueprint. Se gli utenti non sono autorizzati all'azione, non potranno connettersi utilizzando RDP.

Aggiunta della pulizia di Active Directory per il blueprint CentOS

Gli architetti di IaaS possono configurare vRealize Automation per eseguire una pulizia dell'ambiente Active Directory ogni volta che dagli hypervisor vengono rimosse macchine con provisioning eseguito. Modificare il blueprint per configurare il plug-in di pulizia di Active Directory.

Utilizzando il plug-in di pulizia di Active Directory è possibile impostare l'esecuzione delle seguenti azioni sugli account di Active Directory quando una macchina viene eliminata da un hypervisor:

- Eliminare l'account di AD
- Disattivare l'account di AD
- Rinominare l'account di AD

- Spostare l'account di AD in un'altra unità organizzativa (OU) di AD

Prerequisiti

Nota queste informazioni non riguardano i Amazon Web Services.

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Raccogliere le seguenti informazioni sull'ambiente di Active Directory:
 - Nome utente e password di un account di Active Directory dotato di diritti sufficienti a eliminare, disattivare, rinominare o spostare account di Active Directory. Il nome utente deve essere nel formato dominio\nomeutente.
 - (Facoltativo) Il nome dell'unità organizzativa in cui spostare le macchine eliminate.
 - (Facoltativo) Il prefisso da allegare alle macchine eliminate.
- Creare un blueprint macchina. Vedere [Configurazione del blueprint di una macchina](#).

Procedura

- 1 Scegliere **Progettazione > Blueprint**.
- 2 Selezionare il blueprint e fare clic su **Modifica**.
- 3 Selezionare il componente macchina nella tela per mostrare la scheda Dettagli.
- 4 Fare clic sulla scheda **Proprietà**.
- 5 Selezionare la scheda **Proprietà personalizzate** per configurare il plug-in Cleanup di Active Directory.
 - a Fare clic su **Nuova proprietà**.
 - b Immettere `Plugin.AdMachineCleanup.Execute` nella casella di testo **Nome**.
 - c Immettere **true** nella casella di testo **Valore**.
 - d Fare clic sull'icona **Salva** (✓).
- 6 Configurare il plug-in Cleanup di Active Directory aggiungendo proprietà personalizzate.

Opzione	Descrizione e valore
<code>Plugin.AdMachineCleanup.UserName</code>	Immettere il nome dell'utente dell'account di Active Directory nella casella di testo Valore . L'utente deve avere privilegi sufficienti a eliminare, disattivare, spostare e rinominare account di Active Directory. Il nome utente deve essere nel formato dominio\nomeutente.
<code>Plugin.AdMachineCleanup.Password</code>	Immettere la password dell'account di Active Directory nella casella di testo Valore .
<code>Plugin.AdMachineCleanup.Delete</code>	Impostare su True per eliminare gli account delle macchine eliminate invece di disabilitarli.

Opzione	Descrizione e valore
<code>Plugin.AdMachineCleanup.MoveToOu</code>	Sposta l'account delle macchine eliminate in una nuova unità organizzativa di Active Directory. Il valore è l'unità organizzativa in cui si sta spostando l'account. Questo valore deve avere il formato <code>ou=OU, dc=dc</code> , ad esempio <code>ou=trash,cn=computers,dc=lab,dc=local</code> .
<code>Plugin.AdMachineCleanup.RenamePrefix</code>	Rinomina gli account delle macchine eliminate aggiungendo un prefisso. Il valore è la stringa del prefisso da apporre, ad esempio <code>destroyed_</code> .

7 Fare clic su **OK**.

Risultati

L'ambiente Active Directory verrà aggiornato ogni volta che macchine con provisioning eseguito dal blueprint saranno eliminate dall'hypervisor.

Permettere ai richiedenti di specificare il nome host delle macchine

Gli architetti di blueprint possono consentire ai propri utenti di scegliere i nomi macchina che desiderano quando questi richiedono i loro blueprint. A tale scopo, l'architetto dovrà modificare il blueprint aggiungendo la proprietà personalizzata Hostname e configurandola per richiedere agli utenti l'immissione di un valore nelle loro richieste.

Nota se l'amministratore di struttura crea un gruppo di proprietà che contiene le proprietà personalizzate richieste e lo include nel blueprint, non è necessario aggiungere singolarmente le proprietà personalizzate al blueprint.

Prerequisiti

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Creare un blueprint macchina. Vedere [Configurazione del blueprint di una macchina](#).

Procedura

- 1 Scegliere **Progettazione > Blueprint**.
- 2 Selezionare il blueprint e fare clic su **Modifica**.
- 3 Selezionare il componente macchina nella tela per mostrare la scheda dei dettagli.
- 4 Fare clic sulla scheda **Proprietà**.
- 5 Fare clic su **Nuova proprietà**.
- 6 Immettere **Hostname** nella casella di testo **Nome**.
- 7 Lasciare vuota la casella di testo **Valore**.
- 8 Configurare vRealize Automation per mostrare agli utenti la richiesta di immettere il valore relativo al nome host durante la richiesta.
 - a Selezionare **Sovrascrivibile**.
 - b Selezionare **Mostra nella richiesta**.

Poiché i nomi host devono essere univoci, gli utenti potranno richiedere una sola macchina alla volta da questo blueprint.

9 Fare clic sull'icona **Salva** (👍).

10 Fare clic su **OK**.

Risultati

Agli utenti che richiedono una macchina dal blueprint verrà richiesto di specificare un nome host da assegnare alla macchina. vRealize Automation verificherà l'unicità del nome host specificato.

Abilitazione degli utenti a selezionare posizioni di datacenter per distribuzioni tra più regioni

Se un architetto di blueprint desidera consentire agli utenti di scegliere se eseguire il provisioning delle macchine nell'infrastruttura di Boston o di Londra, dovrà modificare il blueprint per abilitare la funzionalità delle posizioni.



Se si dispone di un data center a Londra e uno a Boston, è importante evitare che gli utenti di Boston eseguano il provisioning di macchine sull'infrastruttura di Londra e viceversa. Affinché gli utenti di Boston e Londra possano eseguire il provisioning solo nella propria infrastruttura, è necessario consentire loro di selezionare la posizione appropriata per il provisioning al momento della richiesta delle macchine.

Prerequisiti

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Un amministratore di sistema può definire le posizioni dei data center. Vedere [Scenario: aggiunta di posizioni di data center per distribuzioni tra più regioni](#).
- In qualità di amministratore della struttura, applicare le posizioni appropriate alle risorse di elaborazione. Vedere [Scenario: applicazione di una posizione a una risorsa di elaborazione per distribuzioni tra più regioni](#).
- Creare un blueprint macchina. Vedere [Configurazione del blueprint di una macchina](#).

Procedura

- 1** Scegliere **Progettazione > Blueprint**.
- 2** Selezionare il blueprint e fare clic su **Modifica**.

- 3 Selezionare il componente macchina sulla tela per richiamare la scheda di dettagli **Generale**.
- 4 Selezionare la casella di controllo **Visualizzare la posizione su richiesta?**.
- 5 Fare clic su **Fine**.
- 6 Selezionare il blueprint e fare clic su **Pubblica**.

Risultati

Agli utenti dei gruppi di business che richiedono il provisioning di una macchina dal blueprint in oggetto verrà ora chiesto di selezionare la posizione del data center.

Progettazioni di componenti Software

L'architetto del software può creare componenti software riutilizzabili, standardizzando le proprietà di configurazione e utilizzando script di azione per specificare esattamente le modalità di installazione, configurazione, disinstallazione o aggiornamento dei componenti durante le operazioni di scalabilità delle distribuzioni. È possibile riscrivere questi script di azione in qualsiasi momento ed effettuare la pubblicazione in tempo reale per applicare le modifiche ai componenti software sottoposti a provisioning.

È possibile progettare gli script di azione in modo da renderli generici e riutilizzabili definendo e utilizzando coppie di nomi e valori denominate proprietà software e convalidandole come parametri per gli script di azione. Se le proprietà software presentano valori sconosciuti o che devono essere definiti in futuro, è possibile richiedere o consentire ad altri architetti di blueprint o utenti finali di fornire i valori. Se è necessario un valore da un altro componente in un blueprint, ad esempio l'indirizzo IP di una macchina, è possibile associare la proprietà software alla proprietà dell'indirizzo IP della macchina specificata. L'utilizzo delle proprietà software per configurare gli script di azione li rende generici e riutilizzabili affinché sia possibile distribuire i componenti software in diversi ambienti senza modificare gli script.

Tabella 3-43. Azioni del ciclo di vita

Azioni del ciclo di vita	Descrizione
Installazione	Installare il software. Ad esempio, è possibile scaricare i bit di installazione del server Tomcat e installare un servizio Tomcat. Gli script compilati per l'azione del ciclo di vita di installazione vengono eseguiti quando il software viene sottoposto a provisioning per la prima volta, durante una richiesta di distribuzione iniziale o come parte di un'operazione di scalabilità orizzontale.
Configurazione	Configurare il software. Nel caso dell'esempio Tomcat, è possibile impostare i valori JAVA_OPTS e CATALINA_OPTS. Gli script di configurazione vengono eseguiti al termine dell'azione di installazione.
Avvio	Avviare il software. Ad esempio, è possibile avviare il servizio Tomcat utilizzando il comando di avvio nel server Tomcat. Gli script di avvio vengono eseguiti al termine dell'azione di configurazione.

Tabella 3-43. Azioni del ciclo di vita (continua)

Azioni del ciclo di vita	Descrizione
Aggiornamento	Se si sta progettando il componente software affinché supporti blueprint scalabili, gestire gli eventuali aggiornamenti richiesti dopo un'operazione di scalabilità verticale o scalabilità orizzontale. Ad esempio, è possibile modificare la dimensione del cluster per una distribuzione scalata e gestire i nodi in clustering utilizzando un bilanciamento del carico. Progettare gli script di aggiornamento affinché vengano eseguiti più volte (idempotent) e in modo da poter gestire sia le situazioni di scalabilità verticale che di scalabilità orizzontale. Quando si esegue un'operazione di scalabilità, gli script di aggiornamento vengono eseguiti in tutti i componenti software dipendenti.
Disinstallazione	Disinstallare il software. Ad esempio, è possibile eseguire azioni specifiche nell'applicazione prima della distruzione di una distribuzione. Gli script di disinstallazione vengono eseguiti ogni volta che si distruggono componenti software.

È possibile scaricare componenti di Software predefiniti per un'ampia gamma di servizi e applicazioni middleware da VMware Solution Exchange. Utilizzando vRealize CloudClient o l'API REST di vRealize Automation, è possibile importare in modo programmatico i componenti di Software predefiniti nell'istanza vRealize Automation.

- Per visitare VMware Solution Exchange, vedere https://solutionexchange.vmware.com/store/category_groups/cloud-management.
- Per informazioni sulla REST API di vRealize Automation, vedere *Guida alla programmazione e l'API dei servizi dei contenuti di vRealize Automation* all'indirizzo <https://code.vmware.com>.
- Per informazioni su vRealize CloudClient, vedere <https://developercenter.vmware.com/tool/cloudclient>.

Tipi di proprietà e opzioni di impostazione

È possibile progettare gli script di azione in modo da renderli generici e riutilizzabili definendo e utilizzando coppie di nomi e valori denominate proprietà software e convalidandole come parametri per gli script di azione. È possibile creare proprietà software che prevedano valori di tipo stringa, array, contenuti, booleani o interi. È possibile fornire il valore autonomamente, chiedere a un altro utente di fornire il valore o recuperare il valore da un altro componente di blueprint creando un binding.

Opzioni delle proprietà

È possibile elaborare il valore di qualsiasi proprietà stringa selezionando la casella di controllo Elaborate, nonché rendere qualsiasi proprietà codificata, sovrascrivibile o obbligatoria selezionando le caselle di controllo appropriate durante la configurazione delle proprietà di Software. Combinando queste opzioni con i propri valori è possibile raggiungere obiettivi di vario tipo. Ad esempio, è possibile chiedere agli architetti di blueprint di fornire un valore per una password e codificare tale valore quando utilizzano il componente software in un blueprint. Creare la proprietà password, ma lasciare la casella di testo del valore vuota. Selezionare Sovrascrivibile, Obbligatorio e Codificato. Se la password prevista appartiene all'utente finale, l'architetto di blueprint può selezionare **Mostra nella richiesta** per chiedere agli utenti di immettere la password quando compilano il modulo di richiesta.

Opzione	Descrizione
Codificato	Contrassegnare le proprietà come codificate per mascherare il valore e visualizzarle sovrapponendo asterischi in vRealize Automation. Se si cambia una proprietà da codificata a non codificata, vRealize Automation reimposta il valore della proprietà. Per sicurezza è necessario impostare un nuovo valore per la proprietà.
Sovrascrivibile	Consentire agli architetti di modificare il valore di questa proprietà quando assemblano un blueprint di applicazione. Il valore eventualmente immesso viene visualizzato come predefinito.
Obbligatorio	Impone agli architetti di specificare un valore per la proprietà o accettare il valore predefinito fornito.
Elaborate	I valori delle proprietà elaborate vengono assegnati dagli script del ciclo di vita di INSTALLAZIONE, CONFIGURAZIONE, AVVIO o AGGIORNAMENTO. Il valore assegnato viene propagato alle successive fasi del ciclo di vita disponibili e ai componenti che effettuano il binding a queste proprietà in un blueprint. Se si seleziona Valore elaborato per una proprietà non di tipo stringa, il tipo della proprietà viene modificato in Stringa.

Se si seleziona l'opzione di proprietà Elaborate, non specificare alcun valore per la proprietà personalizzata. Progettare script personalizzati per i valori elaborati.

Tabella 3-44. Esempi di script per l'opzione di proprietà Elaborate

Proprietà stringa campione	Sintassi script	Uso del campione
my_unique_id = ""	Bash - \$my_unique_id	<pre>export my_unique_id="0123456789"</pre>
	Windows CMD - %my_unique_id%	<pre>set my_unique_id=0123456789</pre>
	Windows PowerShell - \$my_unique_id	<pre>\$my_unique_id = "0123456789"</pre>

Proprietà stringa

Le proprietà di stringhe prevedono valori di stringa. È possibile fornire la stringa autonomamente, chiedere a un altro utente di fornire il valore o recuperare il valore da un altro componente di blueprint creando un binding a un'altra proprietà di stringa. I valori di stringa possono contenere qualsiasi carattere ASCII. Per creare un binding di proprietà, usare la scheda **Proprietà** nella tela di progettazione del blueprint per selezionare la proprietà idonea per il binding. Il valore della

proprietà viene quindi passato agli script dell'azione come dati della stringa non elaborati. Quando si esegue il binding a una proprietà stringa di blueprint, accertarsi che il componente di blueprint sottoposto a binding non possa essere aggiunto a un cluster. Se il componente è in clustering, il valore di stringa diventa un array e non si recupera il valore previsto.

Proprietà stringa campione	Sintassi dello script	Uso del campione
admin_email = "admin@email987.com"	Bash - \$admin_email	echo \$admin_email
	Windows CMD - %admin_email%	echo %admin_email%
	Windows PowerShell - \$admin_email	write-output \$admin_email

Proprietà array

Le proprietà di array prevedono un array di valori stringa, interi, decimali o booleani definiti [*"value1"*, *"value2"*, *"value3"*...]. È possibile fornire i valori autonomamente, chiedere a un altro utente di fornire i valori o recuperare i valori da un altro componente di blueprint creando un binding.

Quando si crea una proprietà software di tipo Array, in cui il tipo di dati è intero o decimale, è necessario utilizzare un punto e virgola come separatore dell'elemento di array, indipendentemente dalle impostazioni locali. Non utilizzare una virgola (,) o un punto (.). Per alcune impostazioni locali, è possibile utilizzare una virgola (,) come separatore decimale. Ad esempio:

- Un array valido per il francese è simile a: [1,11;2,22;3,33]
- Un array valido per l'inglese è simile a: [1.11,2.22,3.33]

Quando si passano numeri grandi in un array, non utilizzare il formato di raggruppamento. Ad esempio, non utilizzare **4444 444.000** (francese), **4.444.444,000** (italiano) o **4,444,444.000** (inglese), poiché i file di dati che contengono formati specifici delle impostazioni locali potrebbero essere interpretati erroneamente quando vengono trasferiti in una macchina con impostazioni locali diverse. Il formato di raggruppamento non è consentito, perché un numero come **4,444,444.000** verrebbe considerato come tre numeri separati. Al contrario, è sufficiente immettere **4444444.000**.

Quando i valori di una proprietà array vengono definiti, è necessario includere l'array tra parentesi quadre. Per un array delle stringhe, il valore degli elementi dell'array può contenere qualsiasi carattere ASCII. Per codificare correttamente una barra rovesciata in un valore della proprietà array, aggiungere un'altra barra rovesciata, ad esempio, [*"c:\\test1\\test2"*]. Per una proprietà associata, utilizzare la scheda **Proprietà** nella tela di progettazione per selezionare la proprietà idonea per il binding. Se si esegue il binding a un array, è necessario progettare i componenti software affinché non prevedano l'array di un valore in un ordine specifico.

Ad esempio, se si prende in considerazione una macchina virtuale del bilanciamento del carico che bilancia il carico di un cluster delle macchine virtuali del server delle applicazioni. In tale caso, la proprietà array viene definita per il servizio del bilanciamento del carico e impostata sull'array degli indirizzi IP delle macchine virtuali del server delle applicazioni.

Questi script di configurazione del servizio di bilanciamento del carico usano la proprietà array per configurare lo schema di bilanciamento appropriato sui sistemi operativi Red Hat, Windows e Ubuntu.

Proprietà array campione	Sintassi dello script	Uso del campione
operating_systems = ["Red Hat", "Windows", "Ubuntu"]	Bash - \${operating_systems[@]} per l'intero array delle stringhe \${operating_systems[N]} per l'elemento di array individuale	for ((i = 0 ; i < \$ {#operating_systems[@]}; i++)); do echo \${operating_systems[i]} done
	Windows CMD - %operating_systems_% dove N rappresenta la posizione dell'elemento nell'array	for /F "delims== tokens=2" %%A in ('set operating_systems_') do (echo %%A)
	Windows PowerShell - \$operating_systems per l'intero array delle stringhe \$operating_systems[N] per l'elemento di array individuale	foreach (\$os in \$operating_systems){ write-output \$os }

Proprietà contenuto

Il valore della proprietà contenuto è l'URL di un file per il download dei contenuti. L'agente di Software scarica i contenuti dall'URL nella macchina virtuale e passa la posizione del file locale nella macchina virtuale allo script.

Le proprietà contenuto devono essere definite come URL valido con il protocollo HTTP o HTTPS. Ad esempio, il componente JBOSS Application Server Software nell'applicazione campione Dukes Bank specifica cheetah_tgz_url come proprietà del contenuto. Gli elementi sono ospitati nell'appliance Software e l'URL punta a tale posizione nell'appliance. L'agente di Software scarica gli elementi dalla posizione specificata nella macchina virtuale distribuita.

Per informazioni sulle impostazioni di software.http.proxy che è possibile utilizzare con le proprietà di contenuti, vedere *Guida di riferimento alle proprietà personalizzate*.

Proprietà stringa campione	Sintassi dello script	Uso del campione
cheetah_tgz_url = "http:// app_content_server_ip:port/artifacts/ software/jboss/cheetah-2.4.4.tar.gz"	Bash - \$cheetah_tgz_url	tar -zxvf \$cheetah_tgz_url
	Windows CMD - %cheetah_tgz_url%	start /wait c:\unzip.exe %cheetah_tgz_url%

Proprietà stringa campione	Sintassi dello script	Uso del campione
	Windows PowerShell - \$cheetah_tgz_url	& c:\unzip.exe \$cheetah_tgz_url

Proprietà booleana

Utilizzare il tipo di proprietà booleano per fornire le opzioni True e False nel menu a discesa Valore.

Proprietà numero intero

Utilizzare il tipo di proprietà booleano per zero e numeri interi positivi o negativi.

Proprietà decimale

Utilizzare il tipo di proprietà decimale per valori che rappresentano frazioni decimali senza ripetizioni.

Quando il componente Software richiede informazioni da un altro componente

In diversi scenari di distribuzione, per essere personalizzato, un componente deve avere il valore di proprietà di un altro componente. È possibile eseguire questa operazione con vRealize Automation creando binding di proprietà. È possibile progettare gli script di azione di Software per i binding di proprietà, tuttavia i binding attuali sono configurati dall'architetto che assembla il blueprint.

Oltre a impostare una proprietà con un valore hardcoded, un architetto IaaS, di software o di applicazioni può associare le proprietà dei componenti Software ad altre proprietà nel blueprint. Ad esempio, può associare un indirizzo IP o un percorso di installazione. Quando si associa una proprietà Software a un'altra proprietà, è possibile personalizzare uno script in base al valore della proprietà di un altro componente o di una macchina virtuale. Ad esempio, per un componente WAR, potrebbe essere necessaria la posizione di installazione del server Apache Tomcat. Negli script, configurare il componente WAR affinché il valore della proprietà `server_home` sia impostato sul valore della proprietà `install_path` del server Apache Tomcat server. Se l'architetto che assembla il blueprint associa la proprietà `server_home` alla proprietà `install_path` del server Apache Tomcat, il valore della proprietà `server_home` verrà impostato correttamente.

Gli script di azione possono utilizzare solo le proprietà definite in tali script ed è possibile creare esclusivamente binding di proprietà con valori di stringhe e array. Gli array delle proprietà di binding non vengono restituiti in alcun ordine specifico, quindi la creazione di binding a componenti in cluster o scalabili potrebbe non produrre i valori che previsti. Ad esempio, il componente software richiede i singoli ID delle macchine di un cluster di macchine e si consente agli utenti di richiedere un cluster da 1-10 e di scalare la distribuzione da 1-10 macchine. Se si configura la proprietà software come un tipo di stringa, viene restituito un singolo ID di macchina selezionato in modo casuale dal cluster. Se si configura la proprietà software come un tipo di array, viene restituito un array di tutti gli ID delle macchine nel cluster, senza alcun ordine

particolare. Se gli utenti scalano la distribuzione, l'ordine dei valori potrebbe differire per ogni operazione. Per accertarsi di non perdere mai i valori per i componenti in cluster, è possibile utilizzare il tipo di array per qualsiasi proprietà software. Tuttavia, è necessario progettare i componenti software affinché non prevedano l'array di un valore in un ordine specifico.

La tabella Esempi di binding per proprietà stringa fornisce alcuni esempi di valori di proprietà stringa per il binding a diversi tipi di proprietà.

Tabella 3-45. Esempi di binding per proprietà stringa

Tipo di proprietà campione	Tipo di proprietà da associare	Risultato del binding (A viene associata a B)
Stringa (proprietà A)	Stringa (proprietà B="Hi")	A="Hi"
Stringa (proprietà A)	Contenuto (proprietà B="http://my.com/content")	A="http://my.com/content"
Stringa (proprietà A)	Array (proprietà B=["1","2"])	A=["1","2"]
Stringa (proprietà A)	Elaborata (proprietà B="Hello")	A="Hello"

La tabella Esempi di binding per proprietà array fornisce alcuni esempi di valori di proprietà array per il binding a diversi tipi di proprietà.

Tabella 3-46. Esempi di binding per proprietà array

Tipo di proprietà campione	Tipo di proprietà da associare	Risultato del binding (A viene associata a B)
Array (proprietà A)	Stringa (proprietà B="Hi")	A="Hi"
Array (proprietà A)	Contenuto (proprietà B="http://my.com/content")	A="http://my.com/content"
Array (proprietà A)	Elaborata (proprietà B="Hello")	A="Hello"

Per una spiegazione dettagliata dei tipi di proprietà supportati, vedere [Tipi di proprietà e opzioni di impostazione](#).

Passaggio dei valori delle proprietà tra fasi del ciclo di vita

È possibile modificare e passare valori di proprietà da una fase all'altra del ciclo di vita utilizzando gli script di azione.

Per una proprietà elaborata, è possibile modificare il valore della proprietà e passare il valore alla fase del ciclo di vita successiva dello script di azione. Ad esempio, se il valore `progress_status` del componente A viene definito come installazione eseguita, nella fase del ciclo di vita `INSTALLAZIONE` e `CONFIGURAZIONE`, è possibile modificare il valore in `progress_status=installed` nei rispettivi script di azione. Se il componente B è associato al componente A, i valori di proprietà di `progress_status` nelle fasi del ciclo di vita dello script di azione sono i medesimi del componente A.

Definire nel componente software che il componente B dipende da A. Tale dipendenza definisce il passaggio dei valori di proprietà corretti tra i componenti, che si trovino nello stesso nodo o in nodi differenti.

Ad esempio, è possibile aggiornare il valore di proprietà in uno script di azione usando gli script supportati.

- Bash `progress_status="completed"`
- CMD di Windows `set progress_status=completed`
- Windows PowerShell `$progress_status="completed"`

Nota le proprietà array e contenuto non supportano i valori di proprietà modificati nel passaggio tra script di azione delle fasi del ciclo di vita.

Procedure consigliate per lo sviluppo dei componenti

Per familiarizzare con le procedure consigliate per la definizione di proprietà e script di azioni, è possibile scaricare e importare componenti Software e blueprint di applicazioni da VMware Solution Exchange.

Seguire le procedure consigliate per sviluppare componenti Software.

- Per l'esecuzione di uno script senza interruzioni, il valore restituito deve essere impostato su zero (0). Tale impostazione consente all'agente di acquisire tutte le proprietà e di inviarle al server Software.
- Alcuni programmi di installazione potrebbero dover accedere alla console tty. Reindirizzare l'input da `/dev/console`. Ad esempio, un componente Software RabbitMQ potrebbe utilizzare il comando `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` nel proprio script di installazione.
- Quando un componente usa più fasi del ciclo di vita, il valore della proprietà può essere modificato nella fase del ciclo di vita INSTALLAZIONE. Il nuovo valore viene inviato alla fase del ciclo di vita successiva. Gli script delle azioni sono in grado di elaborare il valore di una proprietà durante la distribuzione, per fornire il valore ad altri script dipendenti. Ad esempio, nell'applicazione Clustered Dukes Bank, il servizio JBossAppServer elabora la proprietà JVM_ROUTE durante la fase Installazione del ciclo di vita. Tale proprietà viene usata dal servizio JBossAppServer per configurare il ciclo di vita. Il servizio di bilanciamento del carico Apache associa quindi la proprietà JVM_ROUTE alla proprietà `all(appserver:JBossAppServer:JVM_ROUTE)`, per ottenere il valore elaborato finale di `node0` e `node1`. Se, per completare correttamente la distribuzione di un'applicazione, un componente necessita di un valore di proprietà di un altro componente, è necessario dichiarare dipendenze esplicite nel blueprint dell'applicazione.

Nota non è possibile modificare il valore di proprietà del contenuto per un componente che utilizza più fasi del ciclo di vita.

Creazione di un componente Software

Configurare e pubblicare un componente Software che possa essere utilizzato dagli altri architetti software, IaaS e di applicazioni per assemblare blueprint di applicazioni.

Prerequisiti

Accedere a vRealize Automation come **architetto del software**.

Procedura

1 Selezionare **Progettazione > Componenti software**.

2 Fare clic sull'icona **Aggiungi** (+).

3 Immettere un nome e, facoltativamente, una descrizione.

Utilizzando il nome specificato per il componente Software, vRealize Automation crea un ID per il componente Software che è univoco all'interno del tenant. È possibile modificare il campo, ma dopo aver salvato il blueprint il campo non potrà più essere modificato. Dato che gli ID sono permanenti e unici all'interno del tenant, è possibile utilizzarli per interagire con i blueprint tramite programmazione e per creare binding di proprietà.

4 (Facoltativo) Se si desidera poter controllare il modo in cui il componente Software viene incluso nei blueprint, selezionare un tipo di contenitore dal menu a discesa **Contenitore**.

Opzione	Descrizione
Macchine	Il componente Software deve essere inserito direttamente in una macchina.
Uno dei componenti Software pubblicati	Se si progetta un componente Software che dovrà essere installato su un altro componente Software già creato, selezionare tale componente Software dall'elenco. Ad esempio, se si progetta un componente EAR da installare sul componente JBOSS precedentemente creato, selezionare il componente JBOSS dall'elenco.
Componenti software	Se si progetta un componente Software che non deve essere installato direttamente su una macchina, ma può essere installato su diversi componenti Software, selezionare l'opzione Componenti software. Ad esempio, se si progetta un componente WAR che dovrà essere installato sul componente Software Tomcat Server e sul componente Software Tcserver, selezionare il tipo di contenitore Componenti software.

5 Fare clic su **Avanti**.

6 Definire eventuali proprietà da utilizzare negli script di azione.

a Fare clic sull'icona **Aggiungi** (+).

b Specificare il nome della proprietà.

c Immettere la descrizione della proprietà.

La descrizione viene visualizzata per gli architetti che utilizzano il componente Software nei blueprint.

- d Selezionare il tipo previsto per il valore della proprietà.
- e Definire il valore della proprietà.

Opzione	Descrizione
Utilizzare il valore fornito	<ul style="list-style-type: none"> ■ Immettere un valore. ■ Deselezionare Sovrascrivibile. ■ Selezionare Obbligatorio.
Chiedere agli architetti di fornire un valore	<ul style="list-style-type: none"> ■ Per fornire un valore predefinito, immettere un valore. ■ Selezionare Sovrascrivibile. ■ Selezionare Obbligatorio.
Consentire agli architetti di fornire un valore se lo desiderano	<ul style="list-style-type: none"> ■ Per fornire un valore predefinito, immettere un valore. ■ Selezionare Sovrascrivibile. ■ Deselezionare Obbligatorio.

Gli architetti possono configurare le proprietà Software da visualizzare per gli utenti nel modulo di richiesta. Per richiedere che gli utenti compilino i valori per le proprietà contrassegnate come sovrascrivibili, gli architetti possono usare l'opzione Mostra nella richiesta.

- 7 Seguire le istruzioni visualizzate per fornire uno script per almeno una delle azioni del ciclo di vita del software.

Tabella 3-47. Azioni del ciclo di vita

Azioni del ciclo di vita	Descrizione
Installazione	Installare il software. Ad esempio, è possibile scaricare i bit di installazione del server Tomcat e installare un servizio Tomcat. Gli script compilati per l'azione del ciclo di vita di installazione vengono eseguiti quando il software viene sottoposto a provisioning per la prima volta, durante una richiesta di distribuzione iniziale o come parte di un'operazione di scalabilità orizzontale.
Configurazione	Configurare il software. Nel caso dell'esempio Tomcat, è possibile impostare i valori JAVA_OPTS e CATALINA_OPTS. Gli script di configurazione vengono eseguiti al termine dell'azione di installazione.
Avvio	Avviare il software. Ad esempio, è possibile avviare il servizio Tomcat utilizzando il comando di avvio nel server Tomcat. Gli script di avvio vengono eseguiti al termine dell'azione di configurazione.
Aggiornamento	Se si sta progettando il componente software affinché supporti blueprint scalabili, gestire gli eventuali aggiornamenti richiesti dopo un'operazione di scalabilità verticale o scalabilità orizzontale. Ad esempio, è possibile modificare la dimensione del cluster per una distribuzione scalata e gestire i nodi in clustering utilizzando un bilanciamento del carico. Progettare gli script di aggiornamento affinché vengano eseguiti più volte (idempotent) e in modo da poter gestire sia le situazioni di scalabilità verticale che di scalabilità orizzontale. Quando si esegue un'operazione di scalabilità, gli script di aggiornamento vengono eseguiti in tutti i componenti software dipendenti.
Disinstallazione	Disinstallare il software. Ad esempio, è possibile eseguire azioni specifiche nell'applicazione prima della distruzione di una distribuzione. Gli script di disinstallazione vengono eseguiti ogni volta che si distruggono componenti software.

Includere codici di uscita e di stato negli script di azione. Ogni tipo di script supportato ha requisiti propri per i codici di uscita e stato.

Tipo di script	Stato di operazione completata	Stato di errore	Comandi non supportati
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Nessuno
Windows CMD	exit /b 0	exit /b non-zero	Non utilizzare i codici exit 0 o exit non-zero.
PowerShell	exit 0	exit non-zero;	Non utilizzare le chiamate warning, verbose, debug o host

- 8** Selezionare la casella di controllo **Riavvia** per gli script che richiedono il riavvio della macchina.

Dopo l'esecuzione dello script, la macchina viene riavviata prima che venga iniziato il successivo script del ciclo di vita.

- 9** Fare clic su **Fine**.

- 10** Selezionare il componente Software e fare clic su **Pubblica**.

Risultati

È stato configurato e pubblicato un componente Software. Gli altri architetti software, IaaS e delle applicazioni possono utilizzare questo componente Software per aggiungere software ai blueprint di applicazioni.

Operazioni successive

Aggiungere il componente Software pubblicato a un blueprint di applicazioni. Vedere [Assemblaggio di blueprint compositi](#).

Impostazioni dei componenti Software

Configurare impostazioni generali, creare proprietà e scrivere script di azione personalizzati per installare, configurare, aggiornare o disinstallare il componente Software sulle macchine con provisioning eseguito.

Un architetto software può fare clic su **Progettazione > Componenti software** e quindi sull'icona **Aggiungi** per creare un nuovo componente Software.

Impostazioni generali nuovo Software

Applicare impostazioni generali al componente Software.

Tabella 3-48. Impostazioni generali nuovo Software

Impostazione	Descrizione
Nome	Specificare il nome del componente Software.
ID	Utilizzando il nome specificato per il componente Software, vRealize Automation crea un ID per il componente Software che è univoco all'interno del tenant. È possibile modificare il campo, ma dopo aver salvato il blueprint il campo non potrà più essere modificato. Dato che gli ID sono permanenti e unici all'interno del tenant, è possibile utilizzarli per interagire con i blueprint tramite programmazione e per creare binding di proprietà.
Descrizione	Testo che riepiloga il componente Software a vantaggio di altri architetti.
Contenitore	<p>Nella tela di progettazione, gli architetti di blueprint possono collocare i componenti di Software solo nel tipo di contenitore selezionato.</p> <ul style="list-style-type: none"> ■ Selezionare Macchine per chiedere agli architetti di collocare il componente di Software direttamente in un componente di macchina nella tela di progettazione. ■ Selezionare Componenti software se si sta progettando un componente di Software che non dovrà mai essere collocato direttamente in un componente di macchina ma che può essere nidificato in uno dei diversi componenti di Software. ■ Selezionare un componente pubblicato specifico di Software se si sta progettando specificamente un componente di Software da nidificare in un altro componente di Software creato. ■ Selezionare Macchina virtuale Azure se si sta progettando specificamente un componente di Software per un blueprint Azure.

Nuove proprietà di Software

Le proprietà del componente Software vengono utilizzate per impostare i parametri degli script in modo tale da trasmettere le proprietà definite come variabili di ambiente agli script in esecuzione in una macchina virtuale. Prima di eseguire script, l'agente Software nella macchina con provisioning eseguito comunica con vRealize Automation per risolvere le proprietà. Da tali proprietà, l'agente crea variabili specifiche per lo script e le trasmette agli script.

Tabella 3-49. Nuove proprietà di Software

Impostazione	Descrizione
Nome	Specificare il nome della proprietà Software. Ai nomi delle proprietà viene applicata la distinzione tra maiuscole e minuscole e possono contenere solo caratteri alfabetici, numerici, il trattino (-) o il carattere di sottolineatura (_).
Descrizione	A vantaggio degli altri utenti, allegare un riepilogo della proprietà e indicazioni su eventuali requisiti del valore.
Tipo	Software supporta tipi di valori stringa, array, contenuti, booleani e interi. Per una spiegazione dettagliata dei tipi di proprietà supportati, vedere Tipi di proprietà e opzioni di impostazione . Per informazioni sui binding delle proprietà, vedere Quando il componente Software richiede informazioni da un altro componente e Creazione di binding di proprietà tra componenti di blueprint .
Valore	<ul style="list-style-type: none"> ■ Per utilizzare il valore fornito: <ul style="list-style-type: none"> ■ Immettere un valore. ■ Selezionare Obbligatorio. ■ Deselezionare Sovrascrivibile. ■ Per chiedere agli architetti di fornire un valore: <ul style="list-style-type: none"> ■ (Facoltativo) Immettere un valore per fornire un'impostazione predefinita. ■ Selezionare Sovrascrivibile. ■ Selezionare Obbligatorio. ■ Consentire agli architetti di fornire un valore o lasciare il valore vuoto: <ul style="list-style-type: none"> ■ (Facoltativo) Immettere un valore per fornire un'impostazione predefinita. ■ Selezionare Sovrascrivibile. ■ Deselezionare Obbligatorio.
Codificato	<p>Contrassegnare le proprietà come codificate per mascherare il valore e visualizzarle sovrapponendo asterischi in vRealize Automation. Se si cambia una proprietà da codificata a non codificata, vRealize Automation reimposta il valore della proprietà. Per sicurezza è necessario impostare un nuovo valore per la proprietà.</p> <p>Importante se le proprietà protette vengono stampate nello script usando il comando echo o altri comandi simili, tali valori vengono visualizzati nei file di registro come testo normale. I valori dei file di registro non sono nascosti.</p>
Sovrascrivibile	Consentire agli architetti di modificare il valore di questa proprietà quando assemblano un blueprint di applicazione. Il valore eventualmente immesso viene visualizzato come predefinito.

Tabella 3-49. Nuove proprietà di Software (continua)

Impostazione	Descrizione
Obbligatorio	Impone agli architetti di specificare un valore per la proprietà o accettare il valore predefinito fornito.
Elaborate	I valori delle proprietà elaborate vengono assegnati dagli script del ciclo di vita di INSTALLAZIONE, CONFIGURAZIONE, AVVIO o AGGIORNAMENTO. Il valore assegnato viene propagato alle successive fasi del ciclo di vita disponibili e ai componenti che effettuano il binding a queste proprietà in un blueprint. Se si seleziona Valore elaborato per una proprietà non di tipo stringa, il tipo della proprietà viene modificato in Stringa.

Nuove azioni Software

Si creano script di azione Bash, Windows CMD o PowerShell per specificare esattamente le modalità di installazione, configurazione, disinstallazione o aggiornamento dei componenti durante le operazioni di scalabilità delle distribuzioni.

Tabella 3-50. Azioni del ciclo di vita

Azioni del ciclo di vita	Descrizione
Installazione	Installare il software. Ad esempio, è possibile scaricare i bit di installazione del server Tomcat e installare un servizio Tomcat. Gli script compilati per l'azione del ciclo di vita di installazione vengono eseguiti quando il software viene sottoposto a provisioning per la prima volta, durante una richiesta di distribuzione iniziale o come parte di un'operazione di scalabilità orizzontale.
Configurazione	Configurare il software. Nel caso dell'esempio Tomcat, è possibile impostare i valori JAVA_OPTS e CATALINA_OPTS. Gli script di configurazione vengono eseguiti al termine dell'azione di installazione.
Avvio	Avviare il software. Ad esempio, è possibile avviare il servizio Tomcat utilizzando il comando di avvio nel server Tomcat. Gli script di avvio vengono eseguiti al termine dell'azione di configurazione.
Aggiornamento	Se si sta progettando il componente software affinché supporti blueprint scalabili, gestire gli eventuali aggiornamenti richiesti dopo un'operazione di scalabilità verticale o scalabilità orizzontale. Ad esempio, è possibile modificare la dimensione del cluster per una distribuzione scalata e gestire i nodi in clustering utilizzando un bilanciamento del carico. Progettare gli script di aggiornamento affinché vengano eseguiti più volte (idempotent) e in modo da poter gestire sia le situazioni di scalabilità verticale che di scalabilità orizzontale. Quando si esegue un'operazione di scalabilità, gli script di aggiornamento vengono eseguiti in tutti i componenti software dipendenti.
Disinstallazione	Disinstallare il software. Ad esempio, è possibile eseguire azioni specifiche nell'applicazione prima della distruzione di una distribuzione. Gli script di disinstallazione vengono eseguiti ogni volta che si distruggono componenti software.

Selezionare la casella di controllo **Riavvia** per gli script che richiedono il riavvio della macchina. Dopo l'esecuzione dello script, la macchina viene riavviata prima che venga iniziato il successivo script del ciclo di vita. Verificare che non vi siano processi che richiedono l'interazione dell'utente quando lo script dell'azione è in esecuzione. Le interruzioni mettono lo script in pausa, causando

uno stato di inattività indefinito, con conseguente esito negativo dell'operazione. Inoltre, gli script devono includere codici di uscita appropriati applicabili alla distribuzione di applicazioni. Se lo script non ha i codici di uscita e di restituzione, l'ultimo comando eseguito nello script diventa lo stato di uscita. I codici di uscita e ritorno variano in base ai tipi di script supportati: Bash, Windows CMD, PowerShell.

Tipo di script	Stato di operazione completata	Stato di errore	Comandi non supportati
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Nessuno
Windows CMD	exit /b 0	exit /b non-zero	Non utilizzare i codici exit 0 o exit non-zero.
PowerShell	exit 0	exit non-zero;	Non utilizzare le chiamate warning, verbose, debug o host

Progettazione di blueprint e azioni risorsa di XaaS

I blueprint di XaaS possono essere pubblicati come elementi del catalogo o utilizzati nelle tele di progettazione di blueprint. Le azioni risorsa sono azioni che possono essere eseguite sugli elementi che vengono distribuiti.

XaaS utilizza vRealize Orchestrator per eseguire i workflow per il provisioning di elementi o l'esecuzione di azioni. Ad esempio, è possibile configurare i workflow per creare macchine virtuali di vSphere, utenti Active Directory in gruppi o per eseguire script di PowerShell. Se si crea un workflow vRealize Orchestrator personalizzato, questo può essere fornito come elemento nel catalogo dei servizi, in modo da consentirne l'esecuzione da parte degli utenti autorizzati.

Un blueprint XaaS può essere utilizzato come componente di un altro blueprint che si sta creando sulla tela di progettazione oppure può essere pubblicato direttamente nel catalogo dei servizi.

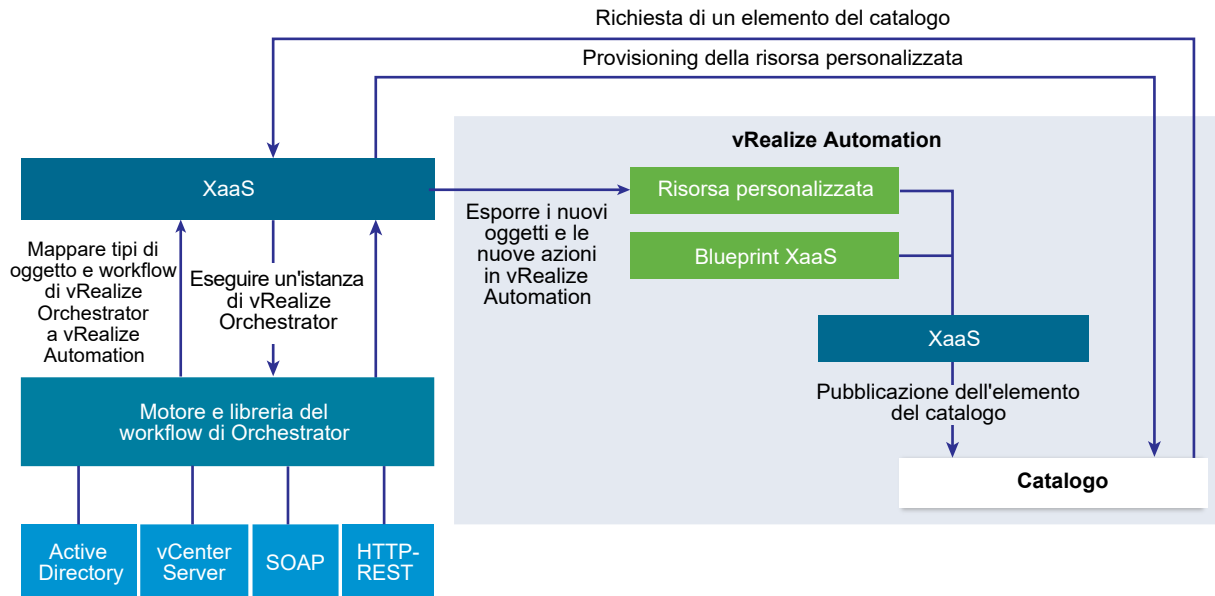
Se si utilizza il blueprint come componente di un altro blueprint, è possibile configurarne la scalabilità per i casi in cui il blueprint da distribuire venga scalato in verticale o in orizzontale.

Integrazione di vRealize Orchestrator in vRealize Automation

vRealize Orchestrator è il motore di workflow integrato in vRealize Automation.

Il server vRealize Orchestrator distribuito con vRealize Automation è preconfigurato e pertanto, quando l'amministratore di sistema distribuisce vRealize Automation Appliance, il server vRealize Orchestrator è configurato e in esecuzione.

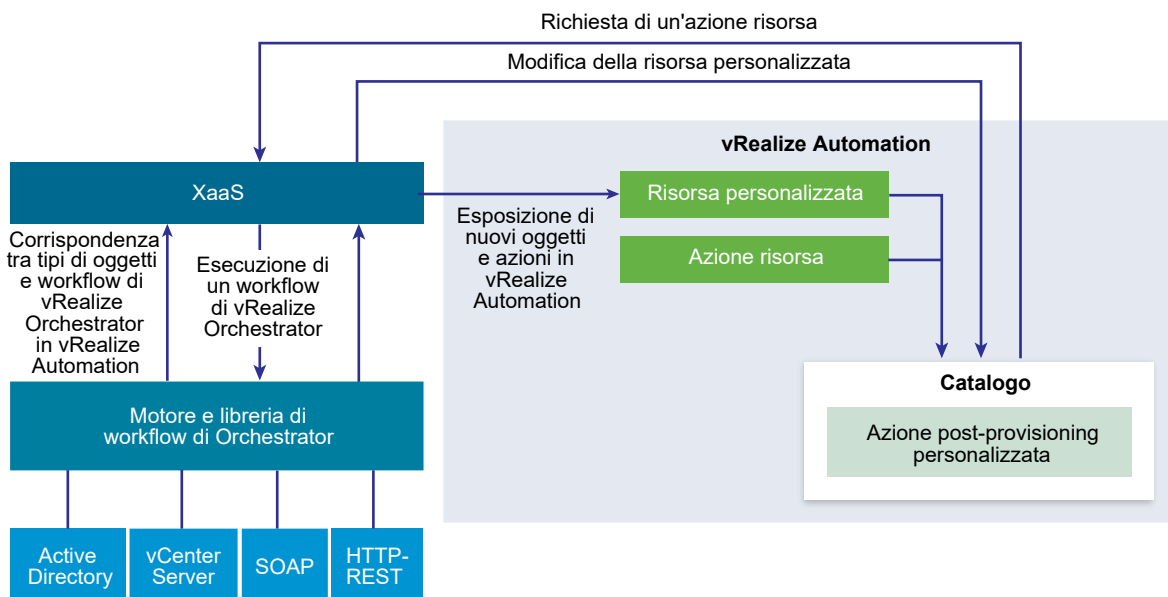
Figura 3-2. Creazione e richiesta di elementi di catalogo inclusi in un XaaS per il provisioning di una risorsa personalizzata



Gli architetti di XaaS aggiungono risorse personalizzate correlate agli endpoint supportati e ai workflow forniti e poi creano blueprint e azioni di XaaS sulla base di queste risorse. Gli amministratori tenant e i manager dei gruppi di business possono aggiungere i blueprint e le azioni di XaaS al catalogo dei servizi. Il blueprint di XaaS può essere utilizzato anche nel designer di blueprint.

Quando l'utente del catalogo dei servizi richiede un elemento, vRealize Automation esegue un workflow di vRealize Orchestrator per eseguire il provisioning della risorsa personalizzata.

Figura 3-3. Creazione e richiesta di azioni di risorse personalizzate per la modifica di una risorsa personalizzata



Gli architetti di XaaS possono aggiungere workflow di vRealize Orchestrator come azioni risorsa per estendere le funzionalità di vRealize Automation. Dopo aver eseguito il provisioning di una risorsa personalizzata, gli utenti del catalogo dei servizi possono eseguire l'azione di post-provisioning. In questo modo, i clienti eseguono un workflow di vRealize Orchestrator e modificano la risorsa personalizzata con provisioning eseguito.

Quando un utente di un catalogo dei servizi richiede un blueprint di XaaS o un'azione risorsa come elemento di catalogo, il servizio XaaS esegue il workflow di vRealize Orchestrator corrispondente, passando al workflow i seguenti dati come parametri globali:

Tabella 3-51. Parametri globali di XaaS

Parametro	Descrizione
__asd_tenantRef	Tenant dell'utente che richiede il workflow.
__asd_subtenantRef	Gruppo di business dell'utente che richiede il workflow.
__asd_catalogRequestId	ID della richiesta dal catalogo per l'esecuzione del workflow.
__asd_requestedFor	Utente di destinazione della richiesta. Se la richiesta è per conto di un utente, questo parametro è l'utente per conto del quale il workflow viene richiesto, altrimenti è l'utente che richiede il workflow.
__asd_requestedBy	L'utente che richiede il workflow.

Se un blueprint di XaaS o un'azione risorsa utilizza un workflow di vRealize Orchestrator che contiene un elemento dello schema di interazione utente, quando un cliente richiede il servizio, il workflow ne sospende l'esecuzione e attende che l'utente fornisca i dati richiesti. Per rispondere a un'interazione utente in attesa, l'utente deve passare a **Posta in arrivo > Azione utente manuale**.

L'inventario del server vRealize Orchestrator predefinito è condiviso tra tutti i tenant e non può essere utilizzato per tenant. Ad esempio, se un architetto di servizi crea un blueprint di servizio per la creazione di una risorsa di elaborazione cluster, i clienti di tenant diversi devono sfogliare gli elementi dell'inventario di tutte le istanze di vCenter Server, sebbene possano appartenere a un altro tenant.

Gli amministratori di sistema possono installare vRealize Orchestrator o distribuire vRealize Orchestrator Appliance separatamente per impostare un'istanza di vRealize Orchestrator esterna e configurare vRealize Automation per lavorare con quella istanza di vRealize Orchestrator esterna.

Gli amministratori di sistema possono anche configurare categorie di workflow di vRealize Orchestrator per tenant e definire quali workflow debbano essere disponibili a ciascun tenant.

Inoltre, gli amministratori tenant possono anche configurare un'istanza di vRealize Orchestrator esterna, ma solo per i propri tenant.

Per informazioni sulla configurazione di un'istanza di vRealize Orchestrator esterna e categorie di workflow di vRealize Orchestrator, vedere *Configurazione di vCenter Orchestrator e plug-in*.

Elenco di plug-in di vRealize Orchestrator

I plug-in consentono di utilizzare vRealize Orchestrator per accedere alle tecnologie e alle applicazioni esterne, nonché controllarle. L'esposizione di una tecnologia esterna in un plug-in di vRealize Orchestrator permette di incorporare oggetti e funzioni in workflow che accedono agli oggetti e alle funzioni della tecnologia esterna.

Le tecnologie esterne alle quali è possibile accedere mediante i plug-in possono includere strumenti di gestione della virtualizzazione, sistemi email, database, servizi di directory, interfacce di controllo remoto e così via.

È possibile utilizzare il set standard di plug-in di vRealize Orchestrator per incorporare nei workflow tecnologie esterne quali l'API di vCenter Server e le funzionalità email. È inoltre possibile utilizzare l'architettura aperta dei plug-in di vRealize Orchestrator per sviluppare plug-in con cui accedere ad altre applicazioni.

Tabella 3-52. Plug-in inclusi per impostazione predefinita in vRealize Orchestrator

Plug-in	Scopo
vCenter Server	Consente di accedere all'API di vCenter Server in modo da poter incorporare tutti gli oggetti e le funzioni di vCenter Server nei processi di gestione che vengono automatizzati utilizzando vRealize Orchestrator.
Configurazione	Offre workflow per la configurazione dell'autenticazione di vRealize Orchestrator, della connessione al database, dei certificati SSL e così via.
vCO Library	Offre workflow che agiscono come componenti costitutivi di base per la personalizzazione e l'automazione dei processi client. La libreria dei workflow include modelli per la gestione del ciclo di vita, il provisioning, il ripristino di emergenza, il backup a caldo e altri processi standard. È possibile copiare e modificare i modelli in base alle proprie esigenze.
SQL	Offre l'API JDBC (Java Database Connectivity), ovvero lo standard di settore per la connettività indipendente dal database tra il linguaggio di programmazione Java e un'ampia gamma di database. I database includono database SQL e altre origini dati in formato tabulare, quali fogli di calcolo o file flat. L'API JDBC offre un'API a livello di chiamata con cui accedere al database basato su SQL dai workflow.
SSH	Offre un'implementazione del protocollo SSH-2 (Secure Shell v2). Consente sessioni remote di trasferimento file e comandi con autenticazione basata su password e chiave pubblica nei workflow. Supporta l'autenticazione interattiva tramite tastiera. Facoltativamente, il plug-in SSH può consentire l'esplorazione remota del file system direttamente dall'inventario del client di vRealize Orchestrator.
XML	Un parser XML DOM (Document Object Model) completo che è possibile implementare nei workflow. In alternativa, è possibile utilizzare l'implementazione E4X (ECMAScript for XML) nell'API JavaScript di vRealize Orchestrator.
Mail	Utilizza il protocollo SMTP (Simple Mail Transfer Protocol) per inviare le email dai workflow.

Tabella 3-52. Plug-in inclusi per impostazione predefinita in vRealize Orchestrator (continua)

Plug-in	Scopo
Net	Include la Jakarta Apache Commons Net Library. Offre implementazioni di Telnet, FTP, POP3 e IMAP. La parte POP3 e IMAP viene utilizzata per leggere le email. In combinazione con il plug-in Mail, il plug-in Net offre funzionalità complete di invio e ricezione delle email nei workflow.
Enumeration	Offre tipi enumerati comuni utilizzabili nei workflow da altri plug-in.
Workflow Documentation	Offre workflow che consentono di generare informazioni in formato PDF su un workflow o una categoria di workflow.
HTTP-REST	Consente di gestire i servizi Web REST permettendo l'interazione tra gli host vCenter Orchestrator e REST.
SOAP	Consente di gestire i servizi Web SOAP permettendo l'interazione tra gli host vCenter Orchestrator e SOAP.
AMQP	Consente di interagire con i server AMQP (Advanced Message Queuing Protocol) anche noti come gestori.
SNMP	Consente a vCenter Orchestrator di connettersi e ricevere informazioni dai sistemi e dai dispositivi abilitati per SNMP.
Active Directory	Consente l'interazione tra vCenter Orchestrator e Microsoft Active Directory.
vCO WebOperator	Una vista Web che consente di accedere ai workflow della libreria di vRealize Orchestrator e interagire con essi attraverso una rete mediante un browser Web.
Dynamic Types	Consente di definire i tipi dinamici, nonché creare e utilizzare gli oggetti di tali tipi dinamici.
PowerShell	Consente di gestire gli host PowerShell ed eseguire operazioni PowerShell personalizzate.
Multi-Node	Contiene workflow per l'orchestrazione gerarchica, la gestione delle istanze di Orchestrator e la scalabilità orizzontale delle attività di Orchestrator.
vRealize Automation	Consente di creare ed eseguire workflow per l'interazione tra vRealize Orchestrator e vRealize Automation.

Per ulteriori informazioni sui plug-in di vRealize Orchestrator sviluppati e distribuiti da VMware, vedere la pagina di destinazione della documentazione di VMware vRealize™ Orchestrator™.

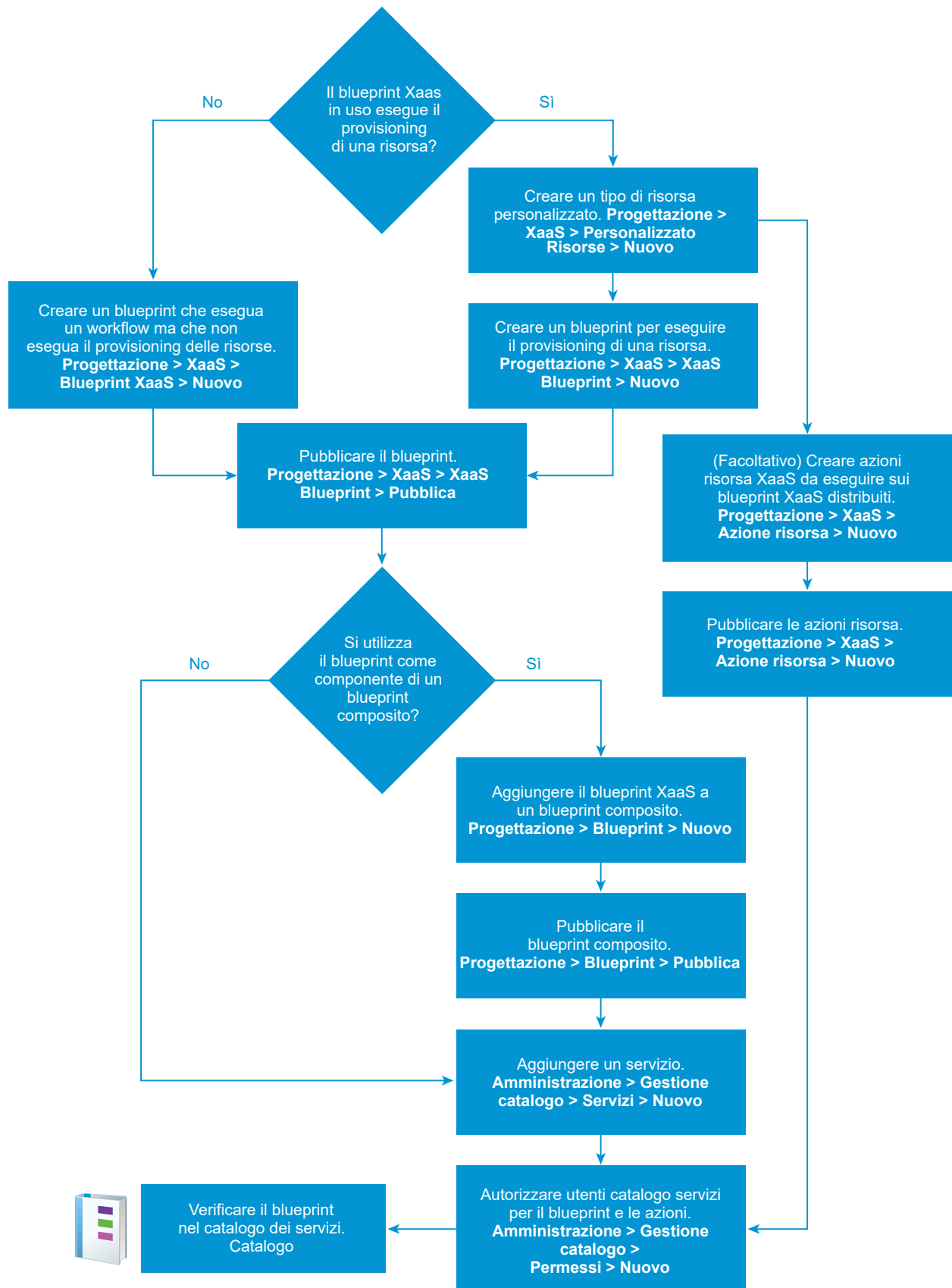
Creazione di blueprint e azioni risorsa di XaaS

I blueprint di XaaS possono essere autorizzati per gli utenti come elementi di catalogo, o assemblati in un blueprint composito utilizzando la tela di progettazione. Le azioni risorsa vengono eseguite sugli elementi forniti in provisioning per poterli gestire dopo il provisioning.

Ad esempio, è possibile utilizzare un blueprint di XaaS per creare gli utenti di Active Directory in un gruppo. È quindi possibile utilizzare un'azione risorsa per rendere la modifica della password da parte degli utenti obbligatoria.

Workflow dei blueprint XaaS

Il workflow da seguire per la creazione di blueprint XaaS ed eventuali azioni risorse facoltative varia a seconda di come si intende utilizzare il blueprint. Il workflow raffigurato di seguito rappresenta il processo di base.



Terminologia dei blueprint XaaS

I blueprint XaaS sono workflow di vRealize Orchestrator in grado di eseguire il provisioning di risorse, apportare modifiche alle risorse sottoposte a provisioning o fungere da servizio che esegue un'attività nell'ambiente. I blueprint e le azioni di risorse presentano diverse sfumature che è necessario comprendere durante la progettazione di blueprint per gli utenti del catalogo dei servizi.

Le seguenti definizioni consentono di comprendere i termini utilizzati quando si utilizzano blueprint di XaaS.

Risorsa personalizzata

Un tipo di oggetto vRealize Orchestrator esposto come risorsa tramite l'API di un plug-in di vRealize Orchestrator. La creazione di una risorsa personalizzata consente di definire il parametro di output di un blueprint di provisioning di XaaS e definire un parametro di input per un'azione di risorse.

Componente del blueprint di XaaS

Un blueprint di provisioning o non di provisioning che è possibile utilizzare nella tela di progettazione del blueprint. Questo blueprint potrebbe essere anche un blueprint autonomo di XaaS.

Blueprint autonomo di XaaS

Un blueprint di provisioning o non di provisioning pubblicato e autorizzato ad accedere direttamente al catalogo dei servizi.

Blueprint di provisioning

Un blueprint di provisioning che esegue un workflow di vRealize Orchestrator per eseguire il provisioning di risorse sull'endpoint di destinazione utilizzando l'API del plug-in di vRealize Orchestrator per l'endpoint. Ad esempio, aggiungere NIC virtuali a un dispositivo di rete in vSphere. Per creare un blueprint di provisioning, è necessario disporre di una risorsa personalizzata che definisca il tipo di risorsa di vRealize Orchestrator.

Quando un utente del catalogo dei servizi richiede questo tipo di elementi del catalogo, il workflow esegue il provisioning dell'elemento e l'elemento distribuito viene archiviato nella scheda **Distribuzioni**. È possibile definire operazioni successive al provisioning per questo tipo di risorse sottoposte a provisioning. È inoltre possibile rendere scalabili i blueprint aggiungendo o rimuovendo l'istanza secondo necessità.

Blueprint non di provisioning

Un blueprint non di provisioning esegue un workflow di vRealize Orchestrator per eseguire un'attività che non richiede l'API per apportare modifiche a un endpoint. Ad esempio, il workflow eseguito che genera un report e lo invia via email o a un sistema di comunicazione di destinazione.

Quando un utente del catalogo dei servizi richiede questo tipo di elementi del catalogo, il workflow viene eseguito per eseguire l'attività di script ma l'elemento non viene aggiunto alla

scheda **Distribuzioni**. Non è possibile eseguire operazioni successive al provisioning su questo tipo di blueprint. È possibile utilizzare blueprint non di provisioning come workflow di supporto nei blueprint scalabili. Ad esempio, è possibile creare un blueprint per aggiornare un bilanciamento del carico con elevata disponibilità.

Blueprint composito

Un blueprint creato utilizzando la tela di progettazione. Il blueprint composito utilizza uno o più componenti. Ad esempio, un componente di macchina, un componente software o un componente di XaaS. Quando viene aggiunto a un servizio, viene elencato come distribuzione. Quando aggiunto a un permesso per renderlo disponibile agli utenti del catalogo dei servizi, viene elencato come blueprint composito. Un blueprint composito può disporre di un solo componente di blueprint oppure può includere un'intera applicazione con più macchine, applicazioni software e reti.

Azione risorsa

Un workflow che è possibile eseguire su un blueprint di provisioning distribuito. Il blueprint distribuito può essere un blueprint di XaaS o un componente di blueprint, oppure può essere un tipo di macchina mappato a un tipo di risorsa di vRealize Orchestrator.

Considerazioni sulla progettazione dei blueprintXaaS

Prima di creare un blueprint di XaaS, è necessario comprendere lo scopo del blueprint affinché sia possibile crearne uno che esegua correttamente il provisioning delle risorse.

È possibile creare e utilizzare blueprint di XaaS come componente di blueprint nella tela di progettazione o come blueprint autonomo. Il blueprint può essere un blueprint di provisioning o un blueprint non di provisioning.

Tabella 3-53. Tipi e risultati di blueprintXaaS

Tipo di blueprint XaaS	È necessaria una risorsa personalizzata?	Il blueprint è scalabile in una distribuzione?	È possibile eseguire un'azione di risorse sul blueprint distribuito?
Componente del blueprint che esegue il provisioning di risorse	Sì	Sì. Se è configurato per la scalabilità, scalerà quando la distribuzione viene scalata.	Sì. Scala quando la distribuzione viene scalata ed è possibile eseguire altre azioni di risorse sul componente distribuito. Il componente del blueprint viene visualizzato nella scheda Distribuzioni.
Componente del blueprint che esegue un workflow ma non esegue il provisioning di risorse	No. Il blueprint utilizza la configurazione server di vRealize Orchestrator ma non richiede una risorsa personalizzata di XaaS.	No. Non esegue il provisioning di risorse ma può essere eseguito come parte di un'operazione di scalabilità. Ad esempio, aggiornare un bilanciamento del carico con la nuova configurazione in base all'operazione di scalabilità.	No. Non è possibile eseguire un'azione di risorse su un componente non di provisioning.
Blueprint autonomo che esegue il provisioning di risorse.	Sì	No. È necessario creare azioni di risorse per aggiungere o distruggere istanze.	Sì. È possibile eseguire azioni di risorse sulla risorsa distribuita, incluse eventuali azioni create per supportare la scalabilità. Il blueprint viene visualizzato nella scheda Distribuzioni.
Il blueprint autonomo che esegue un workflow ma non esegue il provisioning di risorse	No. Il blueprint utilizza la configurazione server di vRealize Orchestrator ma non richiede una risorsa personalizzata di XaaS.	No. Non esegue il provisioning di risorse ma può essere eseguito come parte di un'azione di risorse.	No. Non è possibile eseguire un'azione di risorse su un componente non di provisioning.

Aggiunta di una risorsa XaaS personalizzata.

La creazione di una risorsa personalizzata consente di definire l'elemento XaaS da fornire in provisioning. Prima di poter creare un blueprint o un'azione di XaaS è necessario disporre di una risorsa personalizzata che sia compatibile con il tipo di oggetto del blueprint o del workflow dell'azione.

Quando si crea una risorsa personalizzata, si mappa come una risorsa un tipo di oggetto esposto tramite l'API di plug-in di vRealize Orchestrator. La risorsa personalizzata definisce il parametro di output di un blueprint di XaaS per il provisioning e un parametro di input per un'azione risorsa.

Se un blueprint o un workflow di un'azione risorsa non sono utilizzati per il provisioning di una risorsa o non vengono eseguiti su un blueprint distribuito, non è necessario creare una risorsa personalizzata. Ad esempio, una risorsa personalizzata non è necessaria se il workflow aggiorna un valore in un database o invia un messaggio email dopo una operazione di provisioning.

Durante la creazione di una risorsa personalizzata è possibile specificare i campi del modulo di sola lettura presente nei dettagli di un elemento di cui si è eseguito il provisioning. Vedere [Progettazione di un modulo risorsa personalizzata](#).

Prerequisiti

- Accedere a vRealize Automation come **architetto di XaaS**.
- Utilizzare le informazioni sulle opzioni dettagliate per configurare la risorsa personalizzata. Vedere [Opzioni della procedura guidata delle risorse personalizzate di XaaS](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Risorse personalizzate**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Configurare i valori presenti nella scheda **Tipo di risorsa**.
 - a Immettere o selezionare il tipo di oggetto di vRealize Orchestrator nella casella di testo **Tipo di orchestrator**.
Ad esempio, immettere **v** per visualizzare i tipi che contengono la lettera v. Per visualizzare tutti i tipi, immettere uno spazio.
 - b Immettere un nome e, facoltativamente, una descrizione.
 - c Specificare la versione.
Il formato supportato ha l'estensione major.minor.micro-revisione.
 - d Fare clic su **Avanti**.
- 4 Modificare il contenuto della scheda **Modulo dettagli** secondo le necessità.
È possibile modificare il modulo della risorsa personalizzata eliminando, modificando e ridisponendo gli elementi. È anche possibile aggiungere un modulo e pagine del modulo, nonché trascinare elementi nel nuovo modulo o in una pagina del modulo.
- 5 Fare clic su **Fine**.

Risultati

È stata creata una risorsa personalizzata che verrà elencata nella pagina Risorse personalizzate. La risorsa personalizzata può essere utilizzata come base per la creazione di blueprint o azioni di XaaS.

Operazioni successive

- Creare un blueprint di XaaS. Vedere [Aggiunta di un blueprint XaaS](#).

- Creare un'azione risorsa di XaaS. Vedere [Creazione di un'azione risorsa di XaaS](#).

Opzioni della procedura guidata delle risorse personalizzate di XaaS

È possibile utilizzare queste opzioni di risorse personalizzate per creare o modificare una risorsa personalizzata affinché sia possibile eseguire i workflow di blueprint e azioni di risorse di XaaS che eseguono il provisioning di risorse o modificano le risorse sottoposte a provisioning.

È possibile creare una sola risorsa personalizzata per un tipo di oggetto. È possibile utilizzare la risorsa personalizzata per più blueprint e azioni di risorse.

Per creare un'azione di risorsa personalizzata, selezionare **Progettazione > XaaS > Risorse personalizzate**

Tipo di risorsa

L'elenco di possibili tipi di oggetti visualizzato nella scheda **Tipo di risorsa** basati sui plug-in installati nell'istanza configurata di vRealize Orchestrator. vRealize Automation raccoglie i valori dall'istanza configurata di vRealize Orchestrator.

Tabella 3-54. Opzioni tipo di risorsa

Opzione	Descrizione
Tipo di orchestrator	<p>Inserire o selezionare il tipo che supporta il workflow utilizzato per il provisioning.</p> <p>Il tipo è composto dal nome del plug-in così come visualizzati nell'API di script, ad esempio, VC sta per vCenter, e il tipo di oggetto potrebbe essere VirtualMachine. In questo esempio, l'API utilizza il valore VC:VirtualMachine.</p> <p>Questo tipo può essere il parametro di output del workflow del blueprint o il parametro di input del workflow dell'azione di risorse.</p>
Nome	Assegnare un nome descrittivo alla risorsa personalizzata affinché possa essere identificata durante la creazione di blueprint o azioni di risorse di XaaS.
Descrizione	Immettere una descrizione dettagliata.
Versione	Il formato supportato ha l'estensione major.minor.micro-revision.

Modulo dettagli

I campi di questo modulo vengono visualizzati come valori di sola lettura quando gli utenti del catalogo dei servizi eseguono il provisioning di un elemento che utilizza questa risorsa personalizzata. È possibile modificare i campi esistenti e aggiungere nuovi campi definiti esternamente.

Per ulteriori informazioni sulla configurazione dei moduli, vedere [Progettazione di un modulo risorsa personalizzata](#).

Dove utilizzato

Poiché è possibile creare una sola risorsa personalizzata per tipo di oggetto, questa pagina della procedura guidata può essere utilizzata per comprendere le modalità di utilizzo della risorsa personalizzata.

Questa scheda è disponibile per le risorse personalizzate salvate, non quando si crea la risorsa.

Tabella 3-55. Dove vengono utilizzate le opzioni

Opzione	Descrizione
Blueprint XaaS	<p>Un elenco dei blueprint configurati per l'utilizzo di questa risorsa personalizzata.</p> <p>In questa pagina, è possibile eseguire le seguenti azioni:</p> <ul style="list-style-type: none"> ■ Modifica. Apre il blueprint affinché sia possibile visualizzare come viene configurato o per modificarlo. ■ Pubblica/Annulla pubblicazione. Modifica lo stato del blueprint rendendolo disponibile per l'utilizzo in un blueprint composito o per aggiungerlo a un servizio. Se si annulla la pubblicazione di un blueprint, è possibile renderlo potenzialmente non disponibile per l'utilizzo in blueprint composti, per aggiungerlo a un servizio o renderlo non disponibile nel catalogo dei servizi. ■ Elimina. Rimuove il blueprint dal sistema.
Azioni di risorse	<p>Un elenco di azioni di risorse configurate per l'utilizzo di questa risorsa personalizzata.</p> <p>In questa pagina, è possibile eseguire le seguenti azioni:</p> <ul style="list-style-type: none"> ■ Modifica. Apre l'azione di risorse affinché sia possibile visualizzare come viene configurata o per modificarla. ■ Pubblica/Annulla pubblicazione. Modifica lo stato dell'azione di risorse rendendola disponibile in un permesso. Se si annulla la pubblicazione di un'azione di risorse, è possibile renderla potenzialmente non disponibile per aggiungerla a un servizio o renderla non disponibile per l'esecuzione in blueprint distribuiti. ■ Elimina. Rimuove l'azione di risorse dal sistema.

Creazione di un blueprint XaaS

Esistono blueprint XaaS di provisioning o non di provisioning. Alcuni dei workflow di provisioning forniti in vRealize Orchestrator includono la creazione di macchine virtuali, l'aggiunta di utenti ad Active Directory o l'esecuzione di snapshot delle macchine virtuali. Alcuni dei workflow non di provisioning che è possibile creare includono l'aggiornamento del bilanciamento del carico o la creazione di un report e il relativo invio ai destinatari.

È possibile creare blueprint XaaS basati sui workflow forniti in vRealize Orchestrator oppure utilizzare i workflow creati per raggiungere obiettivi specifici del proprio ambiente.

Procedura

1 Aggiunta di un blueprint XaaS

Un blueprint XaaS è una specifica per l'esecuzione di un workflow di vRealize Orchestrator che comporta una modifica a un sistema di destinazione nell'ambiente in uso. Il blueprint include il workflow ma può anche specificare i parametri di input, i moduli di invio e di sola lettura, la sequenza di azioni e l'operazione di provisioning o di non provisioning.

2 Aggiunta di un blueprint XaaS a un blueprint composito

La procedura di aggiunta di un blueprint XaaS come componente di un blueprint composito è molto simile a quella eseguita per aggiungere altri componenti blueprint nella tela di progettazione.

Aggiunta di un blueprint XaaS

Un blueprint XaaS è una specifica per l'esecuzione di un workflow di vRealize Orchestrator che comporta una modifica a un sistema di destinazione nell'ambiente in uso. Il blueprint include il workflow ma può anche specificare i parametri di input, i moduli di invio e di sola lettura, la sequenza di azioni e l'operazione di provisioning o di non provisioning.

È possibile creare blueprint XaaS da utilizzare in una o più delle modalità seguenti:

- Creare un blueprint di componente XaaS. Un blueprint di componente è un blueprint di provisioning o di non provisioning che è possibile utilizzare nella tela di progettazione dei blueprint come parte di un blueprint composito. Se viene utilizzato come componente, è necessario configurare le opzioni del ciclo di vita del componente che supportano operazioni di scalabilità verticale e orizzontale sul blueprint composito distribuito.

Questo tipo di blueprint può anche essere pubblicato come blueprint autonomo.

- Creare un blueprint XaaS autonomo. Un blueprint autonomo è un blueprint di provisioning o di non provisioning pubblicato e autorizzato direttamente per il catalogo dei servizi.

Per un esempio di come creare gli utenti di Active Directory utilizzando un blueprint XaaS, vedere [Creazione di un blueprint di XaaS e di un'azione per la creazione e la modifica di un utente](#).

Prerequisiti

- Accedere a vRealize Automation come **architetto di XaaS**.
- Se il blueprint deve eseguire il provisioning delle risorse, creare una risorsa personalizzata corrispondente al parametro di output del blueprint del servizio. Vedere [Aggiunta di una risorsa XaaS personalizzata](#). Se non utilizza l'API di un plug-in di vRealize Orchestrator, non è necessario configurare una risorsa personalizzata.
- La creazione di un blueprint XaaS comporta la pubblicazione di un workflow di vRealize Orchestrator come potenziale blueprint di componente o elemento di catalogo. Il blueprint include un modulo che è possibile modificare. Vedere [Progettazione di un modulo blueprint di XaaS](#).

- Per configurare il blueprint, fare riferimento alle informazioni dettagliate sulle opzioni. Vedere [Opzioni di creazione di un nuovo blueprint o di modifica di un blueprint di XaaS](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Nella scheda **Workflow**, selezionare il workflow che viene eseguito quando il blueprint esegue il provisioning della risorsa.

Questa scheda non è disponibile se si sta modificando un blueprint.
 - a Navigare all'interno della libreria di workflow di vRealize Orchestrator e selezionare un workflow correlato alla risorsa personalizzata.
 - b Esaminare i parametri di input e di output per assicurarsi di poter fornire i valori corretti successivamente.
 - c Fare clic su **Avanti**.
- 4 Nella scheda **Generale**, configurare le opzioni e fare clic su **Avanti**.
 - a Nella casella di testo **Nome**, immettere un nome con cui distinguere questo blueprint dagli altri blueprint simili.
 - b Se non si desidera utilizzare questo blueprint come componente in un blueprint composito, deselezionare la casella di controllo **Rendi disponibile come componente nella tela di progettazione**.
- 5 Nella scheda **Modulo blueprint**, modificare il modulo nel modo appropriato e fare clic su **Avanti**.
- 6 Nella pagina **Risorsa di provisioning**, selezionare un valore e fare clic su **Avanti**.

Opzione	Descrizione
Nessun provisioning	Se il workflow non esegue il provisioning delle risorse, è possibile selezionare questa opzione o lasciare vuoto il campo.
<Risorsa personalizzata creata in precedenza>	Selezionare la risorsa personalizzata che supporta questo workflow di provisioning.

- 7 Nella scheda **Ciclo di vita del componente**, definire il comportamento di questo blueprint durante le operazioni di scalabilità verticale, scalabilità orizzontale ed eliminazione.

Questi workflow vengono eseguiti in un blueprint composito distribuito in cui il blueprint è un componente. La disponibilità delle diverse opzioni dipende dal blueprint. Non tutti i workflow dei blueprint supportano o richiedono tutte le opzioni.
- 8 Fare clic su **Fine**.
- 9 Selezionare la riga relativa al blueprint e fare clic su **Pubblica**.

Risultati

La creazione e la pubblicazione di un blueprint XaaS è terminata.

Operazioni successive

- Per inserire il blueprint direttamente nel catalogo dei servizi come blueprint autonomo, aggiungere un servizio e procedere quindi all'aggiunta del blueprint. Vedere [Aggiunta di un servizio](#).
- Per utilizzare il blueprint come componente in un blueprint composito, vedere [Aggiunta di un blueprint XaaS a un blueprint composito](#).

Opzioni di creazione di un nuovo blueprint o di modifica di un blueprint di XaaS

È possibile utilizzare queste opzioni per creare un blueprint XaaS che esegue un workflow di vRealize Orchestrator durante la distribuzione del blueprint. Il workflow modifica un sistema di destinazione nell'ambiente.

Per ulteriori informazioni sulla procedura da seguire per creare il blueprint, vedere [Aggiunta di un blueprint XaaS](#).

Per utilizzare questa procedura guidata, selezionare **Progettazione > XaaS > Blueprint XaaS**.

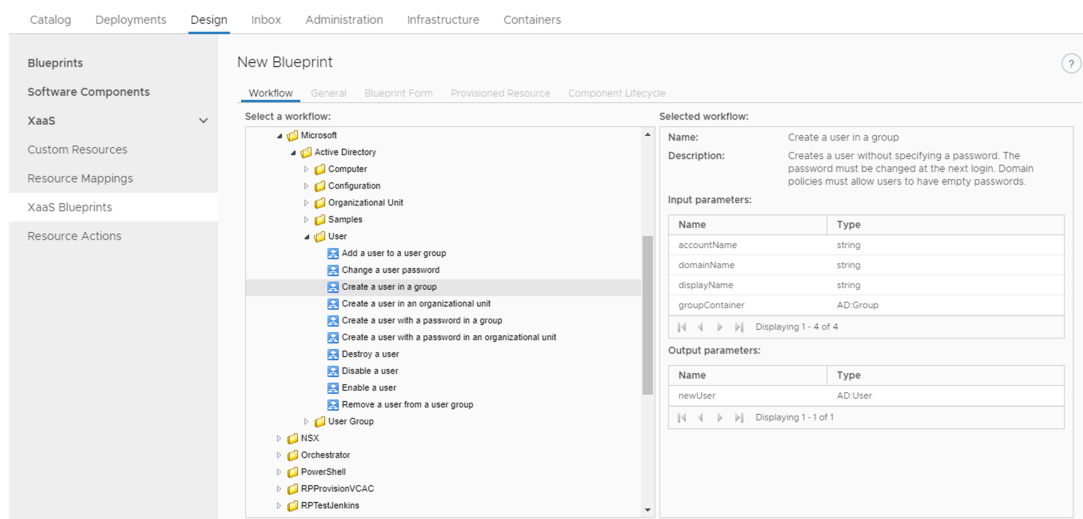
Scheda Workflow

Selezionare il workflow eseguito quando il blueprint esegue il provisioning della risorsa.

Questa scheda non è disponibile se si sta modificando un blueprint.

Nella seguente figura, la struttura del workflow si trova nella parte sinistra, mentre i parametri sono sulla destra.

Figura 3-4. Scheda Workflow nella procedura guidata Blueprint di XaaS



Rivedere i parametri di input e di output per assicurarsi che l'utente corrente o gli utenti del catalogo dei servizi possano specificare i valori corretti nei seguenti casi:

- Se si personalizza il modulo del blueprint in questa procedura guidata o nella tela di progettazione del blueprint.
- Se si lasciano tutti i parametri di input vuoti, gli utenti del catalogo dei servizi possono impostare i valori.

Scheda Generale

Configurare i metadati del blueprint e il relativo comportamento.

Tabella 3-56. Opzioni della scheda Generale

Opzione	Descrizione
Nome	<p>Il nome del blueprint così come si desidera venga visualizzato nelle seguenti posizioni:</p> <ul style="list-style-type: none"> ■ Tela di progettazione. Se si seleziona Rendi disponibile come componente nella tela di progettazione, tale valore è il nome visualizzato nell'elenco delle categorie. ■ Servizi. Se il blueprint viene utilizzato come blueprint autonomo, tale valore è il nome visualizzato quando si aggiungono elementi del catalogo al servizio. ■ Permessi. Se il blueprint viene autorizzato come elemento individuale, tale valore è il nome visualizzato nell'elenco Aggiungi elementi.
Descrizione	Fornire una descrizione dettagliata che consenta di differenziare l'elemento da altri elementi simili.
Nascondi pagina delle informazioni di richiesta del catalogo	Selezionare la casella di controllo se non si desidera che gli utenti del catalogo dei servizi forniscano una descrizione e un motivo quando richiedono l'elemento. La casella di controllo è selezionata per impostazione predefinita.
Versione	Il formato supportato ha l'estensione major.minor.micro-revisione.
Rendi disponibile come componente nella tela di progettazione	<p>Se si prevede di utilizzare il blueprint come componente in un blueprint della tela di progettazione, selezionare questa opzione.</p> <p>Quando viene pubblicato, il blueprint è disponibile nella categoria selezionata durante la configurazione della risorsa personalizzata.</p> <p>Se non si seleziona questa opzione, il blueprint non viene visualizzato nella tela di progettazione. Tuttavia, è sempre possibile aggiungerlo a un servizio e autorizzare gli utenti a distribuirlo come blueprint autonomo.</p>

Scheda Modulo blueprint

I campi visualizzati in questa pagina della procedura guidata sono i parametri di input del workflow. È possibile apportare una o più delle seguenti modifiche:

- Aggiungi campi al modulo.
- Modificare i campi esistenti eliminando o riordinando i campi.
- Specificare i valori predefiniti come parametri di input.

Le eventuali modifiche influiscono sul modulo presentato a:

- L'architetto di applicazioni che lavora nella tela di progettazione quando questo blueprint di XaaS viene utilizzato come componente del blueprint.
- L'utente del catalogo dei servizi se questo blueprint è pubblicato come blueprint autonomo.

Per ulteriori informazioni sulla configurazione dei moduli, vedere [Progettazione di un modulo blueprint di XaaS](#).

Risorsa di provisioning

La risorsa di provisioning collega il blueprint a una risorsa personalizzata pertinente di XaaS configurata nella pagina Risorsa personalizzata in **Progettazione > XaaS > Risorsa personalizzata**.

Tabella 3-57. Opzioni Risorsa di provisioning

Opzione	Descrizione
Risorsa personalizzata creata in precedenza	<p>Selezionare la risorsa personalizzata che definisce il tipo di risorsa di vRealize Orchestrator richiesto per l'esecuzione del blueprint sottoposto a provisioning.</p> <p>Un blueprint di provisioning esegue un workflow di vRealize Orchestrator per eseguire il provisioning di risorse sull'endpoint di destinazione utilizzando l'API del plug-in di vRealize Orchestrator per l'endpoint. Ad esempio, aggiungere NIC virtuali a un dispositivo di rete in vSphere.</p> <p>È possibile definire operazioni successive al provisioning per questo tipo di risorse sottoposte a provisioning. È inoltre possibile rendere scalabile il blueprint aggiungendo o rimuovendo le istanze secondo necessità.</p> <p>Risultati</p> <ul style="list-style-type: none"> ■ Il blueprint è idoneo per la scalabilità. ■ Il blueprint viene visualizzato nella tela di progettazione nella categoria specificata per la risorsa personalizzata selezionata. ■ Il blueprint viene visualizzato nella scheda Distribuzioni quando si distribuisce un blueprint che lo include, ed è possibile eseguire qualsiasi azione sull'elemento dopo la distribuzione.
Nessun provisioning	<p>Un blueprint non di provisioning esegue un workflow di vRealize Orchestrator per eseguire un'attività che non richiede l'API per apportare modifiche a un endpoint. Ad esempio, generare un report e inviarlo via email o pubblicarlo in un sistema di comunicazione di destinazione.</p> <p>Risultati</p> <ul style="list-style-type: none"> ■ Il blueprint non è idoneo per la scalabilità. È possibile utilizzare blueprint non di provisioning come workflow di supporto nei blueprint scalabili. Ad esempio, è possibile creare un blueprint per aggiornare un bilanciamento del carico con elevata disponibilità. ■ Il blueprint viene visualizzato nella categoria XaaS della tela di progettazione. ■ Il blueprint non viene visualizzato nella scheda Distribuzioni quando si distribuisce un blueprint che lo include, e non è possibile eseguire azioni sull'elemento dopo la distribuzione.

Scheda Ciclo di vita del componente

La scheda Ciclo di vita del componente è disponibile se è stata selezionata l'opzione **Rendi disponibile come componente nella tela di progettazione** nella scheda **Generale**.

È possibile utilizzare tali opzioni per definire il comportamento del blueprint nelle fasi successive alla distribuzione durante le operazioni di scalabilità verticale e scalabilità orizzontale quando viene utilizzato come componente in un blueprint composito.

La disponibilità delle diverse opzioni varia in base al blueprint. Non tutti i workflow dei blueprint supportano o richiedono tutte le opzioni. Poiché XaaS potrebbe essere utilizzato in un blueprint composito, si consiglia di configurare l'aggiornamento ed eliminare le opzioni, nonché allocare, allocarle e deallocarle, se sono disponibili per il blueprint, affinché la scalabilità del blueprint venga eseguita correttamente.

Tabella 3-58. Opzioni Ciclo di vita del componente

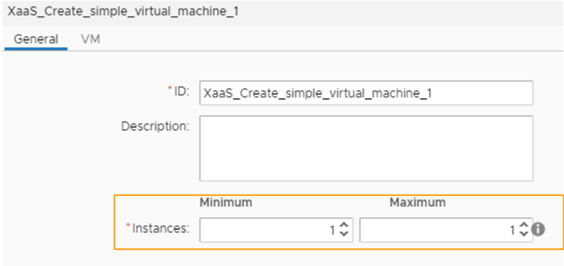
Opzione	Descrizione
Scalabile	<p>Selezionare l'opzione per consentire all'utente del catalogo dei servizi di modificare il numero di istanze di questo componente del blueprint se è stato distribuito come parte di un'operazione di scalabilità verticale oppure orizzontale.</p> <p>Questa opzione è disponibile se è stata selezionata una risorsa personalizzata nella scheda Risorsa di provisioning. Non è disponibile se è stata selezionata l'opzione Nessun provisioning.</p> <p>Se si rende scalabile il blueprint, l'opzione Istanze viene aggiunta alla scheda Generale nella tela di progettazione. Vedere l'esempio riportato di seguito. Se non si seleziona Scalabile, l'opzione Istanze non è disponibile nella tela di progettazione.</p> 
Workflow di provisioning	<p>Il workflow eseguito durante un'operazione di provisioning o di scalabilità orizzontale. Questo workflow è stato selezionato quando il blueprint è stato creato, e non è possibile modificare il valore.</p>

Tabella 3-58. Opzioni Ciclo di vita del componente (continua)

Opzione	Descrizione
Workflow allocazione	<p>Selezionare il workflow eseguito prima di qualsiasi operazione iniziale di provisioning o di scalabilità orizzontale.</p> <p>Questo workflow di ciclo di vita è disponibile per la allocazioni Azure. Se si crea un workflow di allocazione per un'operazione di scalabilità, deve includere i seguenti valori:</p> <ul style="list-style-type: none"> ■ Parametri di input <ul style="list-style-type: none"> ■ Il nome del parametro è <code>requestData</code> e il tipo di parametro è <code>Properties</code>. ■ Il nome del parametro è <code>subtenant</code> e il tipo di parametro è <code>Properties</code>. ■ <code>reservations</code> e il tipo di parametro è <code>Arrays/Properties</code>. ■ Parametro di output <ul style="list-style-type: none"> ■ Deve includere un parametro in cui il tipo di parametro è <code>Properties</code>
Aggiorna workflow	<p>Selezionare il workflow eseguito durante le operazioni di aggiornamento, incluse quelle di scalabilità verticale oppure orizzontale in cui il componente non è scalabile ma può essere aggiornato.</p> <p>Ad esempio, un bilanciamento del carico viene aggiornato con la nuova configurazione creata con l'operazione di scalabilità verticale o scalabilità orizzontale per qualsiasi componente nel blueprint composito.</p> <p>Il workflow di aggiornamento dovrebbe essere applicato a un componente associato al componente scalato, ma che a sua volta non è scalabile. Questo workflow di aggiornamento può modificare il componente non scalabile in base a un'operazione di aggiornamento.</p> <p>Se si crea un workflow di aggiornamento per un'operazione di scalabilità, deve includere i seguenti valori:</p> <ul style="list-style-type: none"> ■ Parametri di input. <ul style="list-style-type: none"> ■ Deve includere un parametro, indipendentemente dal nome del parametro, che corrisponda al tipo di parametro di output del workflow di provisioning. ■ Il nome del parametro è <code>data</code> e il tipo di parametro è <code>Properties</code>.

Tabella 3-58. Opzioni Ciclo di vita del componente (continua)

Opzione	Descrizione
Elimina workflow	<p>Selezionare il workflow eseguito durante un'operazione di scalabilità verticale o eliminazione.</p> <p>Se si crea un workflow di eliminazione per un'operazione di scalabilità, deve includere il seguente valore:</p> <ul style="list-style-type: none"> ■ Parametro di input. <ul style="list-style-type: none"> ■ Deve includere un parametro, indipendentemente dal nome del parametro, che corrisponda al tipo di parametro di output del workflow di provisioning. <p>Ad esempio, se il workflow di provisioning per la creazione di una macchina virtuale semplice include il parametro di output VC:VirtualMachine, il workflow di eliminazione deve includere un parametro di input in cui il tipo è VC:VirtualMachine.</p>
Workflow deallocazione	<p>Selezionare il workflow eseguito dopo qualsiasi operazione di eliminazione o di scalabilità verticale. Se la deallocazione non riesce durante l'operazione, il workflow di eliminazione viene eseguito comunque come previsto.</p> <p>La deallocazione è il processo finale in un'operazione di scalabilità verticale o eliminazione di un blueprint composito. Viene eseguita dopo l'operazione di eliminazione, rilasciando le risorse.</p> <p>Questo workflow di ciclo di vita è disponibile per la allocazioni Azure. Se si crea un workflow di deallocazione per un'operazione di scalabilità, deve includere il seguente valore:</p> <ul style="list-style-type: none"> ■ Parametro di input. <ul style="list-style-type: none"> ■ Il nome del parametro è <i>data</i> e il tipo di parametro è <i>Properties</i>.
Categoria	<p>Per specificare la posizione in cui viene visualizzato il blueprint di XaaS nella tela di progettazione, selezionare un valore nel menu a discesa Categoria tela di progettazione.</p> <p>Se non si seleziona una categoria, il blueprint viene aggiunto alla categoria XaaS quando pubblicato.</p>

Aggiunta di un blueprint XaaS a un blueprint composito

La procedura di aggiunta di un blueprint XaaS come componente di un blueprint composito è molto simile a quella eseguita per aggiungere altri componenti blueprint nella tela di progettazione.

Utilizzare questo metodo per aggiungere un servizio XaaS a un blueprint composito. Tale blueprint può essere un componente blueprint specifico oppure uno dei vari componenti che compongono un blueprint di applicazione.

Se il blueprint XaaS è l'unico elemento che si desidera fornire agli utenti, è possibile aggiungerlo a un servizio e permettere l'accesso agli utenti senza aggiungerlo a un blueprint composito.

Se si esegue un'operazione di scalabilità verticale o orizzontale su un blueprint di applicazione distribuito, il blueprint XaaS viene scalato in base alla modalità di configurazione delle opzioni del ciclo di vita del blueprint.

Prerequisiti

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Creare e pubblicare un blueprint XaaS. Vedere [Creazione di un blueprint XaaS](#). Al momento della creazione del blueprint, è stata specificata la categoria associata al blueprint nella tela di progettazione.
- Esaminare la modalità di personalizzazione dei moduli di blueprint XaaS nel blueprint composito. Vedere [Progettazione di moduli per blueprint e azioni di XaaS](#).

Procedura

1 Scegliere **Progettazione > Blueprint**.

2 Selezionare il nome del blueprint a cui si sta aggiungendo lo XaaS.

Viene visualizzata la tela di progettazione. Contiene i blueprint del componente dell'applicazione corrente e altri componenti.

3 Individuare il blueprint nell'elenco Categorie.

4 Trascinare il blueprint nella tela.

5 Configurare i valori predefiniti nelle schede Generale e Crea.

Questi valori predefiniti vengono visualizzati nel modulo del catalogo dei servizi quando un utente richiede l'elemento.

6 Fare clic su **Fine**.

7 Selezionare il blueprint e fare clic su **Pubblica**.

Risultati

Il blueprint XaaS fa ora parte del blueprint composito.

Operazioni successive

Aggiungere il blueprint composito a un servizio. Vedere [Gestione del catalogo dei servizi](#).

Creazione di un'azione risorsa di XaaS

È possibile creare un'azione risorsa in modo da poter gestire gli elementi con provisioning utilizzando i workflow di vRealize Orchestrator.

Prerequisiti

- Accedere a vRealize Automation come **architetto di XaaS**.
- Assicurarsi di disporre di una risorsa personalizzata che supporti l'azione. Vedere [Aggiunta di una risorsa XaaS personalizzata..](#)

- Se si stanno creando azioni da eseguire su elementi non sottoposti a provisioning come elementi di catalogo XaaS, assicurarsi di aver mappato le risorse di destinazione. Vedere [Mappatura di altre risorse per l'utilizzo delle azioni risorsa XaaS](#).

Procedura

1 Creazione di un'azione risorsa

Un'azione risorsa è un workflow di XaaS che gli utenti del catalogo dei servizi possono eseguire sugli elementi di catalogo con provisioning eseguito. Gli architetti di XaaS possono creare azioni risorsa per definire le operazioni che i clienti possono eseguire sugli elementi con provisioning eseguito.

2 Pubblicazione di un'azione risorsa

L'azione risorsa appena creata è in uno stato di bozza ed è necessario pubblicarla.

3 Assegnazione di un'icona a un'azione risorsa XaaS

Dopo aver creato e pubblicato un'azione risorsa, è possibile modificarla per assegnarle un'icona.

Creazione di un'azione risorsa

Un'azione risorsa è un workflow di XaaS che gli utenti del catalogo dei servizi possono eseguire sugli elementi di catalogo con provisioning eseguito. Gli architetti di XaaS possono creare azioni risorsa per definire le operazioni che i clienti possono eseguire sugli elementi con provisioning eseguito.

Creando un'azione risorsa si associa un workflow di vRealize Orchestrator come operazione di post-provisioning. Durante questa procedura è possibile modificare l'invio predefinito e i moduli di sola lettura. Vedere [Progettazione di un modulo azione risorsa](#).

Prerequisiti

- Accedere a vRealize Automation come **architetto di XaaS**.
- Creazione di una risorsa personalizzata corrispondente al parametro di input dell'azione risorsa.

Procedura

1 Selezionare **Progettazione > XaaS > Azioni risorsa**.

2 Fare clic sull'icona **Nuovo** (+).

3 Navigare all'interno della libreria di workflow di vRealize Orchestrator e selezionare un workflow correlato alla risorsa personalizzata.

Si possono vedere il nome e la descrizione del workflow selezionato, nonché i parametri di input e output come sono definiti in vRealize Orchestrator.

4 Fare clic su **Avanti**.

5 Selezionare la risorsa personalizzata precedentemente creata dal menu a discesa **Tipo di risorsa**.

- 6 Selezionare il parametro di input per l'azione risorsa dal menu a discesa **Parametro di input**.
- 7 Fare clic su **Avanti**.
- 8 Immettere un nome e, facoltativamente, una descrizione.

Le caselle di testo **Nome** e **Descrizione** vengono compilate con il nome e la descrizione del workflow così come definiti in vRealize Orchestrator.

- 9 (Facoltativo) Se non si desidera richiedere ai clienti di immettere una descrizione e un motivo della richiesta dell'azione risorsa, selezionare la casella di controllo **Nascondi pagina delle informazioni di richiesta del catalogo**.
- 10 Specificare la versione.
Il formato supportato ha l'estensione major.minor.micro-revisione.
- 11 (Facoltativo) Selezionare il tipo di azione.

Opzione	Descrizione
Eliminazione	Il parametro di input del workflow dell'azione risorsa viene eliminato e l'elemento rimosso dalla scheda Distribuzioni . Ad esempio, l'azione risorsa elimina una macchina di cui è stato eseguito il provisioning.
Provisioning	L'azione risorsa esegue il provisioning. Ad esempio, l'azione risorsa ha l'obiettivo di copiare un elemento di catalogo. Selezionare un parametro di output dal menu a discesa. È possibile selezionare una risorsa personalizzata precedentemente creata in modo da aggiungere gli elementi forniti in provisioning alla scheda Distribuzioni quando i clienti richiedono l'azione risorsa. Se è presente solo l'opzione Nessun provisioning , l'azione risorsa non è destinata al provisioning oppure non è stata creata una risorsa personalizzata valida per il parametro di output, pertanto non si potrà procedere.
Provisioning come figlio	È possibile eseguire il provisioning di una risorsa come elemento figlio della risorsa padre. Quando si elimina una risorsa padre o si esegue la scalabilità verticale e orizzontale, è innanzitutto necessario occuparsi delle risorse figlio.

In base al workflow dell'azione, è possibile selezionare una, entrambe o nessuna opzione.

- 12 Selezionare le condizioni alle quali l'azione risorsa è disponibile agli utenti e fare clic su **Avanti**.

13 (Facoltativo) Modificare il modulo dell'azione risorsa nella scheda **Modulo**.

Il modulo dell'azione risorsa si collega alla presentazione del workflow vRealize Orchestrator. È possibile modificare il modulo eliminando, modificando e ridisponendo gli elementi. È anche possibile aggiungere un nuovo modulo e nuove pagine di modulo, nonché trascinare gli elementi necessari nel nuovo modulo o nella pagina del modulo.

Opzione	Azione
Aggiungi un modulo	Fare clic sull'icona Nuovo modulo (+) accanto al nome del modulo, fornire le informazioni richieste e fare clic su Invia .
Modifica un modulo	Fare clic sull'icona Modifica (penna) accanto al nome del modulo, apportare le modifiche necessarie e fare clic su Invia .
Rigenera la presentazione del workflow	Fare clic sull'icona Rigenera (ciclo) accanto al nome del modulo e scegliere OK .
Elimina un modulo	Fare clic sull'icona Elimina (X) accanto al nome del modulo, quindi scegliere OK nella finestra di dialogo di conferma.
Aggiungi una pagina di modulo	Fare clic sull'icona Nuova pagina (+) accanto al nome della pagina del modulo, fornire le informazioni richieste e fare clic su Invia .
Modifica una pagina di modulo	Fare clic sull'icona Modifica (penna) accanto al nome della pagina del modulo, apportare le modifiche necessarie e fare clic su Invia .
Elimina una pagina di modulo	Fare clic sull'icona Elimina (X) accanto al nome del modulo, quindi scegliere OK nella finestra di dialogo di conferma.
Aggiungi un elemento alla pagina del modulo	Trascinare un elemento dal riquadro Nuovi campi di sinistra al riquadro di destra. Quindi è possibile specificare le informazioni richieste e fare clic su Invia .
Modificare un elemento	Fare clic sull'icona Modifica (penna) accanto all'elemento da modificare, apportare le modifiche necessarie e fare clic su Invia .
Eliminare un elemento	Fare clic sull'icona Elimina (X) accanto all'elemento da eliminare, quindi scegliere OK nella finestra di dialogo di conferma.

14 Fare clic su **Fine**.**Risultati**

È stata creata un'azione risorsa, che verrà elencata nella pagina Azioni risorsa.

Operazioni successive

Pubblicare l'azione risorsa. Vedere [Pubblicazione di un'azione risorsa](#).

Pubblicazione di un'azione risorsa

L'azione risorsa appena creata è in uno stato di bozza ed è necessario pubblicarla.

Prerequisiti

Accedere a vRealize Automation come **architetto di Xaas**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Selezionare la riga dell'azione risorsa da pubblicare e fare clic su **Pubblica**.

Risultati

Anche lo stato dell'azione risorsa cambia in Pubblicato.

Operazioni successive

Assegnare un'icona all'azione risorsa. Vedere [Assegnazione di un'icona a un'azione risorsa XaaS](#). A questo punto, i manager dei gruppi di business e gli amministratori tenant possono utilizzare l'azione quando creano un permesso.

Assegnazione di un'icona a un'azione risorsa XaaS

Dopo aver creato e pubblicato un'azione risorsa, è possibile modificarla per assegnarle un'icona.

Prerequisiti

Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Azioni**.
- 2 Selezionare l'azione risorsa creata.
- 3 Fare clic su **Configura**.
- 4 Fare clic su **Sfoglia** e selezionare l'icona da aggiungere.
- 5 Fare clic su **Apri**.
- 6 Fare clic su **Aggiorna**.

Risultati

L'icona è stata assegnata all'azione risorsa. I manager dei gruppi di business e gli amministratori tenant possono utilizzare l'azione risorsa in un permesso.

Mappatura di altre risorse per l'utilizzo delle azioni risorsa XaaS

È possibile mappare elementi che non sono stati sottoposti a provisioning utilizzando XaaS in modo da poter eseguire azioni risorsa su questi elementi.

Workflow e azioni di script per la mappatura delle risorse

È possibile utilizzare le mappature delle risorse fornite per le macchine virtuali vSphere, vCloud Director o vCloud Air oppure creare azioni di script o workflow di vRealize Orchestrator personalizzati per mappare altri tipi di risorse di catalogo di vRealize Automation ai tipi di inventario di vRealize Orchestrator.

Mappatura delle risorse fornite con vRealize Automation

vRealize Automation include le mappature delle risorse per le macchine virtuali vSphere IaaS, vCloud Director IaaS e le distribuzioni.

vRealize Automation include azioni di script per la mappatura delle risorse di vRealize Orchestrator per ognuna delle mappature delle risorse di XaaS fornite. Le azioni di script per le mappature delle risorse fornite si trovano nel pacchetto `com.vmware.vcac.asd.mappings` del server vRealize Orchestrator incorporato.

Quando si crea un'azione risorsa che viene eseguita su un blueprint composito distribuito che utilizza un workflow vRealize Orchestrator con `vCACAFE:CatalogResource` come parametro di input, la mappatura della distribuzione viene applicata come tipo della risorsa di input. La mappatura della distribuzione viene applicata solo se il workflow selezionato include `vCACAFE:CatalogResource` come parametro di input. Ad esempio, se si crea un'azione per richiedere un'azione risorsa per conto di un utente, il tipo di risorsa sulla scheda Risorsa di input è Distribuzione, in quanto questo workflow utilizza `vCACAFE:CatalogResource`.

Le mappature delle risorse di IaaS vCD VM e IaaS VC VirtualMachine sono utilizzate da un'azione per mappare alla macchina virtuale vRealize Orchestrator vSphere o vCloud Director le macchine virtuali che corrispondono alla risorsa IaaS.

Sviluppo delle mappature delle risorse

A seconda della versione di vRealize Orchestrator, è possibile creare un workflow o un'azione di script di vRealize Orchestrator per mappare le risorse tra vRealize Orchestrator e vRealize Automation.

Per sviluppare la mappatura delle risorse, si utilizza un parametro di input di tipo `Properties`, che contiene una coppia chiave-valore che definisce la risorsa con provisioning e un parametro di output di un tipo di inventario di vRealize Orchestrator previsto dal plug-in di vRealize Orchestrator corrispondente. Le proprietà disponibili per la mappatura dipendono dal tipo di risorsa. Ad esempio, la proprietà `EXTERNAL_REFERENCE_ID` è un parametro chiave comune che definisce singole macchine virtuali ed è utilizzabile per eseguire la query di una risorsa di catalogo. Se si sta creando una mappatura per una risorsa che non utilizza un `EXTERNAL_REFERENCE_ID`, è possibile utilizzare una delle altre proprietà passate per le singole macchine virtuali. Ad esempio, nome, descrizione e così via.

Per ulteriori informazioni sullo sviluppo dei workflow e delle azioni di script, vedere *Sviluppare con VMware vCenter Orchestrator*.

Creazione di una mappatura di risorse

vRealize Automation fornisce le mappature di risorse per macchine vSphere, vCloud Director e vCloud Air. È possibile creare mappature di risorse aggiuntive per altri tipi di risorse del catalogo.

Prerequisiti

- Accedere a vRealize Automation come **architetto di XaaS**.

- Assicurarsi che lo script o il workflow di mappatura sia disponibile in vRealize Orchestrator. Vedere [Workflow e azioni di script per la mappatura delle risorse](#)

Procedura

- 1 Selezionare **Progettazione > XaaS > Mappature risorse**.

- 2 Fare clic sull'icona **Nuovo** (+).

- 3 Immettere un nome e, facoltativamente, una descrizione.

- 4 Specificare la versione.

Il formato supportato ha l'estensione major.minor.micro-revisione.

- 5 Immettere il tipo di risorsa del catalogo nella casella di testo **Tipo di risorsa del catalogo**.

Il tipo di risorsa del catalogo viene visualizzato nella vista dei dettagli dell'elemento di cui è stato eseguito il provisioning.

- 6 Specificare il tipo di oggetto vRealize Orchestrator nella casella di testo **Tipo di orchestrator** e premere Invio.

Questo è il parametro di output del workflow di mappatura delle risorse.

- 7 (Facoltativo) Aggiungere i criteri di destinazione per limitare la disponibilità delle azioni risorse create utilizzando questa mappatura delle risorse.

Le azioni risorse sono inoltre soggette a limitazioni in base alle approvazioni e ai permessi assegnati.

- a Selezionare **Disponibile in base alle condizioni**.
- b Selezionare il tipo di condizione.

Opzione	Descrizione
Tutti tra i seguenti	Se sono soddisfatte tutte le clausole definite, le azioni risorse create utilizzando la mappatura delle risorse in oggetto sono disponibili per l'utente.
Qualsiasi tra i seguenti	Se è soddisfatta una qualsiasi delle clausole definite, le azioni risorse create utilizzando la mappatura delle risorse in oggetto sono disponibili per l'utente.
Non i seguenti	Se la clausola definita esiste, le azioni risorse create utilizzando la mappatura delle risorse in oggetto non sono disponibili.

- c Attenersi alle istruzioni visualizzate per creare le clausole e completare la condizione.

- 8 Selezionare un workflow o un'azione script di mappatura risorse dalla libreria di vRealize Orchestrator.
- 9 Fare clic su **OK**.

Progettazione di moduli per blueprint e azioni di XaaS

XaaS include un designer modulo che è possibile utilizzare per creare moduli di invio e di dettaglio per blueprint e azioni risorsa. In base alla presentazione dei workflow, il designer modulo genera dinamicamente moduli predefiniti e campi utilizzabili per modificare i moduli predefiniti.

È possibile creare moduli interattivi che l'utente può completare, per l'invio di elementi del catalogo e azioni risorsa. Inoltre, è possibile creare moduli di sola lettura che definiscono quali informazioni sono accessibili ai consumatori, nella vista dei dati, per un elemento del catalogo o per una risorsa con provisioning.

Quando si creano risorse personalizzate di XaaS, blueprint di XaaS e azioni risorsa, i moduli vengono generati per i casi di uso comune.

Tabella 3-59. Tipi di oggetti di XaaS e moduli associati

Tipo di oggetto	Modulo predefinito	Moduli aggiuntivi
Risorsa personalizzata	Modulo dei dettagli della risorsa basato sugli attributi del tipo di inventario del plug-in vRealize Orchestrator (sola lettura).	■ Nessuno
Blueprint di XaaS	Modulo di invio della richiesta basato sulla presentazione del workflow selezionato.	■ Dettagli elementi del catalogo (sola lettura) ■ Dettagli richiesta inviata (sola lettura)
Azione risorsa	Modulo di invio dell'azione basato sulla presentazione del workflow selezionato.	■ Dettagli dell'azione inviata (sola lettura)

È possibile modificare i moduli predefiniti e progettare nuovi moduli. È possibile trascinare i campi per aggiungerli e riordinarli sul modulo. È possibile stabilire vincoli sui valori di alcuni campi, specificare valori predefiniti o fornire un testo di istruzioni per l'utente finale che sta compilando il modulo.

In considerazione delle diverse finalità, le operazioni eseguibili per progettare moduli in sola lettura sono limitate, rispetto a quelle per la progettazione dei moduli di invio.

Campi nel designer modulo

È possibile estendere la presentazione e le funzionalità del workflow aggiungendo nuovi campi definiti ai moduli di azioni risorsa e blueprint di XaaS generati in maniera predefinita.

Se nel workflow di vRealize Orchestrator viene definito un parametro di input, in vRealize Automation questo appare nel modulo generato in maniera predefinita. Se non si desidera utilizzare nel modulo i campi generati in maniera predefinita, è possibile eliminarli e trascinare nuovi campi dal riquadro. È possibile sostituire i campi generati in maniera predefinita senza interrompere le mappature del workflow utilizzando lo stesso ID del campo che si sta sostituendo.

È anche possibile aggiungere nuovi campi, diversi da quelli generati in base agli input del workflow di vRealize Orchestrator, in modo da estendere la presentazione e le funzionalità del workflow nei casi elencati di seguito.

- Aggiungere vincoli ai campi esistenti

Ad esempio, è possibile creare un nuovo menu a discesa e denominarlo **dd**. Successivamente si possono creare opzioni predefinite Oro, Argento, Bronzo e Personalizzato. Se è presente un campo predefinito, come CPU, è possibile aggiungere i seguenti vincoli a questo campo:

- Se dd è uguale a Oro, la CPU è da 2.000 MHz
- Se dd è uguale ad Argento, la CPU è da 1.000 MHz
- Se dd è uguale a Bronzo, la CPU è da 500 MHz
- Se dd è uguale a Personalizzato, il campo CPU è modificabile e il cliente può specificare un valore personalizzato

- Aggiungere definizioni di valori esterni ai campi

È possibile aggiungere la definizione di un valore esterno a un campo in modo che sia possibile eseguire azioni script di vRealize Orchestrator e fornire informazioni aggiuntive ai clienti dei moduli progettati. Ad esempio, può essere utile creare un workflow per cambiare le impostazioni del firewall di una macchina virtuale. Nella pagina delle richieste di azioni risorsa, si desidera fornire all'utente la possibilità di cambiare le impostazioni delle porte aperte, ma si desidera anche limitare le opzioni alle porte che sono aperte. È possibile aggiungere la definizione di un valore esterno a un campo elenco doppio e selezionare un'azione script di vRealize Orchestrator personalizzata che interroghi il sistema per conoscere le porte aperte. Quando il modulo della richiesta viene caricato, le azioni script vengono eseguite e le porte aperte vengono presentate come opzioni all'utente.

- Aggiungere nuovi campi gestiti nel workflow di vRealize Orchestrator come parametri globali

Ad esempio, il workflow offre un'integrazione a un sistema di terze parti e lo sviluppatore del workflow ha definito parametri di input da gestire nel caso generale, ma ha anche fornito un modo per passare campi personalizzati. Ad esempio, in una finestra di scripting vengono gestiti tutti i parametri globali che iniziano con **my3rdparty**. Quindi, se l'architetto di XaaS desidera passare valori specifici forniti dai clienti, l'architetto di XaaS può aggiungere un nuovo campo chiamato **my3rdparty_CPU**.

Tabella 3-60. Nuovi campi nel modulo dell'azione risorsa o di un blueprint di XaaS

Campo	Descrizione
Campo testo	Casella di testo a singola riga
Area testo	Casella di testo con più righe
Collegamento	Campo in cui i clienti immettono un URL. È possibile utilizzare http, https, ftp, mailto o /. Non utilizzare file://.
Email	Campo in cui i clienti immettono un indirizzo di email

Tabella 3-60. Nuovi campi nel modulo dell'azione risorsa o di un blueprint di XaaS (continua)

Campo	Descrizione
Campo password	Campo in cui i clienti immettono una password
Campo numero intero	Casella di testo in cui i clienti immettono un valore intero È possibile rendere questo campo un cursore con un valore minimo e un valore massimo, nonché come incremento.
Campo decimale	Casella di testo in cui i clienti immettono un valore decimale È possibile rendere questo campo un cursore con un valore minimo e un valore massimo, nonché come incremento.
Data e ora	Caselle di testo in cui i clienti specificano una data (selezionandola da un calendario) e possono anche selezionare l'orario (utilizzando le frecce su e giù)
Elenco doppio	Generatore di elenchi in cui i clienti spostano un set di valori predefinito tra due elenchi, il primo elenco contiene tutte le opzioni deselectionate e il secondo elenco contiene le scelte dell'utente.
Casella di controllo	Casella di controllo
Sì/No	Menu a discesa per la selezione di Sì o No
Menu a discesa	Menu a discesa
Elenco	Elenco
Elenco caselle di controllo	Elenco caselle di controllo
Gruppo pulsanti di opzione	Gruppo di pulsanti di opzione
Cerca	Casella di testo di ricerca con completamento automatico della query e dove i clienti possono selezionare un oggetto
Albero	Albero utilizzato dai clienti per individuare e selezionare gli oggetti disponibili
Mappa	Tabella di mappature utilizzata dai clienti per definire coppie chiave-valore per le proprietà

È possibile utilizzare anche il campo **Intestazione sezione** per dividere le pagine dei moduli in sezioni con intestazioni separate e il campo del modulo **Testo** per aggiungere testi informativi di sola lettura.

Vincoli e valori in designer modulo

Quando si modifica un elemento del blueprint o un modulo azione risorsa, è possibile applicare diversi vincoli e valori all'elemento.

Vincoli

I vincoli che si possono applicare a un elemento variano in base al tipo di elemento modificato o aggiunto al modulo. Alcuni valori di vincolo potrebbero essere configurati nel workflow di vRealize Orchestrator. Questi valori non vengono visualizzati nella scheda Vincoli perché spesso dipendono da condizioni che vengono valutate durante l'esecuzione del workflow. Eventuali valori di vincolo configurati per il modulo blueprint sovrascrivono i vincoli inclusi nel workflow di vRealize Orchestrator.

Dopo aver effettuato il calcolo per un campo, i binding minimo e massimo vengono ricalcolati solo quando viene richiesto un blueprint.

Per ogni vincolo applicato a un elemento, è possibile selezionare una delle seguenti opzioni per definire il vincolo:

Non impostato

Ottiene la proprietà dalla presentazione del workflow di vRealize Orchestrator.

Costante

Imposta l'elemento modificato su obbligatorio o facoltativo.

Campo

Collega l'elemento a un altro elemento dal modulo. È possibile ad esempio impostare l'elemento come obbligatorio solo quando è selezionato un altro elemento, come una casella di controllo.

Condizionale

Applica una condizione. Utilizzare le condizioni per creare varie clausole ed espressioni e applicarle allo stato o ai vincoli dell'elemento.

Esterno

Selezionare un'azione di script di vRealize Orchestrator che definisce il valore.

Tabella 3-61. Vincoli in designer modulo

Vincolo	Descrizione
Obbligatorio	Indica se l'elemento è obbligatorio.
Sola lettura	Indica se il campo è di sola lettura.
Valore	Imposta un valore per l'elemento.

Tabella 3-61. Vincoli in designer modulo (continua)

Vincolo	Descrizione
Visibile	<p>Indica se l'elemento sarà visibile dal cliente.</p> <p>Se si applica un vincolo di visibilità a un gruppo di visualizzazione nel workflow di vRealize Orchestrator, il vincolo viene ignorato nel modulo Dettagli richiesta inviata di XaaS e i campi che si desidera nascondere vengono visualizzati nel modulo.</p> <p>Per nascondere i campi che non si desidera visualizzare nel modulo Dettagli richiesta inviata e che non sono necessari per l'utente richiedente, rimuovere i campi dal modulo Dettagli richiesta inviata nella scheda Modulo blueprint nel designer di blueprint di XaaS. Per individuare questa scheda, vedere Aggiunta di un nuovo modulo blueprint di XaaS.</p>
Lunghezza minima	Imposta il numero minimo di caratteri dell'elemento di input stringa.
Lunghezza massima	Imposta il numero massimo di caratteri consentito dell'elemento di input stringa.
Valore minimo	Imposta il valore minimo dell'elemento di input numero.
Valore massimo	Imposta il valore massimo dell'elemento di input numero.
Incremento	Imposta un incremento per un elemento, ad esempio il campo Decimale o Intero . Se ad esempio si desidera presentare un campo Intero come dispositivo di scorrimento , è possibile utilizzare il valore per definirne il passo.
Conteggio minimo	<p>Imposta un numero minimo di voci selezionabili per l'elemento.</p> <p>Ad esempio, quando si aggiunge o si modifica un elenco caselle di controllo, è possibile impostare il numero minimo di caselle di controllo che il cliente deve selezionare per poter procedere.</p>
Conteggio massimo	<p>Imposta un numero massimo di voci selezionabili per l'elemento.</p> <p>Ad esempio, quando si aggiunge o si modifica un elenco caselle di controllo, è possibile impostare il numero massimo di caselle di controllo che il cliente deve selezionare per poter procedere.</p>

Valori

È possibile applicare valori ad alcuni degli elementi e definire cosa vedranno i clienti per alcuni dei campi. Le opzioni disponibili variano in base al tipo di elemento che si sta modificando o aggiungendo al modulo.

Tabella 3-62. Valori nel designer modulo

Valore	Descrizione
Non impostato	Ottiene il valore dell'elemento che si sta modificando dalla presentazione del workflow di vRealize Orchestrator.
Valori predefiniti	Selezionare valori da un elenco di oggetti correlati dall'inventario di vRealize Orchestrator.

Tabella 3-62. Valori nel designer modulo (continua)

Valore	Descrizione
Valore	Consente di definire un valore personalizzato statico con etichette.
Valori esterni	Selezionare un'azione di script di vRealize Orchestrator che definisce il valore con informazioni non direttamente esposte tramite il workflow.

Definizioni di valori esterni nel designer modulo

Quando si modificano alcuni elementi nel designer modulo, è possibile assegnare definizioni di valori esterni che utilizzano azioni script di vRealize Orchestrator personalizzate per fornire informazioni non esposte direttamente dal workflow.

Ad esempio, può essere utile pubblicare una risorsa azione per installare software su una macchina fornita in provisioning. Invece di fornire al cliente un elenco statico di tutti i software disponibili per il download, è possibile aggiornare dinamicamente l'elenco con il software adatto al sistema operativo della macchina, il software che l'utente non ha installato sulla macchina precedentemente o il software presente sulla macchina che è obsoleto e che richiede un aggiornamento.

Per fornire contenuti dinamici al cliente, è possibile creare un'azione script di vRealize Orchestrator che recupera le informazioni da visualizzare ai clienti. L'azione script viene assegnata a un campo nel designer modulo come definizione di un valore esterno. Quando la risorsa o il modulo blueprint servizio viene presentato al cliente, l'azione script recupera le informazioni personalizzate e le visualizza al cliente.

È possibile utilizzare definizioni di valori esterni per fornire valori predefiniti o di sola lettura, creare espressioni booleane, definire vincoli o fornire opzioni che i clienti possono selezionare da elenchi, caselle di controllo e così via.

Se si crea un blueprint con un workflow che include un campo obbligatorio, è obbligatorio nel modulo di richiesta anche se viene impostato come non obbligatorio.

Funzionamento di designer modulo

Quando si creano blueprint di XaaS, azioni risorsa personalizzate e risorse personalizzate, è possibile modificare i moduli di blueprint, azioni e risorse utilizzando il designer modulo. È possibile modificare la rappresentazione e definire cosa mostrare ai clienti dell'elemento o dell'azione quando questi richiedono l'elemento del catalogo o eseguono l'operazione post-provisioning.

Per impostazione predefinita, tutti moduli dei blueprint di di XaaS, delle azioni risorsa e delle risorse personalizzate vengono generati in base alla presentazione del workflow in vRealize Orchestrator.

Start Workflow: Create cluster

1 Common parameters

2 vCloud Distributed Storage

* Parent host folder
Not set

* Name of the new cluster

* Enable VMware HA
☐ Yes ☒ No

* Enable VMware DRS
☐ Yes ☒ No

Cancel Back Next Submit

I passaggi nella presentazione di vRealize Orchestrator sono rappresentati come pagine del modulo, mentre i gruppi della presentazione di vRealize Orchestrator sono rappresentati come sezioni separate. I tipi di input del workflow selezionato sono visualizzati come campi differenti nel modulo. Ad esempio, il tipo vRealize Orchestrator di string è rappresentato da una casella di testo. Un tipo complesso come VC:VirtualMachine è rappresentato da una casella di ricerca o da un albero, che permettono ai clienti di cercare una macchina virtuale digitando un valore alfanumerico o di selezionarla esplorare una struttura.

Workflow General **Blueprint Form** Provisioned Resource Component Lifecycle

Form: Request form

New fields

- Text field
- Text area
- Link
- Email
- Image URL field
- Password field
- Integer field
- Decimal field
- Date & time
- Check box
- Yes/No

Form page: Step

Step Distributed Storage cluster + Select
No VC.StoragePod selected

Virtual machines to update

Automation level

Keep VMDKs together No

È possibile cambiare il modo in cui un oggetto viene rappresentato in designer modulo. Ad esempio, è possibile modificare la rappresentazione predefinita di VC:VirtualMachine per cambiarla da una casella di ricerca a un albero. È anche possibile aggiungere nuovi campi come caselle di controllo, menu a discesa e così via, nonché applicare svariati vincoli. Se i nuovi campi aggiunti non sono validi o non sono correttamente mappati agli input del workflow di vRealize Orchestrator, all'esecuzione del workflow da parte del cliente, vRealize Orchestrator salterà i campi non validi o mappati erroneamente.

Progettazione di un modulo risorsa personalizzata

Tutti i campi del modulo dei dettagli della risorsa vengono visualizzati al cliente in sola lettura nella pagina dei dettagli degli elementi, quando viene eseguito il provisioning della risorsa personalizzata. È possibile eseguire operazioni di modifica di base sul modulo, come l'eliminazione, la modifica o la risistemazione dei campi, oppure è possibile aggiungere nuovi campi definiti esternamente che utilizzano azioni di script di vRealize Orchestrator per fornire ai clienti informazioni aggiuntive a sola lettura.

- **Modifica di un elemento risorsa personalizzata**

È possibile modificare alcune caratteristiche di un elemento nella pagina Modulo dettagli della risorsa personalizzata. Ciascun campo predefinito nella pagina rappresenta una proprietà della risorsa personalizzata. Non è possibile cambiare il tipo di una proprietà o i valori predefiniti, ma è possibile modificare il nome, la dimensione e la descrizione.

- **Aggiunta di una nuova pagina modulo per una risorsa personalizzata**

È possibile aggiungere una nuova pagina per riorganizzare il modulo in schede multiple.

- **Inserimento di un'intestazione di sezione in un modulo risorsa personalizzata**

È possibile inserire un'intestazione di sezione per suddividere il modulo in sezioni.

- **Inserimento di un elemento Testo in un modulo risorsa personalizzata**

È possibile inserire una casella di testo per aggiungere del testo descrittivo all'interno di un modulo.

- **Inserimento di un campo definito esternamente in un modulo risorsa personalizzata**

È possibile inserire un nuovo campo e assegnarlo a una definizione di valore esterno per fornire dinamicamente informazioni di sola lettura ai clienti, che potranno vederle nella pagina dei dettagli degli elementi quando eseguono il provisioning di una risorsa personalizzata.

Modifica di un elemento risorsa personalizzata

È possibile modificare alcune caratteristiche di un elemento nella pagina Modulo dettagli della risorsa personalizzata. Ciascun campo predefinito nella pagina rappresenta una proprietà della risorsa personalizzata. Non è possibile cambiare il tipo di una proprietà o i valori predefiniti, ma è possibile modificare il nome, la dimensione e la descrizione.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- **Aggiunta di una risorsa XaaS personalizzata..**

Procedura

- 1** Selezionare **Progettazione > XaaS > Risorse personalizzate**.
- 2** Fare clic sulla risorsa personalizzata da modificare.
- 3** Fare clic sulla scheda **Modulo dettagli**.
- 4** Selezionare l'elemento da modificare e fare clic sull'icona **Modifica**.
- 5** Immettere un nuovo nome per il campo nella casella di testo **Etichetta** per modificare l'etichetta.
- 6** Modificare la descrizione nella casella di testo **Descrizione**.
- 7** Selezionare un'opzione dal menu a discesa **Dimensioni** per cambiare la dimensione dell'elemento.
- 8** Selezionare un'opzione dal menu a discesa **Dimensioni etichetta** per cambiare la dimensione dell'etichetta.
- 9** Fare clic su **Invia**.
- 10** Fare clic su **Fine**.

Aggiunta di una nuova pagina modulo per una risorsa personalizzata

È possibile aggiungere una nuova pagina per riorganizzare il modulo in schede multiple.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa XaaS personalizzata..](#)

Procedura

- 1** Selezionare **Progettazione > XaaS > Risorse personalizzate**.
- 2** Fare clic sulla risorsa personalizzata da modificare.
- 3** Fare clic sulla scheda **Modulo dettagli**.
- 4** Fare clic sull'icona **Nuova pagina (+)** accanto al nome della **pagina del modulo**.
- 5** Selezionare il tipo di schermo inutilizzato e fare clic su **Invia**.

Se si ha già una visualizzazione dettagli risorsa o elenco risorse non è possibile crearne due dello stesso tipo.

- 6** Fare clic su **Invia**.
- 7** Configurare il modulo.
- 8** Fare clic su **Fine**.

Risultati

È possibile eliminare alcuni degli elementi dalla pagina modulo originale e inserirli nella nuova pagina modulo, o aggiungere nuovi campi che utilizzano definizioni di valori esterni per fornire informazioni ai clienti non mostrate direttamente dal workflow di vRealize Orchestrator.

Inserimento di un'intestazione di sezione in un modulo risorsa personalizzata

È possibile inserire un'intestazione di sezione per suddividere il modulo in sezioni.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa XaaS personalizzata..](#)

Procedura

- 1 Selezionare **Progettazione > XaaS > Risorse personalizzate**.
- 2 Fare clic sulla risorsa personalizzata da modificare.
- 3 Fare clic sulla scheda **Modulo dettagli**.
- 4 Trascinare l'elemento **Intestazione sezione** dal riquadro Modulo al riquadro della pagina Modulo.
- 5 Immettere un nome per la sezione.
- 6 Fare clic all'esterno dell'elemento per salvare le modifiche.
- 7 Fare clic su **Fine**.

Inserimento di un elemento Testo in un modulo risorsa personalizzata

È possibile inserire una casella di testo per aggiungere del testo descrittivo all'interno di un modulo.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa XaaS personalizzata..](#)

Procedura

- 1 Selezionare **Progettazione > XaaS > Risorse personalizzate**.
- 2 Fare clic sulla risorsa personalizzata da modificare.
- 3 Fare clic sulla scheda **Modulo dettagli**.
- 4 Trascinare l'elemento **Testo** dal riquadro Modulo al riquadro della pagina Modulo.
- 5 Immettere il testo da aggiungere.
- 6 Fare clic all'esterno dell'elemento per salvare le modifiche.
- 7 Fare clic su **Fine**.

Inserimento di un campo definito esternamente in un modulo risorsa personalizzata

È possibile inserire un nuovo campo e assegnarlo a una definizione di valore esterno per fornire dinamicamente informazioni di sola lettura ai clienti, che potranno vederle nella pagina dei dettagli degli elementi quando eseguono il provisioning di una risorsa personalizzata.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa XaaS personalizzata..](#)
- Creare o importare un'azione script di vRealize Orchestrator per recuperare le informazioni che si desidera fornire ai clienti.

Procedura

- 1 Selezionare **Progettazione > XaaS > Risorse personalizzate**.
- 2 Fare clic sulla risorsa personalizzata da modificare.
- 3 Fare clic sulla scheda **Modulo dettagli**.
- 4 Trascinare un elemento dal riquadro Nuovi campi al riquadro della pagina Modulo.
- 5 Immettere un ID per l'elemento nella casella di testo **ID**.
- 6 Immettere un'etichetta nella casella di testo **Etichetta**.
Le etichette sono scritte che i clienti possono vedere nei moduli.
- 7 (Facoltativo) Selezionare il tipo del campo dal menu a discesa **Tipo**.
- 8 Immettere il tipo di risultato dell'azione script di vRealize Orchestrator nella casella di ricerca **Tipo entità** e premere Invio.
Ad esempio, se si desidera utilizzare un'azione script per visualizzare l'utente corrente e lo script restituisce il tipo di risultato LdapUser di vRealize Orchestrator, immettere **LdapUser** nella casella di ricerca **Tipo entità** e premere Invio.
- 9 Fare clic su **Aggiungi valore esterno**.
- 10 Selezionare l'azione di script di vRealize Orchestrator personalizzata.
- 11 Fare clic su **Invia**.
- 12 Fare di nuovo clic su **Invia**.
- 13 Fare clic su **Fine**.

Risultati

Quando il modulo viene presentato al cliente, l'azione script recupera le informazioni personalizzate e le visualizza al cliente.

Progettazione di un modulo blueprint di XaaS

Quando si crea un blueprint di XaaS è possibile modificare il modulo del blueprint aggiungendo nuovi campi al modulo, modificando i campi esistenti, eliminando o risistemando i campi. È anche possibile creare nuovi moduli e pagine di modulo, nonché trascinare in essi nuovi campi.

■ Aggiunta di un nuovo modulo blueprint di XaaS

Quando si modifica il modulo generato in maniera predefinita per un workflow che si desidera pubblicare come blueprint di XaaS, è possibile aggiungere un nuovo modulo blueprint di XaaS.

■ Modifica di un elemento blueprint di XaaS

È possibile modificare alcune caratteristiche di un elemento nella pagina Modulo blueprint di un blueprint di XaaS. Si può cambiare il tipo di un elemento, i suoi valori predefiniti e applicare diversi vincoli e valori.

■ Aggiunta di un nuovo elemento

Quando si modifica il modulo di un blueprint di XaaS generato in maniera predefinita, è possibile aggiungere al modulo un nuovo elemento precedentemente definito. Se ad esempio non si desidera utilizzare un campo generato in maniera predefinita, è possibile eliminarlo e sostituirlo con uno nuovo.

■ Inserimento di un'intestazione di sezione in un modulo blueprint di XaaS

È possibile inserire un'intestazione di sezione per suddividere il modulo in sezioni.

■ Aggiunta di un elemento Testo a un modulo blueprint di XaaS

È possibile inserire una casella di testo per aggiungere del testo descrittivo all'interno di un modulo.

Aggiunta di un nuovo modulo blueprint di XaaS

Quando si modifica il modulo generato in maniera predefinita per un workflow che si desidera pubblicare come blueprint di XaaS, è possibile aggiungere un nuovo modulo blueprint di XaaS.

Aggiungendo un nuovo modulo blueprint di XaaS, si definisce quale sarà l'aspetto delle pagine di dettagli degli elementi del catalogo e delle richieste inviate. Se non si aggiungono moduli dei dettagli degli elementi del catalogo e delle richieste inviate, il cliente vedrà ciò che è definito nel modulo di richiesta.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di un blueprint XaaS](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Fare clic sul blueprint XaaS da modificare.
- 3 Fare clic sulla scheda **Modulo blueprint**.

- 4 Fare clic sull'icona **Nuovo modulo** (+).
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Selezionare il tipo di schermata dal menu **Tipo di schermo**.

Opzione	Descrizione
Dettagli elementi del catalogo	Pagina dei dettagli degli elementi del catalogo visualizzata ai clienti che fanno clic su un elemento del catalogo.
Modulo di richiesta	Modulo blueprint di XaaS predefinito. Modulo di richiesta mostrato ai clienti che richiedono l'elemento del catalogo.
Dettagli richiesta inviata	Pagina dei dettagli richiesta visualizzata ai clienti che hanno richiesto l'elemento e desiderano visualizzare i dettagli della richiesta nella scheda Distribuzione .

- 7 Fare clic su **Invia**.

Operazioni successive

Aggiungere i campi desiderati trascinandoli dal riquadro Nuovi campi al riquadro della pagina Modulo.

Modifica di un elemento blueprint di XaaS

È possibile modificare alcune caratteristiche di un elemento nella pagina Modulo blueprint di un blueprint di XaaS. Si può cambiare il tipo di un elemento, i suoi valori predefiniti e applicare diversi vincoli e valori.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di un blueprint XaaS](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Fare clic sul blueprint XaaS da modificare.
- 3 Fare clic sulla scheda **Modulo blueprint**.
- 4 Individuare l'elemento da modificare.
- 5 Fare clic sull'icona **Modifica** (✎).
- 6 Immettere un nuovo nome per il campo nella casella di testo **Etichetta**, sarà questa la scritta che vedranno i clienti.
- 7 Modificare la descrizione nella casella di testo **Descrizione**.
- 8 Selezionare un'opzione dal menu a discesa **Tipo** per cambiare il tipo di visualizzazione dell'elemento.

Le opzioni variano in base al tipo di elemento modificato.

- 9 Selezionare un'opzione dal menu a discesa **Dimensioni** per cambiare la dimensione dell'elemento.
- 10 Selezionare un'opzione dal menu a discesa **Dimensioni etichetta** per cambiare la dimensione dell'etichetta.
- 11 Modificare il valore predefinito dell'elemento.

Opzione	Descrizione
Non impostato	Ottiene il valore dell'elemento che si sta modificando dalla presentazione del workflow di vRealize Orchestrator.
Costante	Imposta il valore predefinito dell'elemento che si sta modificando su un valore costante specificato.
Campo	Collega il valore predefinito dell'elemento a un parametro di un altro elemento dalla rappresentazione.
Condizionale	Applica una condizione. Utilizzando le condizioni è possibile creare clausole ed espressioni varie e applicarle a un elemento.
Esterno	Selezionare un'azione di script di vRealize Orchestrator per definire il valore.

- 12 Dalla scheda **Vincoli** è possibile applicare vincoli all'elemento.

Opzione	Descrizione
Non impostato	Ottiene il valore dell'elemento che si sta modificando dalla presentazione del workflow di vRealize Orchestrator.
Costante	Imposta il valore predefinito dell'elemento che si sta modificando su un valore costante specificato.
Campo	Collega il valore predefinito dell'elemento a un parametro di un altro elemento dalla rappresentazione.
Condizionale	Applica una condizione. Utilizzando le condizioni è possibile creare clausole ed espressioni varie e applicarle a un elemento.
Esterno	Selezionare un'azione di script di vRealize Orchestrator per definire il valore.

- 13 Aggiungere uno o più valori per l'elemento nella scheda **Valori**.

Le opzioni disponibili variano in base al tipo di elemento che si sta modificando.

Opzione	Descrizione
Non impostato	Ottiene il valore dell'elemento che si sta modificando dalla presentazione del workflow di vRealize Orchestrator.
Valori predefiniti	<p>Selezionare valori da un elenco di oggetti correlati dall'inventario di vRealize Orchestrator.</p> <ol style="list-style-type: none"> a Immettere un valore nella casella di ricerca Valori predefiniti per cercare nell'inventario di vRealize Orchestrator. b Selezionare un valore dai risultati della ricerca e premere Invio.

Opzione	Descrizione
Valore	<p>Definire valori personalizzati con etichette.</p> <ul style="list-style-type: none"> a Immettere un valore nella casella di testo Valore. b Immettere un'etichetta per il valore nella casella di testo Etichetta. c Fare clic sull'icona Aggiungi (+).
Valori esterni	<p>Selezionare un'azione di script di vRealize Orchestrator per definire il valore con informazioni non direttamente esposte tramite il workflow.</p> <ul style="list-style-type: none"> ■ Selezionare Aggiungi valore esterno. ■ Selezionare l'azione di script di vRealize Orchestrator. ■ Fare clic su Invia.

14 Fare clic su **Invia**.

15 Fare clic su **Fine**.

Aggiunta di un nuovo elemento

Quando si modifica il modulo di un blueprint di XaaS generato in maniera predefinita, è possibile aggiungere al modulo un nuovo elemento precedentemente definito. Se ad esempio non si desidera utilizzare un campo generato in maniera predefinita, è possibile eliminarlo e sostituirlo con uno nuovo.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di un blueprint XaaS](#).

Procedura

- 1** Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2** Fare clic sul blueprint XaaS da modificare.
- 3** Fare clic sulla scheda **Modulo blueprint**.
- 4** Trascinare un elemento dal riquadro Nuovi campi al riquadro della pagina Modulo.
- 5** Immettere l'ID di un parametro di input del workflow nella casella di testo **ID**.
- 6** Immettere un'etichetta nella casella di testo **Etichetta**.
Le etichette sono scritte che i clienti possono vedere nei moduli.
- 7** (Facoltativo) Selezionare il tipo del campo dal menu a discesa **Tipo**.

- 8 Specificare un oggetto vRealize Orchestrator nella casella di testo **Tipo entità** e premere Invio.

Questo passaggio non è necessario per tutti i tipi di campi.

Opzione	Descrizione
Tipo di risultato	Se si sta utilizzando un'azione di script per definire un valore esterno per il campo, specificare il tipo del risultato dell'azione di script di vRealize Orchestrator.
Parametro di input	Se il campo dev'essere utilizzato per accettare un input da parte dei clienti e passare parametri indietro a vRealize Orchestrator, specificare il tipo del parametro di input accettato dal workflow di vRealize Orchestrator.
Parametro di output	Se il campo dev'essere utilizzato per visualizzare informazioni ai clienti, specificare il tipo del parametro di output del workflow di vRealize Orchestrator.

- 9 (Facoltativo) Selezionare la casella di controllo **Valori multipli** per consentire ai clienti di selezionare più di un oggetto.

Questa opzione non è disponibile per tutti i tipi di campi.

- 10 Fare clic su **Invia**.

- 11 Fare clic su **Aggiorna**.

Operazioni successive

È possibile modificare l'elemento per cambiare le impostazioni predefinite e applicare vincoli o valori diversi.

Inserimento di un'intestazione di sezione in un modulo blueprint di XaaS

È possibile inserire un'intestazione di sezione per suddividere il modulo in sezioni.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di un blueprint XaaS](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Fare clic sul blueprint XaaS da modificare.
- 3 Fare clic sulla scheda **Modulo blueprint**.
- 4 Trascinare l'elemento **Intestazione sezione** dal riquadro Modulo al riquadro della pagina Modulo.
- 5 Immettere un nome per la sezione.
- 6 Fare clic all'esterno dell'elemento per salvare le modifiche.
- 7 Fare clic su **Aggiorna**.

Aggiunta di un elemento Testo a un modulo blueprint di XaaS

È possibile inserire una casella di testo per aggiungere del testo descrittivo all'interno di un modulo.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di un blueprint XaaS](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Fare clic sul blueprint XaaS da modificare.
- 3 Fare clic sulla scheda **Modulo blueprint**.
- 4 Trascinare l'elemento **Testo** dal riquadro Nuovi campi al riquadro della pagina Modulo.
- 5 Immettere il testo da aggiungere.
- 6 Fare clic all'esterno dell'elemento per salvare le modifiche.
- 7 Fare clic su **Aggiorna**.

Progettazione di un modulo azione risorsa

Quando si crea un'azione risorsa è possibile modificare il modulo dell'azione aggiungendo nuovi campi al modulo, modificando i campi esistenti, eliminando o risistemando i campi. È anche possibile creare nuovi moduli e pagine di modulo, nonché trascinare in essi nuovi campi.

Aggiunta di un nuovo modulo azione risorsa

Quando si modifica il modulo generato in maniera predefinita per un workflow che si desidera pubblicare come azione risorsa, è possibile aggiungere un nuovo modulo azione risorsa.

Aggiungendo un nuovo modulo azione risorsa, si definisce quale sarà l'aspetto della pagina di dettagli dell'azione inviata. Se non si aggiunge un modulo di dettagli dell'azione inviata, il cliente vedrà ciò che è definito nel modulo azione.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione di un'azione risorsa](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic sull'azione risorsa da modificare.
- 3 Fare clic sulla scheda **Modulo**.
- 4 Fare clic sull'icona **Nuovo modulo** (+).
- 5 Immettere un nome e, facoltativamente, una descrizione.

6 Selezionare il tipo di schermata dal menu **Tipo di schermo**.

Opzione	Descrizione
Modulo azione	Modulo azione risorsa predefinito visualizzato ai clienti che eseguono l'azione post-provisioning.
Dettagli azione inviata	Pagina dei dettagli richiesta visualizzata ai clienti che richiedono l'azione e decidono di visualizzare i dettagli della richiesta nella scheda Distribuzione .

7 Fare clic su **Invia**.

Operazioni successive

Aggiungere i campi desiderati trascinandoli dal riquadro Nuovi campi al riquadro della pagina Modulo.

Aggiunta di un nuovo elemento a un modulo azione risorsa

Quando si modifica il modulo di un'azione risorsa generato in maniera predefinita, è possibile aggiungere al modulo un nuovo elemento precedentemente definito. Se ad esempio non si desidera utilizzare un campo generato in maniera predefinita, è possibile eliminarlo e sostituirlo con uno nuovo.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione di un'azione risorsa](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic sull'azione risorsa da modificare.
- 3 Fare clic sulla scheda **Modulo**.
- 4 Trascinare un elemento dal riquadro Nuovi campi al riquadro della pagina Modulo.
- 5 Immettere l'ID di un parametro di input del workflow nella casella di testo **ID**.
- 6 Immettere un'etichetta nella casella di testo **Etichetta**.
Le etichette sono scritte che i clienti possono vedere nei moduli.
- 7 (Facoltativo) Selezionare il tipo del campo dal menu a discesa **Tipo**.

- 8 Specificare un oggetto vRealize Orchestrator nella casella di testo **Tipo entità** e premere Invio.

Questo passaggio non è necessario per tutti i tipi di campi.

Opzione	Descrizione
Tipo di risultato	Se si sta utilizzando un'azione di script per definire un valore esterno per il campo, specificare il tipo del risultato dell'azione di script di vRealize Orchestrator.
Parametro di input	Se il campo dev'essere utilizzato per accettare un input da parte dei clienti e passare parametri indietro a vRealize Orchestrator, specificare il tipo del parametro di input accettato dal workflow di vRealize Orchestrator.
Parametro di output	Se il campo dev'essere utilizzato per visualizzare informazioni ai clienti, specificare il tipo del parametro di output del workflow di vRealize Orchestrator.

- 9 (Facoltativo) Selezionare la casella di controllo **Valori multipli** per consentire ai clienti di selezionare più di un oggetto.

Questa opzione non è disponibile per tutti i tipi di campi.

- 10 Fare clic su **Invia**.

- 11 Fare clic su **Fine**.

Operazioni successive

È possibile modificare l'elemento per cambiare le impostazioni predefinite e applicare vincoli o valori diversi.


Modifica di un elemento azione risorsa

È possibile modificare alcune caratteristiche di un elemento nella pagina Modulo di un'azione risorsa. Si può cambiare il tipo di un elemento, i suoi valori predefiniti e applicare diversi vincoli e valori.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione di un'azione risorsa](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic sull'azione risorsa da modificare.
- 3 Fare clic sulla scheda **Modulo**.
- 4 Individuare l'elemento da modificare.
- 5 Fare clic sull'icona **Modifica** ()

- 6 Immettere un nuovo nome per il campo nella casella di testo **Etichetta**, sarà questa la scritta che vedranno i clienti.
- 7 Modificare la descrizione nella casella di testo **Descrizione**.
- 8 Selezionare un'opzione dal menu a discesa **Tipo** per cambiare il tipo di visualizzazione dell'elemento.

Le opzioni variano in base al tipo di elemento modificato.

- 9 Selezionare un'opzione dal menu a discesa **Dimensioni** per cambiare la dimensione dell'elemento.
- 10 Selezionare un'opzione dal menu a discesa **Dimensioni etichetta** per cambiare la dimensione dell'etichetta.
- 11 Modificare il valore predefinito dell'elemento.

Opzione	Descrizione
Non impostato	Ottiene il valore dell'elemento che si sta modificando dalla presentazione del workflow di vRealize Orchestrator.
Costante	Imposta il valore predefinito dell'elemento che si sta modificando su un valore costante specificato.
Campo	Collega il valore predefinito dell'elemento a un parametro di un altro elemento dalla rappresentazione.
Condizionale	Applica una condizione. Utilizzando le condizioni è possibile creare clausole ed espressioni varie e applicarle a un elemento.
Esterno	Selezionare un'azione di script di vRealize Orchestrator per definire il valore.

- 12 Dalla scheda **Vincoli** è possibile applicare vincoli all'elemento.

Opzione	Descrizione
Non impostato	Ottiene il valore dell'elemento che si sta modificando dalla presentazione del workflow di vRealize Orchestrator.
Costante	Imposta il valore predefinito dell'elemento che si sta modificando su un valore costante specificato.
Campo	Collega il valore predefinito dell'elemento a un parametro di un altro elemento dalla rappresentazione.
Condizionale	Applica una condizione. Utilizzando le condizioni è possibile creare clausole ed espressioni varie e applicarle a un elemento.
Esterno	Selezionare un'azione di script di vRealize Orchestrator per definire il valore.

13 Aggiungere uno o più valori per l'elemento nella scheda **Valori**.

Le opzioni disponibili variano in base al tipo di elemento che si sta modificando.

Opzione	Descrizione
Non impostato	Ottiene il valore dell'elemento che si sta modificando dalla presentazione del workflow di vRealize Orchestrator.
Valori predefiniti	<p>Selezionare valori da un elenco di oggetti correlati dall'inventario di vRealize Orchestrator.</p> <ul style="list-style-type: none"> a Immettere un valore nella casella di ricerca Valori predefiniti per cercare nell'inventario di vRealize Orchestrator. b Selezionare un valore dai risultati della ricerca e premere Invio.
Valore	<p>Definire valori personalizzati con etichette.</p> <ul style="list-style-type: none"> a Immettere un valore nella casella di testo Valore. b Immettere un'etichetta per il valore nella casella di testo Etichetta. c Fare clic sull'icona Aggiungi (+).
Valori esterni	<p>Selezionare un'azione di script di vRealize Orchestrator per definire il valore con informazioni non direttamente esposte tramite il workflow.</p> <ul style="list-style-type: none"> ■ Selezionare Aggiungi valore esterno. ■ Selezionare l'azione di script di vRealize Orchestrator. ■ Fare clic su Invia.

14 Fare clic su **Invia**.**15** Fare clic su **Aggiorna**.

Inserimento di un'intestazione di sezione in un modulo azione risorsa

È possibile inserire un'intestazione di sezione per suddividere il modulo in sezioni.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione di un'azione risorsa](#).

Procedura

- 1** Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2** Fare clic sull'azione risorsa da modificare.
- 3** Fare clic sulla scheda **Modulo**.
- 4** Trascinare l'elemento **Intestazione sezione** dal riquadro Modulo al riquadro della pagina Modulo.
- 5** Immettere un nome per la sezione.
- 6** Fare clic all'esterno dell'elemento per salvare le modifiche.
- 7** Fare clic su **Fine**.

Aggiunta di un elemento Testo in un modulo azione risorsa

È possibile inserire una casella di testo per aggiungere del testo descrittivo all'interno di un modulo.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione di un'azione risorsa](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic sull'azione risorsa da modificare.
- 3 Fare clic sulla scheda **Modulo**.
- 4 Trascinare l'elemento **Testo** dal riquadro Nuovi campi al riquadro della pagina Modulo.
- 5 Immettere il testo da aggiungere.
- 6 Fare clic all'esterno dell'elemento per salvare le modifiche.
- 7 Fare clic su **Fine**.

Esempi e scenari di XaaS

Esempi e scenari sono di ausilio all'utente nel suggerire come utilizzare vRealize Automation per realizzare attività comuni utilizzando blueprint di XaaS e azioni risorsa.

Creazione di un blueprint di XaaS e di un'azione per la creazione e la modifica di un utente

Tramite XaaS è possibile creare e pubblicare un elemento di catalogo per il provisioning di un utente in un gruppo. È inoltre possibile associare una nuova operazione di post-provisioning all'utente di cui si è eseguito il provisioning. Ad esempio, un'operazione che consenta agli utenti del catalogo dei servizi di cambiare la propria password.

Un architetto di XaaS può creare una risorsa personalizzata, un blueprint di XaaS e pubblicare un elemento del catalogo per la creazione di un utente. Può inoltre creare un'azione risorsa per cambiare la password dell'utente.

Un amministratore del catalogo può creare un servizio e includere in esso l'elemento di catalogo dei blueprint. Può inoltre modificare la presentazione del workflow dell'elemento del catalogo utilizzando il designer modulo e cambiando la modalità di visualizzazione del modulo di richiesta ai clienti.

Un manager gruppo di business o un amministratore tenant può autorizzare un cliente per il nuovo servizio creato, l'elemento del catalogo e l'azione risorsa.

Prerequisiti

Verificare che il plug-in di Active Directory sia configurato correttamente e che si disponga dei diritti necessari per creare utenti in Active Directory.

Procedura

1 Creazione di un utente di prova come risorsa personalizzata

È possibile creare una risorsa personalizzata e mapparla al tipo di oggetto AD:User di vRealize Orchestrator.

2 Creazione di un blueprint di XaaS per la creazione di un utente

È possibile creare il blueprint Crea utente in un blueprint XaaS di gruppo in modo da poter eseguire il workflow che aggiunge utenti Active Directory e li assegna a gruppi di Active Directory. Il blueprint può essere creato come blueprint XaaS autonomo o come componente di un altro blueprint. In questo scenario verrà creato un blueprint autonomo.

3 Creazione di un'azione risorsa per cambiare una password utente

È possibile creare un'azione risorsa per consentire ai clienti del blueprint di creazione utente di XaaS di cambiare la password dell'utente dopo aver eseguito il provisioning dell'utente.

4 Creazione di un servizio e aggiunta di un blueprint per la creazione di un utente di prova

È possibile creare un servizio per visualizzare l'elemento Crea utente nel catalogo dei servizi.

5 Autorizzazione di un cliente per un servizio e un'azione risorsa

I manager dei gruppi di business e gli amministratori tenant possono autorizzare un utente o un gruppo di utenti per il servizio e l'azione risorsa. Una volta che questi sono stati autorizzati, il servizio verrà visualizzato nel loro catalogo ed essi potranno richiedere l'elemento del catalogo Crea utente di prova incluso nel servizio. Una volta che hanno eseguito il provisioning dell'elemento, i clienti possono richiedere il cambiamento della password dell'utente.

Creazione di un utente di prova come risorsa personalizzata

È possibile creare una risorsa personalizzata e mapparla al tipo di oggetto AD:User di vRealize Orchestrator.

Prerequisiti

Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

1 Selezionare **Progettazione > XaaS > Risorse personalizzate**.

2 Fare clic sull'icona **Nuovo** (+).

3 Nella casella di testo **Tipo di orchestrator** immettere **AD:User** e premere Invio.

4 Selezionare **AD:User** nell'elenco.

- 5 Immettere un nome per la risorsa.

Ad esempio **Utente di prova**.

- 6 Immettere la descrizione della risorsa.

Ad esempio

Risorsa personalizzata di prova da usare per creare un utente in un gruppo nel mio elemento di catalogo.

- 7 Fare clic su **Avanti**.

- 8 Lasciare invariati i valori predefiniti contenuti nel modulo.

- 9 Fare clic su **Fine**.

Risultati

È stata creata la risorsa personalizzata Utente di prova che verrà elencata nella pagina Risorse personalizzate.

Operazioni successive

Creare un blueprint di XaaS.

Creazione di un blueprint di XaaS per la creazione di un utente

È possibile creare il blueprint Crea utente in un blueprint XaaS di gruppo in modo da poter eseguire il workflow che aggiunge utenti Active Directory e li assegna a gruppi di Active Directory. Il blueprint può essere creato come blueprint XaaS autonomo o come componente di un altro blueprint. In questo scenario verrà creato un blueprint autonomo.

Prerequisiti

- Accertarsi di aver creato una risorsa personalizzata che supporti il provisioning di utenti Active Directory. Vedere [Creazione di un utente di prova come risorsa personalizzata](#).
- Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Nel riquadro Seleziona un workflow, passare a **Orchestrator > Libreria > Microsoft > Active Directory > Utente** e selezionare il workflow **Crea utente in un gruppo**.
- 4 Fare clic su **Avanti**.

5 Configurare le opzioni disponibili nella scheda Generale.

- a Cambiare il nome del blueprint in **Crea utente di prova** e lasciare invariata la descrizione.
- b Deselezionare la casella di controllo **Rendi disponibile come componente nella tela di progettazione**.

Poiché si sta pubblicando il blueprint direttamente nel catalogo dei servizi piuttosto che utilizzarlo come componente di un altro blueprint nella tela di progettazione, non è necessario configurare workflow per la scalabilità verticale o orizzontale.

La scheda **Ciclo di vita del componente** viene rimossa dall'interfaccia utente.

6 Fare clic su Avanti.**7 Modificare il modulo del blueprint.**

- a Fare clic su **Il nome di dominio nella forma Win2000**.
- b Fare clic sulla scheda **Vincoli**.
- c Fare clic sulla freccia a discesa **Valore**, selezionare **Costante** nel menu a discesa e immettere **test.domain**.
- d Fare clic sulla freccia a discesa **Visibile**, selezionare **Costante** nel menu a discesa e selezionare **No** nel menu a discesa.

Il nome del dominio è stato reso invisibile ai clienti dell'elemento del catalogo.

- e Fare clic su **Applica** per salvare le modifiche.

8 Fare clic su Avanti.**9 Selezionare newUser [Utente di prova] come parametro di output di cui eseguire il provisioning.****10 Fare clic su Avanti.****11 Fare clic su Fine.****12 Nella pagina Blueprint XaaS, selezionare la riga Crea utente di prova e fare clic su Pubblica.****Risultati**

La configurazione di un blueprint per la creazione di un utente di prova è completa e il blueprint è stato reso disponibile per l'aggiunta a un servizio.

Operazioni successive

Creare un'azione da eseguire sull'account utente di cui si è eseguito il provisioning. Vedere [Creazione di un'azione risorsa per cambiare una password utente](#).

Creazione di un'azione risorsa per cambiare una password utente

È possibile creare un'azione risorsa per consentire ai clienti del blueprint di creazione utente di XaaS di cambiare la password dell'utente dopo aver eseguito il provisioning dell'utente.

Prerequisiti

- Accedere a vRealize Automation come **architetto di XaaS**.
- Accertarsi di aver creato una risorsa personalizzata che supporti il provisioning di utenti Active Directory. Vedere [Creazione di un utente di prova come risorsa personalizzata](#).

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Passare a **Orchestrator > Libreria > Microsoft > Active Directory > Utente** nella libreria dei workflow di vRealize Orchestrator e selezionare il workflow **Cambia password utente**.
- 4 Fare clic su **Avanti**.
- 5 Selezionare **Utente di prova** dal menu a discesa **Tipo di risorsa**.
La selezione corrisponde alla risorsa personalizzata precedentemente creata.
- 6 Selezionare **utente** dal menu a discesa **Parametro di input**.
- 7 Fare clic su **Avanti**.
- 8 Cambiare il nome dell'azione risorsa in **Cambia password dell'utente di prova** e lasciare invariata la descrizione così come appare nella scheda **Dettagli**.
- 9 Fare clic su **Avanti**.
- 10 (Facoltativo) Lasciare il modulo invariato.
- 11 Fare clic su **Fine**.
- 12 Nella pagina Azioni risorsa, selezionare la riga **Cambia password dell'utente di prova** e fare clic su **Pubblica**.

Risultati

La creazione di un'azione risorsa per la modifica della password di un utente è completa e l'azione è stata resa disponibile per l'aggiunta a un permesso.

Operazioni successive

Aggiungere il blueprint Crea utente di prova a un servizio. Vedere [Creazione di un servizio e aggiunta di un blueprint per la creazione di un utente di prova](#).

Creazione di un servizio e aggiunta di un blueprint per la creazione di un utente di prova
È possibile creare un servizio per visualizzare l'elemento Crea utente nel catalogo dei servizi.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.

- Verificare di aver creato un blueprint di XaaS. Vedere [Creazione di un blueprint di XaaS per la creazione di un utente](#).

Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere **Utente Active Directory di prova** come nome del servizio.
- 4 Selezionare **Attivo** dal menu a discesa **Stato**.
- 5 Lasciare vuote le altre caselle di testo.
- 6 Fare clic su **OK**.
- 7 Nell'elenco Servizi, selezionare la riga **Utente Active Directory di prova** e fare clic su **Gestisci elementi del catalogo**.
- 8 Fare clic sull'icona **Nuovo** (+).
- 9 Selezionare **Crea utente di prova** e fare clic su **OK**.
Il blueprint XaaS Crea utente di prova viene aggiunto all'elenco degli elementi del catalogo.
- 10 Fare clic su **Chiudi**.

Risultati

Il servizio Utente Active Directory di prova include ora il blueprint Crea utente di prova. Non è necessario aggiungere azioni ai servizi.

Operazioni successive

È possibile autorizzare gli utenti a richiedere il blueprint ed eseguire l'azione. Vedere [Autorizzazione di un cliente per un servizio e un'azione risorsa](#).

Autorizzazione di un cliente per un servizio e un'azione risorsa

I manager dei gruppi di business e gli amministratori tenant possono autorizzare un utente o un gruppo di utenti per il servizio e l'azione risorsa. Una volta che questi sono stati autorizzati, il servizio verrà visualizzato nel loro catalogo ed essi potranno richiedere l'elemento del catalogo Crea utente di prova incluso nel servizio. Una volta che hanno eseguito il provisioning dell'elemento, i clienti possono richiedere il cambiamento della password dell'utente.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **manager del gruppo di business**.
- Verificare che il blueprint Crea utente sia aggiunto a un servizio Vedere [Creazione di un servizio e aggiunta di un blueprint per la creazione di un utente di prova](#).

- Verificare l'esistenza dell'azione risorsa Cambia password utente. Vedere [Creazione di un'azione risorsa per cambiare una password utente](#).

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere **Crea utente Active Directory** nella casella di testo **Nome**.
- 4 Lasciare vuote le caselle di testo **Descrizione** e **Data di scadenza**.
- 5 Selezionare **Attivo** dal menu a discesa **Stato**.
- 6 Selezionare un gruppo di business di destinazione dal menu a discesa **Gruppo di business**.
Ad esempio, Manager account IT.
- 7 Selezionare **Tutti gli utenti e i gruppi** per autorizzare tutti i membri del gruppo di business, ad esempio: Manager account IT, a creare account utente.
Gli utenti selezionati vedranno nel catalogo il servizio e gli elementi di catalogo inclusi nel servizio. Essi potranno quindi eseguire l'azione Cambia password utente sugli account utente che hanno creato.
- 8 Fare clic su **Avanti**.
- 9 Immettere **Utente Active Directory di prova** nella casella di testo **Servizi autorizzati** e premere Invio.
- 10 Immettere **Cambia password dell'utente di prova** nella casella di testo **Azioni autorizzate** e premere Invio.
- 11 Fare clic su **Fine**.

Risultati

La creazione di un permesso attivo che consente ai membri del gruppo di business Manager account IT di creare utenti è completa. Una volta eseguito il provisioning di un utente, sarà possibile eseguire l'azione risorsa per la modifica della password sull'account di tale utente.

Operazioni successive

Eseguire l'accesso come un utente autorizzato alla creazione di utenti Active Directory. Nella scheda **Catalogo**, verificare che il blueprint di XaaS crei l'utente come previsto. Una volta che la creazione dell'utente è stata completata, eseguire l'azione per la modifica della password dalla scheda **Distribuzioni**.

Creazione e pubblicazione di un'azione di XaaS per migrare una macchina virtuale

È possibile creare e pubblicare un'azione risorsa di XaaS per ampliare la gamma delle operazioni che i clienti possono eseguire su macchine virtuali vSphere con provisioning eseguito da IaaS.

In questo scenario, è possibile creare un'azione risorsa per migrare rapidamente una macchina virtuale vSphere.

Prerequisiti

Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

1 Creazione di un'azione risorsa per migrare una macchina virtuale vSphere

È possibile creare un'azione risorsa personalizzata per consentire ai clienti di migrare le macchine virtuali vSphere dopo che hanno eseguito il provisioning delle macchine virtuali vSphere con IaaS.

2 Pubblicazione di un'azione per migrare una macchina virtuale vSphere

Per utilizzare l'azione risorsa Migrazione rapida macchina virtuale come operazione successiva al provisioning, è necessario pubblicarla.

Creazione di un'azione risorsa per migrare una macchina virtuale vSphere

È possibile creare un'azione risorsa personalizzata per consentire ai clienti di migrare le macchine virtuali vSphere dopo che hanno eseguito il provisioning delle macchine virtuali vSphere con IaaS.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic su **Aggiungi (+)**.
- 3 Passare a **Orchestrator > Libreria > vCenter > Gestione macchina virtuale > Sposta e migra** nella libreria dei workflow di vRealize Orchestrator e selezionare il workflow **Migrazione rapida della macchina virtuale**.
- 4 Fare clic su **Avanti**.
- 5 Selezionare **IaaS VC VirtualMachine** dal menu a discesa **Tipo di risorsa**.
- 6 Selezionare **vm** dal menu a discesa **Parametro di input**.
- 7 Fare clic su **Avanti**.
- 8 Lasciare invariato il nome dell'azione risorsa e la descrizione così come appaiono nella scheda **Dettagli**.
- 9 Fare clic su **Avanti**.
- 10 Lasciare il modulo invariato.
- 11 Fare clic su **Fine**.

Risultati

È stata creata un'azione risorsa per la migrazione di una macchina virtuale che verrà elencata nella pagina Azioni risorsa.

Operazioni successive

[Pubblicazione di un'azione per migrare una macchina virtuale vSphere](#)

Pubblicazione di un'azione per migrare una macchina virtuale vSphere

Per utilizzare l'azione risorsa Migrazione rapida macchina virtuale come operazione successiva al provisioning, è necessario pubblicarla.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Selezionare la riga dell'azione risorsa Migrazione rapida macchina virtuale e fare clic sul pulsante **Pubblica**.

Risultati

È stato creato e pubblicato un workflow di vRealize Orchestrator come azione risorsa. È possibile passare a **Amministrazione > Gestione catalogo > Azioni** e vedere l'azione risorsa Migrazione rapida macchina virtuale nell'elenco delle azioni. È possibile assegnare un'icona all'azione risorsa. Vedere [Assegnazione di un'icona a un'azione risorsa XaaS](#).

Operazioni successive

Aggiungere l'azione ai permessi che contengono le macchine virtuali vSphere con provisioning eseguito da IaaS. Vedere [Autorizzazione degli utenti per servizi, elementi di catalogo e azioni](#).

Creazione di un'azione di XaaS per migrare una macchina virtuale con vMotion

Tramite XaaS è possibile creare e pubblicare un'azione risorsa per migrare una macchina virtuale con provisioning eseguito da IaaS con vMotion.

In questo scenario, è possibile creare un'azione risorsa per migrare una macchina virtuale vSphere con vMotion. Inoltre è possibile modificare la presentazione del workflow utilizzando il designer modulo e cambiando la modalità di visualizzazione dell'azione ai clienti quando questi la richiedono.

Prerequisiti

Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

- 1 [Creazione di un'azione per migrare una macchina virtuale vSphere con vMotion](#)

È possibile creare un'azione risorsa personalizzata per consentire agli utenti del catalogo dei servizi di migrare una macchina virtuale vSphere con vMotion dopo che hanno eseguito il provisioning della macchina con IaaS.

- 2 [Modifica del modulo azione risorsa](#)

Il modulo dell'azione risorsa corrisponde alla presentazione del workflow vRealize Orchestrator. È possibile modificare il modulo e definire cosa mostrare ai clienti dell'azione risorsa quando questi decidono di eseguire un'operazione post-provisioning.

3 Aggiunta di un modulo dettagli azione inviata e salvataggio dell'azione

È possibile aggiungere un nuovo modulo all'azione risorsa di migrazione macchina virtuale con vMotion per definire cosa mostrare ai clienti quando questi richiedono l'esecuzione di un'operazione post-provisioning.

4 Pubblicazione di un'azione per migrare una macchina virtuale con vMotion

Per utilizzare l'azione risorsa Migrazione macchina virtuale con vMotion come operazione successiva al provisioning, è necessario pubblicarla.

Creazione di un'azione per migrare una macchina virtuale vSphere con vMotion

È possibile creare un'azione risorsa personalizzata per consentire agli utenti del catalogo dei servizi di migrare una macchina virtuale vSphere con vMotion dopo che hanno eseguito il provisioning della macchina con IaaS.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic su **Aggiungi (+)**.
- 3 Passare a **Orchestrator > Libreria > vCenter > Gestione macchina virtuale > Sposta e migra** nella libreria dei workflow di vRealize Orchestrator e selezionare il workflow **Migrazione macchina virtuale con vMotion**.
- 4 Fare clic su **Avanti**.
- 5 Selezionare **IaaS VC VirtualMachine** dal menu a discesa **Tipo di risorsa**.
- 6 Selezionare **vm** dal menu a discesa **Parametro di input**.
- 7 Fare clic su **Avanti**.
- 8 Lasciare invariato il nome dell'azione risorsa e la descrizione così come appaiono nella scheda **Dettagli**.
- 9 Fare clic su **Avanti**.

Operazioni successive

[Modifica del modulo azione risorsa](#) .


Modifica del modulo azione risorsa

Il modulo dell'azione risorsa corrisponde alla presentazione del workflow vRealize Orchestrator. È possibile modificare il modulo e definire cosa mostrare ai clienti dell'azione risorsa quando questi decidono di eseguire un'operazione post-provisioning.


Procedura

- 1 Fare clic sull'icona **Elimina (X)** per eliminare l'elemento **pool**.

2 Modificare l'elemento **host**.


- a Fare clic sull'icona **Modifica** () accanto al campo **host**.
- b Digitare **Target host** nella casella di testo **Etichetta**.
- c Selezionare **Cerca** dal menu a discesa **Tipo**.
- d Fare clic sulla scheda **Vincoli**.
- e Selezionare **Costante** dal menu a discesa **Obbligatorio** e selezionare **Sì**.
Il campo dell'host è stato reso sempre obbligatorio.
- f Fare clic su **Invia**.

3 Modificare l'elemento **Priorità**.

- a Fare clic sull'icona **Modifica** () accanto al campo **Priorità**.
- b Digitare **Priority of the task** nella casella di testo **Etichetta**.
- c Selezionare **Gruppo pulsanti di opzione** dal menu a discesa **Tipo**.
- d Fare clic sulla scheda **Valori** e deselezionare la casella di controllo **Non impostato**.
- e Immettere **lowPriority** nella casella di testo di ricerca **Valori predefiniti** e premere Invio.
- f Immettere **defaultPriority** nella casella di testo di ricerca **Valori predefiniti** e premere Invio.
- g Immettere **highPriority** nella casella di testo di ricerca **Valori predefiniti** e premere Invio.
- h Fare clic su **Invia**.

Quando richiederanno l'azione risorsa, i clienti vedranno un gruppo di tre pulsanti di opzione: **lowPriority**, **defaultPriority** e **highPriority**.

4 Modificare l'elemento **Stato**.

- a Fare clic sull'icona **Modifica** () accanto al campo **Stato**.
- b Digitare **Virtual machine state** nella casella di testo **Etichetta**.
- c Selezionare **Menu a discesa** dal menu a discesa **Tipo**.
- d Fare clic sulla scheda **Valori** e deselezionare la casella di controllo **Non impostato**.
- e Immettere **poweredOff** nella casella di testo di ricerca **Valori predefiniti** e premere Invio.
- f Immettere **poweredOn** nella casella di testo di ricerca **Valori predefiniti** e premere Invio.
- g Immettere **suspended** nella casella di testo di ricerca **Valori predefiniti** e premere Invio.
- h Fare clic su **Invia**.

Quando richiederanno l'azione risorsa, i clienti vedranno un menu a discesa con tre opzioni: **poweredOff**, **poweredOne** **suspended**.

Risultati

È stata modificata la presentazione del workflow Migrazione macchina virtuale con vMotion.

Operazioni successive

[Aggiunta di un modulo dettagli azione inviata e salvataggio dell'azione.](#)

Aggiunta di un modulo dettagli azione inviata e salvataggio dell'azione

È possibile aggiungere un nuovo modulo all'azione risorsa di migrazione macchina virtuale con vMotion per definire cosa mostrare ai clienti quando questi richiedono l'esecuzione di un'operazione post-provisioning.

Procedura

- 1 Fare clic sull'icona **Nuovo modulo** (+) accanto al menu a discesa **Modulo**.
- 2 Digitare **Azione inviata** nella casella di testo **Nome**.
- 3 Lasciare vuoto il campo **Descrizione**.
- 4 Selezionare **Dettagli azione inviata** dal menu **Tipo di schermo**.
- 5 Fare clic su **Invia**.
- 6 Fare clic sull'icona **Modifica** (penna) accanto al menu a discesa **Pagina modulo**.
- 7 Digitare **Dettagli** nella casella di testo **Intestazione**.
- 8 Fare clic su **Invia**.
- 9 Trascinare l'elemento **Testo** dal riquadro Modulo alla pagina **Modulo**.
- 10 Digitare
È stata inviata una richiesta di migrazione della macchina virtuale con vMotion.
Attendere il completamento del processo.
- 11 Fare clic all'esterno della casella di testo per salvare le modifiche.
- 12 Fare clic su **Invia**.
- 13 Fare clic su **Aggiungi**.

Risultati

È stata creata un'azione risorsa per migrare una macchina virtuale con vMotion, che verrà elencata nelle pagina Azioni risorsa.

Operazioni successive

[Pubblicazione di un'azione per migrare una macchina virtuale con vMotion.](#)

Pubblicazione di un'azione per migrare una macchina virtuale con vMotion

Per utilizzare l'azione risorsa Migrazione macchina virtuale con vMotion come operazione successiva al provisioning, è necessario pubblicarla.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Selezionare la riga dell'azione Migrazione macchina virtuale con vMotion e fare clic sul pulsante **Pubblica**.

Risultati

È stato creato e pubblicato un workflow di vRealize Orchestrator come azione risorsa. È possibile passare a **Amministrazione > Gestione catalogo > Azioni** e vedere l'azione Migrazione macchina virtuale con vMotion nell'elenco delle azioni. È possibile assegnare un'icona all'azione risorsa. Vedere [Assegnazione di un'icona a un'azione risorsa XaaS](#).

Inoltre è stata modificata la presentazione del workflow e definito l'aspetto dell'azione.

Operazioni successive

I manager dei gruppi di business e gli amministratori tenant possono includere un'azione risorsa Migrazione macchina virtuale con vMotion in un permesso. Per ulteriori informazioni su come creare e pubblicare blueprint di IaaS per piattaforme virtuali, vedere [Progettazione dei blueprint delle macchine](#).

Creazione e pubblicazione di un'azione di XaaS per creare uno snapshot

Tramite XaaS è possibile creare e pubblicare un'azione risorsa per creare uno snapshot di una macchina virtuale vSphere con provisioning eseguito con IaaS.

In questo scenario, è possibile creare un'azione risorsa per creare uno snapshot di una macchina virtuale vSphere con provisioning eseguito con IaaS. Inoltre è possibile modificare la presentazione del workflow utilizzando il designer modulo e cambiando la modalità di visualizzazione dell'azione ai clienti quando questi la richiedono.

Prerequisiti

Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

- 1 [Creazione dell'azione per la cattura di uno snapshot di una macchina virtuale vSphere](#)
È possibile creare un'azione risorsa personalizzata per consentire ai clienti di catturare uno snapshot di una macchina virtuale vSphere dopo che hanno eseguito il provisioning della macchina con IaaS.
- 2 [Pubblicazione dell'azione di creazione di uno snapshot](#)
Per utilizzare l'azione risorsa Create a snapshot come operazione successiva al provisioning, è necessario pubblicarla.

Creazione dell'azione per la cattura di uno snapshot di una macchina virtuale vSphere

È possibile creare un'azione risorsa personalizzata per consentire ai clienti di catturare uno snapshot di una macchina virtuale vSphere dopo che hanno eseguito il provisioning della macchina con IaaS.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic su **Aggiungi (+)**.
- 3 Passare a **Orchestrator > Libreria > vCenter > Gestione macchina virtuale > Snapshot** nella libreria dei workflow di vRealize Orchestrator e selezionare il workflow **Crea snapshot**.
- 4 Fare clic su **Avanti**.
- 5 Selezionare **IaaS VC VirtualMachine** dal menu a discesa **Tipo di risorsa**.
- 6 Selezionare **vm** dal menu a discesa **Parametro di input**.
- 7 Fare clic su **Avanti**.
- 8 Lasciare invariato il nome dell'azione risorsa e la descrizione così come appaiono nella scheda **Dettagli**.
- 9 Fare clic su **Avanti**.
- 10 Lasciare il modulo invariato.
- 11 Fare clic su **Aggiungi**.

Risultati

È stata creata un'azione risorsa per la creazione di uno snapshot di una macchina virtuale che verrà elencata nella pagina Azioni risorsa.

Operazioni successive

[Pubblicazione dell'azione di creazione di uno snapshot.](#)

Pubblicazione dell'azione di creazione di uno snapshot

Per utilizzare l'azione risorsa Create a snapshot come operazione successiva al provisioning, è necessario pubblicarla.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Selezionare la riga dell'azione Create a snapshot e fare clic sul pulsante **Pubblica**.

Risultati

È stato creato e pubblicato un workflow di vRealize Orchestrator come azione risorsa. È possibile passare a **Amministrazione > Gestione catalogo > Azioni** e vedere l'azione risorsa Crea snapshot nell'elenco delle azioni. È possibile assegnare un'icona all'azione risorsa. Vedere [Assegnazione di un'icona a un'azione risorsa XaaS](#).

Operazioni successive

I manager dei gruppi di business e gli amministratori tenant possono includere l'azione risorsa Crea snapshot in un permesso. Per ulteriori informazioni su come creare e pubblicare blueprint di IaaS per piattaforme virtuali, vedere [Progettazione dei blueprint delle macchine](#).

Creazione e pubblicazione di un'azione di XaaS per avviare una macchina virtuale Amazon

Tramite XaaS è possibile creare e pubblicare azioni per ampliare la gamma di operazioni che i clienti possono eseguire su risorse di terzi con provisioning eseguito.

In questo scenario, è possibile creare e pubblicare un'azione risorsa per avviare rapidamente le macchine virtuali Amazon.

Prerequisiti

- Installare il plug-in di vRealize Orchestrator per Amazon Web Services sul server vRealize Orchestrator predefinito.
- Creare o importare un workflow di vRealize Orchestrator per la mappatura delle risorse delle istanze di Amazon.

Procedura

1 [Creazione di una mappatura delle risorse per istanze Amazon](#)

È possibile creare una mappatura delle risorse per associare le istanze di Amazon fornite in provisioning mediante l'uso di IaaS con il tipo AWS:EC2Instance di vRealize Orchestrator esposto dal plug-in Amazon Web Services.

2 [Creazione di un'azione risorsa per avviare una macchina virtuale Amazon](#)

È possibile creare un'azione risorsa per consentire ai clienti di avviare macchine virtuali Amazon di cui è stato eseguito il provisioning.

3 [Pubblicazione dell'azione per l'avvio di istanze Amazon](#)

Per utilizzare la nuova azione risorsa Start Instances creata per operazioni successive al provisioning su macchine virtuali Amazon, è necessario pubblicarla.

Creazione di una mappatura delle risorse per istanze Amazon

È possibile creare una mappatura delle risorse per associare le istanze di Amazon fornite in provisioning mediante l'uso di IaaS con il tipo AWS:EC2Instance di vRealize Orchestrator esposto dal plug-in Amazon Web Services.

Prerequisiti

- Accedere a vRealize Automation come **architetto di XaaS**.
- Creare o importare un workflow di mappatura delle risorse o un'azione script di vRealize Orchestrator.

Procedura

- 1 Selezionare **Progettazione > XaaS > Mappature risorse**.

- 2 Fare clic su **Aggiungi** (+).
- 3 Immettere **EC2 Instance** nella casella di testo **Nome**.
- 4 Specificare **Cloud Machine** nella casella di testo **Tipo di risorsa catalogo**.
- 5 Specificare **AWS:EC2Instance** nella casella di testo **Tipo di orchestrator**.
- 6 Selezionare **Sempre disponibile**.
- 7 Selezionare il tipo di mappatura risorse da utilizzare.
- 8 Selezionare un workflow o un'azione script di mappatura risorse personalizzata dalla libreria di vRealize Orchestrator.
- 9 Fare clic su **Aggiungi**.

Risultati

È possibile utilizzare la mappatura risorse di Amazon per creare azioni risorsa per le macchine Amazon di cui è stato eseguito il provisioning utilizzando IaaS.

Operazioni successive

[Creazione di un'azione risorsa per avviare una macchina virtuale Amazon.](#)

Creazione di un'azione risorsa per avviare una macchina virtuale Amazon

È possibile creare un'azione risorsa per consentire ai clienti di avviare macchine virtuali Amazon di cui è stato eseguito il provisioning.

Prerequisiti

Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Fare clic su **Aggiungi** (+).
- 3 Selezionare **Orchestrator > Libreria > Amazon Web Services > Cloud flessibile > Istanze** e scegliere il workflow **Avvia istanze** nella cartella dei workflow.
- 4 Fare clic su **Avanti**.
- 5 Selezionare **Istanza EC2** dal menu a discesa **Tipo di risorsa**.
Questo è il nome della mappatura risorse precedentemente creata.
- 6 Selezionare **istanza** dal menu a discesa **Parametro di input**.
Questo è il parametro di input del workflow dell'azione risorsa corrispondente alla mappatura risorse.
- 7 Fare clic su **Avanti**.

8 Lasciare invariati il nome e la descrizione.

Il nome predefinito dell'azione risorsa è **Avvia istanze**.

9 Fare clic su **Avanti**.

10 Lasciare invariati i campi della scheda **Modulo**.

11 Fare clic su **Aggiungi**.

Risultati

È stata creata un'azione risorsa per l'avvio di macchine virtuali Amazon che verrà elencata nella pagina Azioni risorsa.

Operazioni successive

[Pubblicazione dell'azione per l'avvio di istanze Amazon](#).

Pubblicazione dell'azione per l'avvio di istanze Amazon

Per utilizzare la nuova azione risorsa Start Instances creata per operazioni successive al provisioning su macchine virtuali Amazon, è necessario pubblicarla.

Prerequisiti

Accedere a vRealize Automation come **architetto di XaaS**.

Procedura

1 Selezionare **Progettazione > XaaS > Azioni risorsa**.

2 Selezionare la riga dell'azione risorsa Start Instances e fare clic su **Pubblica**.

Risultati

Anche lo stato dell'azione risorsa Start Instances cambia in **Pubblicato**.

Operazioni successive

Aggiungere l'azione di avvio delle istanze al permesso che include l'elemento di catalogo Amazon. Vedere [Autorizzazione degli utenti per servizi, elementi di catalogo e azioni](#).

Risoluzione dei problemi correlati ad accenti errati e caratteri speciali contenuti nei blueprint di XaaS

Quando si creano blueprint di XaaS per lingue che utilizzano caratteri non ASCII, gli accenti e i caratteri speciali vengono visualizzati in modo errato e/o illeggibile.

Causa

Potrebbe essere abilitata una proprietà di configurazione di vRealize Orchestrator non impostata in maniera predefinita.

Soluzione

1 Nel file system del server Orchestrator, passare a `/etc/vco/app-server/`.

- 2 Aprire il file di configurazione `vmo.properties` in un editor di testo.
- 3 Verificare che la proprietà seguente sia disattivata.

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 Salvare il file `vmo.properties`.
- 5 Riavviare il server di vRealize Orchestrator.

Pubblicazione di un blueprint

I blueprint vengono salvati nello stato di bozza e devono essere pubblicati manualmente prima di poterli configurare come elementi di catalogo o utilizzare come componenti blueprint nella tela di progettazione.

Dopo aver pubblicato il blueprint, è possibile autorizzarlo per renderlo disponibile per le richieste di provisioning nel catalogo dei servizi.

È necessario pubblicare una sola volta un blueprint. Tutte le modifiche apportate a un blueprint pubblicato vengono automaticamente riportate nel catalogo e nei componenti nidificati del blueprint.

Pubblicazione di un blueprint

È possibile pubblicare un blueprint per utilizzarlo nel provisioning delle macchine e, facoltativamente, riutilizzarlo in un altro blueprint. Per utilizzare il blueprint per la richiesta del provisioning di macchine, è necessario autorizzare il blueprint dopo averlo pubblicato. I blueprint utilizzati come componenti in altri blueprint non devono essere autorizzati.

Prerequisiti

- Accedere a vRealize Automation come **architetto dell'infrastruttura**.
- Creare un blueprint. Vedere *Elenco di controllo per la creazione di blueprint di vRealize Automation*.

Procedura

- 1 Fare clic sulla scheda **Progettazione**.
- 2 Fare clic su **Blueprint**.
- 3 Selezionare il blueprint da pubblicare e fare clic su **Pubblica**.
- 4 Fare clic su **OK**.

Risultati

Il blueprint viene pubblicato come elemento di catalogo, ma è necessario prima autorizzarlo per renderlo disponibile agli utenti nel catalogo dei servizi.

Operazioni successive

Aggiungere il blueprint al servizio del catalogo e autorizzare gli utenti a richiedere l'elemento di catalogo per il provisioning delle macchine in base a quanto definito nel blueprint.

Utilizzo di blueprint gestiti dagli sviluppatori

Oltre al metodo gestito dall'interfaccia utente per la creazione di blueprint di vRealize Automation, è possibile utilizzare blueprint anche a livello di programmazione utilizzando strumenti come vRealize CloudClient, con blueprint autonomi forniti o provenienti da altre origini, e in collaborazione con altri sviluppatori mediante applicazioni e workflow di vRealize Suite, nonché strumenti di terze parti.

Per informazioni su questi metodi, vedere gli argomenti seguenti:

- [Esportazione e importazione di blueprint e contenuti](#)
- [Download e configurazione del blueprint autonomo fornito](#)
- [Creazione di blueprint e altri contenuti di IaaS in un ambiente con più sviluppatori](#)

Esportazione e importazione di blueprint e contenuti

È possibile esportare blueprint e contenuti tramite programma da un ambiente vRealize Automation a un altro utilizzando l'interfaccia API REST di vRealize Automation o tramite vRealize CloudClient.

Ad esempio, è possibile creare e testare i blueprint in un ambiente di sviluppo e quindi importarli nel proprio ambiente di produzione. In alternativa, è possibile importare una definizione di proprietà da un forum della community nella propria istanza tenant vRealize Automation attiva.

È possibile importare ed esportare tramite programma i seguenti elementi contenuto di vRealize Automation:

- Blueprint di applicazioni e tutti i rispettivi componenti
- Blueprint di macchine IaaS
- Componenti di Software
- Blueprint di XaaS
- Profili componente
- Gruppi di proprietà

Le informazioni sui gruppi di proprietà sono specifiche del tenant e vengono importate soltanto con il blueprint se il gruppo di proprietà esiste già nell'istanza target di vRealize Automation.

Quando si esporta un blueprint da un tenant dell'istanza di vRealize Automation in un altro, le informazioni del gruppo di proprietà definite per tale blueprint non vengono riconosciute per il blueprint importato a meno che il gruppo di proprietà esista già nell'istanza target del tenant. Ad esempio, se si importa un blueprint che contiene un gruppo di proprietà denominato `mica1`, il gruppo di proprietà `mica1` sarà presente nel blueprint importato solo se il gruppo di proprietà `mica1` esiste già nell'istanza di vRealize Automation nella quale si importa il blueprint. Per evitare di perdere le informazioni sul gruppo di proprietà durante l'esportazione di un blueprint da un'istanza di vRealize Automation a un'altra, utilizzare vRealize CloudClient per creare un file zip di esportazione contenente il gruppo di proprietà e importare tale file nel tenant target prima di importare il blueprint. Per maggiori informazioni sull'uso di vRealize CloudClient per l'elencazione, la creazione di pacchetti, l'esportazione e l'importazione dei gruppi di proprietà e altri elementi di vRealize Automation, vedere il VMware Developer Center all'indirizzo <https://developercenter.vmware.com/tool/cloudclient>.

Tabella 3-63. Scelta dello strumento di importazione ed esportazione

Strumento	Ulteriori informazioni
vRealize CloudClient	Vedere la pagina vRealize CloudClient sul sito VMware code.vmware.com https://developercenter.vmware.com/tool/cloudclient .
API REST di vRealize Automation	Vedere la documentazione dell'API in VMware API Explorer per vRealize Automation all'indirizzo https://code.vmware.com/apis/vrealize-automation .

Nota quando si esportano o importano blueprint tramite programma tra distribuzioni vRealize Automation, ad esempio da un ambiente di test a uno di produzione o da un'organizzazione all'altra, è importante rilevare quali sono i dati del modello di clone che vengono inclusi nel pacchetto. Quando si importa il pacchetto del blueprint, le impostazioni predefinite vengono popolate in base alle informazioni presenti nel pacchetto. Se ad esempio si esporta e poi si importa un blueprint creato utilizzando un workflow di tipo clonazione e il modello da cui derivano quei dati di clonazione non esiste in alcun endpoint all'interno della distribuzione vRealize Automation in cui si importa il blueprint, alcune impostazioni del blueprint importato non saranno applicate a quella distribuzione.

Scenario: importazione di Dukes Bank per l'applicazione campione di vSphere e configurazione dell'ambiente

Un professionista IT impegnato nella valutazione o nell'apprendimento di vRealize Automation è interessato a importare una robusta applicazione di esempio nella propria istanza di vRealize Automation, che gli consenta di esplorare rapidamente le funzionalità disponibili e stabilire come creare i blueprint di vRealize Automation più adatti alle esigenze della sua organizzazione.

Prerequisiti

- Preparare una macchina di riferimento Linux CentOS 6.x, convertirla in un modello e creare una specifica di personalizzazione. Vedere [Scenario: preparazione per l'importazione di Dukes Bank per il blueprint dell'applicazione campione di vSphere](#).

- Creare un profilo di rete esterna per fornire un gateway e un intervallo di indirizzi IP. Vedere [Creazione di un profilo di rete esterna mediante un provider IPAM di terze parti](#).
- Mappare il profilo di rete esterno sulla prenotazione vSphere. Vedere [Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer](#). L'applicazione campione non può eseguire correttamente il provisioning senza un profilo di rete esterna.
- Verificare di avere entrambi i privilegi di **architetto dell'infrastruttura** e **architetto software**. Entrambi i ruoli sono necessari per importare l'applicazione campione Dukes Bank e per interagire con i componenti software e i blueprint di Dukes Bank.

Procedura

1 Scenario: importazione di Dukes Bank per l'applicazione campione di vSphere

È possibile scaricare Dukes Bank per l'applicazione di vSphere dall'appliance vRealize Automation. Importare l'applicazione campione nel tenant di vRealize Automation per visualizzare un campione funzionante di un blueprint multilivello di vRealize Automation che include più componenti macchina con componenti di rete e software.

2 Scenario: configurazione dei componenti campione di Dukes Bank di vSphere per il proprio ambiente

Utilizzando i privilegi di architetto dell'infrastruttura, è possibile configurare i singoli componenti macchina di Dukes Bank per utilizzare specifica di personalizzazione, modello e prefissi macchina creati per l'ambiente.

Risultati

Da questo momento l'applicazione campione Dukes Bank di vSphere è configurata per l'ambiente e può essere impiegata come punto di partenza per lo sviluppo dei propri blueprint, come strumento di valutazione di vRealize Automation e come valida risorsa di formazione per apprendere le nozioni fondamentali su funzionalità e componenti di vRealize Automation.

Scenario: importazione di Dukes Bank per l'applicazione campione di vSphere

È possibile scaricare Dukes Bank per l'applicazione di vSphere dall'appliance vRealize Automation. Importare l'applicazione campione nel tenant di vRealize Automation per visualizzare un campione funzionante di un blueprint multilivello di vRealize Automation che include più componenti macchina con componenti di rete e software.

Procedura

- 1 Accedere all'appliance vRealize Automation come utente root utilizzando SSH.
- 2 Scaricare Dukes Bank per l'applicazione campione di vSphere dall'appliance vRealize Automation in /tmp.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/DukesBankAppForvSphere.zip
```

Non decomprimere il pacchetto.

- 3 Scaricare vRealize CloudClient da <http://developercenter.vmware.com/tool/cloudclient> in /tmp.
- 4 Decomprimere il pacchetto cloudclient-4x-dist.zip.
- 5 Eseguire vRealize CloudClient nella directory /bin.

```
$>./bin/cloudclient.sh
```

- 6 Se richiesto, accettare il contratto di licenza.
- 7 Mediante vRealize CloudClient, accedere all'appliance vRealize Automation come utente con privilegi **Architetto del software** e **Architetto dell'infrastruttura**.

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user  
<user@domain.com> --tenant <TenantName>
```

- 8 Quando richiesto, immettere la password di accesso.
- 9 Verificare che il contenuto del file DukesBankAppForvSphere.zip sia disponibile.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run true --resolution OVERWRITE
```

Si noti che per la voce OVERWRITE viene fatta distinzione tra lettere maiuscole e minuscole ed è necessario utilizzare tutte lettere maiuscole.

Configurando la risoluzione per sovrascrivere invece di *ignorare*, si permette a vRealize Automation di correggere i conflitti quando possibile.

- 10 Importare l'applicazione campione Dukes Bank.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run false --resolution  
OVERWRITE
```

Si noti che per la voce OVERWRITE viene fatta distinzione tra lettere maiuscole e minuscole ed è necessario utilizzare tutte lettere maiuscole.

Risultati

Quando si accede alla console di vRealize Automation come utente con privilegi Architetto del software e Architetto dell'infrastruttura, i componenti software e i blueprint di Dukes Bank vengono visualizzati nella scheda **Progettazione > Blueprint** e nella scheda **Progettazione > Componenti software**.

Scenario: configurazione dei componenti campione di Dukes Bank di vSphere per il proprio ambiente

Utilizzando i privilegi di architetto dell'infrastruttura, è possibile configurare i singoli componenti macchina di Dukes Bank per utilizzare specifica di personalizzazione, modello e prefissi macchina creati per l'ambiente.

In questo scenario vengono configurati i componenti macchina per clonare le macchine dal modello creato nel vSphere Web Client. Se si desidera creare copie con ottimizzazione dello spazio di una macchina virtuale basata su uno snapshot, l'applicazione campione supporta anche i cloni collegati. I cloni collegati utilizzano una catena di dischi delta per tenere traccia delle differenze da una macchina padre, il loro provisioning è particolarmente rapido, i costi di storage sono ridotti e si rivelano ideali quando le prestazioni non rappresentano una priorità.

Procedura

- 1 Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.

È possibile configurare l'applicazione campione Dukes Bank per funzionare nell'ambiente utilizzando unicamente il ruolo di **architetto dell'infrastruttura**, ma se si desidera visualizzare o modificare i componenti software del campione è richiesto anche il ruolo di **architetto software**.

- 2 Scegliere **Progettazione > Blueprint**.

- 3 Selezionare il blueprint **DukesBankApplication** e fare clic sull'icona **Modifica**.

- 4 Modificare appserver-node in modo che vRealize Automation possa eseguire il provisioning di questo componente macchina nell'ambiente.

Configurare il blueprint per eseguire il provisioning di più istanze di questo componente macchina in modo da poter verificare il funzionamento del nodo di bilanciamento del carico.

- a Fare clic sul componente **appserver-node** nella tela di progettazione.

Nel pannello inferiore vengono mostrati i dettagli della configurazione.

- b Selezionare il prefisso macchina dal menu a discesa **Prefisso macchina**.
- c Configurare il blueprint per eseguire il provisioning di alcune istanze di questo nodo selezionando minimo 2 e massimo 10 istanze.

Nel modulo di richiesta, gli utenti possono eseguire il provisioning di almeno due e massimo dieci nodi appserver. Se gli utenti sono autorizzati a eseguire la scalabilità verticale e la scalabilità orizzontale, possono scalare la propria distribuzione per soddisfare le esigenze in continua evoluzione.

- d Fare clic sulla scheda **Informazioni build**.
- e Selezionare **Cloneworkflow** dal menu a discesa **Provisioning workflow**.
- f Selezionare il **dukes_bank_template** dal catalogo **Clona da**.
- g Specificare il **Customspecs_sample** nella casella di testo **Specifica personalizzazione**.

Per questo campo viene fatta distinzione tra lettere maiuscole e minuscole.

- h Fare clic sulla scheda **Risorse macchina**.
- i Verificare che le impostazioni di memoria siano almeno di 2048 MB.

- 5 Modificare loadbalancer-node in modo che vRealize Automation possa eseguire il provisioning di questo componente macchina nell'ambiente.
 - a Fare clic sul componente **loadbalancer-node** nella tela di progettazione.
 - b Selezionare il prefisso macchina dal menu a discesa **Prefisso macchina**.
 - c Fare clic sulla scheda **Informazioni build**.
 - d Selezionare **Cloneworkflow** dal menu a discesa **Provisioning workflow**.
 - e Selezionare il **dukes_bank_template** dal catalogo **Clona da**.
 - f Specificare il **Customspecs_sample** nella casella di testo **Specifica personalizzazione**.
Per questo campo viene fatta distinzione tra lettere maiuscole e minuscole.
 - g Fare clic sulla scheda **Risorse macchina**.
 - h Verificare che le impostazioni di memoria siano almeno di 2048 MB.
- 6 Ripetere per il componente macchina **database-node**.
- 7 Fare clic su **Salva e termina**.
Le modifiche vengono salvate e si ritorna alla scheda **Blueprint**.
- 8 Selezionare il blueprint **DukesBankApplication** e fare clic su **Pubblica**.

Risultati

Il blueprint dell'applicazione campione Dukes Bank è stato configurato per il proprio ambiente e il blueprint completato è stato pubblicato.

Operazioni successive

I blueprint pubblicati non vengono mostrati agli utenti nel catalogo finché non si configura un servizio del catalogo, si aggiunge il blueprint al servizio e si autorizzano gli utenti a richiedere il blueprint. Vedere [Elenco di controllo per la configurazione del catalogo dei servizi](#).

Dopo aver configurato il blueprint Dukes Bank per la visualizzazione nel catalogo, è possibile richiedere di eseguire il provisioning nell'applicazione campione. Vedere [Scenario: test dell'applicazione campione Dukes Bank](#).

Scenario: test dell'applicazione campione Dukes Bank

È possibile richiedere l'elemento di catalogo Dukes Bank e accedere all'applicazione di esempio per verificare il proprio lavoro e constatare il funzionamento dei blueprint di vRealize Automation.

Prerequisiti

- Importare l'applicazione campione Dukes Bank e configurare i componenti del blueprint affinché operino correttamente nell'ambiente esistente. Vedere [Scenario: importazione di Dukes Bank per l'applicazione campione di vSphere e configurazione dell'ambiente](#).

- Configurare il catalogo dei servizi e rendere il blueprint di Dukes Bank pubblicato disponibile per le richieste da parte degli utenti. Vedere [Elenco di controllo per la configurazione del catalogo dei servizi](#).
- Verificare che le macchine virtuali fornite in provisioning possano raggiungere il repository yum.

Procedura

- 1 Accedere alla console di vRealize Automation come utente autorizzato all'elemento di catalogo Dukes Bank.
- 2 Fare clic sulla scheda **Catalogo**.
- 3 Individuare l'elemento di catalogo dell'applicazione campione Dukes Bank e fare clic su **Richiesta**.
- 4 Inserire le informazioni sulla richiesta necessarie per ogni componente indicato da un asterisco rosso.
 - a Passare al componente JBossAppServer per inserire le informazioni sulla richiesta necessarie.
 - b Immettere il nome di dominio completo dell'appliance vRealize Automation nella casella di testo **app_content_server_ip**.
 - c Passare al componente software Dukes_Bank_App per inserire le informazioni sulla richiesta necessarie.
 - d Immettere il nome di dominio completo dell'appliance vRealize Automation nelle caselle di testo **app_content_server_ip**.

- 5 Fare clic su **Invia**.

In base alla rete e all'istanza di vCenter Server corrente, il provisioning completo dell'applicazione campione Dukes Bank può impiegare circa 15-20 minuti. È possibile monitorare lo stato nella scheda **Distribuzioni**. Una volta effettuato il provisioning dell'applicazione, è possibile visualizzare i dettagli dell'elemento del catalogo nella scheda **Distribuzioni**.

- 6 Dopo il provisioning dell'applicazione, individuare l'indirizzo IP del server del bilanciamento del carico in modo da poter accedere all'applicazione campione Dukes Bank.
 - a Fare clic su **Distribuzioni**.
 - b Individuare la distribuzione dell'applicazione campione Dukes Bank e fare clic sul nome della distribuzione.
 - c Nella scheda **Componenti**, selezionare il server di bilanciamento del carico Apache.
 - d Selezionare la scheda **Rete**.
 - e Annotare l'indirizzo IP.

7 Accedere all'applicazione campione Dukes Bank.

- a Passare al server di bilanciamento del carico all'indirizzo `http://IP_Apache_Load_Balancer:8081/bank/main.faces`.

Per accedere direttamente ai server delle applicazioni, passare a `http://IP_AppServer:8080/bank/main.faces`.

- b Immettere **200** nella casella di testo **Nome utente**.
- c Immettere **foobar** nella casella di testo **Password**.

Risultati

Da questo momento l'applicazione campione Dukes Bank è operativa e può essere impiegata come punto di partenza per lo sviluppo dei propri blueprint, come strumento di valutazione di vRealize Automation e come valida risorsa di formazione per apprendere le nozioni fondamentali su funzionalità e componenti di vRealize Automation.

Download e configurazione del blueprint autonomo fornito

È possibile scaricare un blueprint autonomo fornito e i relativi componenti software associati, dall'appliance vRealize Automation.

Il documento [Download e configurazione del blueprint autonomo vRealize Automation](#) illustra come scaricare un blueprint vRealize Automation autonomo dall'appliance vRealize Automation e quindi come importare, configurare e utilizzare tale blueprint in vRealize Automation in combinazione con diversi workflow di vRealize Orchestrator.

Creazione di blueprint e altri contenuti di IaaS in un ambiente con più sviluppatori

Più sviluppatori possono utilizzare i workflow di vRealize Orchestrator insieme a strumenti di sviluppo di vRealize Suite e di terze parti per lavorare contemporaneamente su artefatti diversi di blueprint di vRealize Automation per lo stesso blueprint di vRealize Automation o per blueprint diversi.

È possibile utilizzare strumenti come vRealize Suite Lifecycle Manager per favorire un ambiente con più sviluppatori per vRealize Automation e altri strumenti di vRealize Suite e OVA, nonché strumenti di terze parti come GitLab/GitHub, Houdini e altri artefatti applicativi di [VMware Solutions Exchange](#).

Per ulteriori informazioni sulla creazione di blueprint di vRealize Automation e altri contenuti di IaaS come le proprietà, le sottoscrizioni dei gestori eventi, i componenti software e i workflow di vRealize Orchestrator in un ambiente con più sviluppatori, consultare le seguenti risorse:

- [Video - What's New in Lifecycle Manager](#)
- [Post di blog - vRealize Automation with Infrastructure Blueprint - Configuring Multi-developer Environment](#)
- [Doc - Download e configurazione del blueprint autonomo fornito](#)

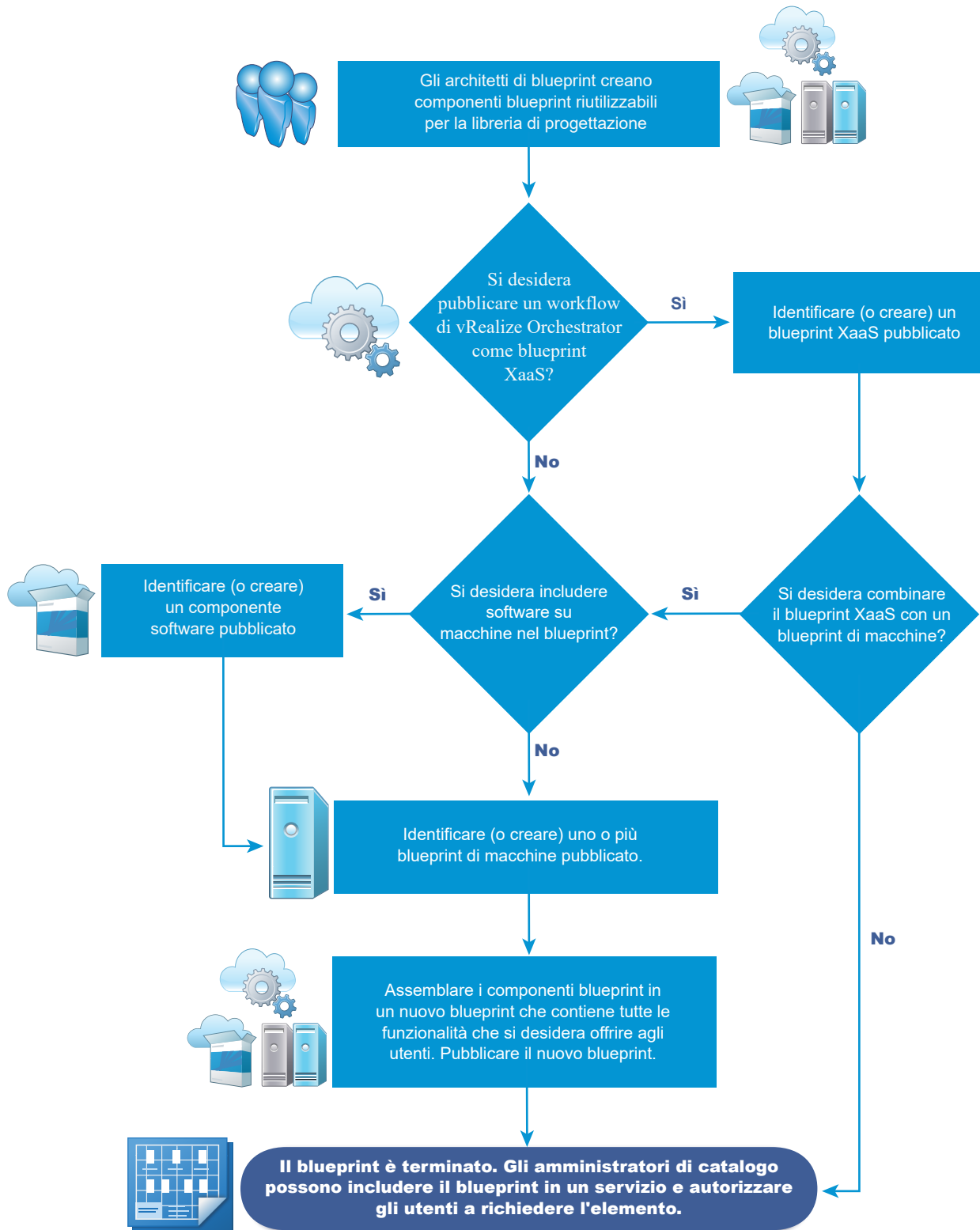
- [Post di blog - Lifecycle Manager with GitLab Integration](#)
- [Post di blog - LifeCycle Manager overview](#)

Assemblaggio di blueprint compositi

I componenti blueprint e i blueprint pubblicati possono essere riutilizzati, combinandoli per creare nuovi pacchetti di servizi IT con cui offrire agli utenti funzionalità articolate.

Se i blueprint del componente dispongono di moduli personalizzati, i moduli di richiesta personalizzati non vengono applicati al nuovo blueprint. Per il nuovo blueprint è necessario creare nuovi moduli. Per ulteriori informazioni sui moduli di richiesta personalizzati, vedere [Personalizzazione dei moduli di richiesta di blueprint](#).

Figura 3-5. Workflow per l'assemblaggio di blueprint compositi



■ Informazioni sul comportamento dei blueprint nidificati

È possibile riutilizzare i blueprint nidificandoli in un altro blueprint come componente. I blueprint vengono nidificati per il riutilizzo e il controllo della modularità nel provisioning delle macchine; tuttavia esistono regole e considerazioni specifiche quando si opera con blueprint nidificati.

- **Utilizzo di componenti macchina e componenti Software durante l'assemblaggio di un blueprint**

Per fornire i componenti di Software, è necessario collocarli sopra i componenti della macchina supportati quando si assemblano blueprint.

- **Creazione di binding di proprietà tra componenti di blueprint**

In diversi scenari di distribuzione, per essere personalizzato, un componente deve avere il valore di proprietà di un altro componente. In un blueprint è possibile effettuare il binding di XaaS, macchine, Software e proprietà personalizzate ad altre proprietà.

- **Creazione di dipendenze e controllo dell'ordine di provisioning**

Se sono necessarie informazioni da uno dei componenti di blueprint per completare il provisioning di un altro componente, è possibile tracciare una dipendenza esplicita sulla tela di progettazione per scaglionare il provisioning in modo da non eseguire il provisioning prematuro del componente dipendente. Le dipendenze esplicite controllano l'ordine di build di una distribuzione e attivano aggiornamenti dipendenti durante un'operazione di scalabilità verticale o orizzontale. I componenti software in un blueprint devono essere ordinati.

Informazioni sul comportamento dei blueprint nidificati

È possibile riutilizzare i blueprint nidificandoli in un altro blueprint come componente. I blueprint vengono nidificati per il riutilizzo e il controllo della modularità nel provisioning delle macchine; tuttavia esistono regole e considerazioni specifiche quando si opera con blueprint nidificati.

Un blueprint contenente uno o più blueprint nidificati viene definito blueprint esterno. Quando si aggiunge un componente blueprint alla tela di progettazione durante la creazione o la modifica di un altro blueprint, il componente blueprint viene chiamato blueprint nidificato, mentre il blueprint contenitore al quale viene aggiunto viene chiamato blueprint esterno.

L'utilizzo dei blueprint nidificati comporta alcune considerazioni che non sono sempre ovvie. Per utilizzare al meglio le funzionalità di provisioning della macchina, è importante comprendere le regole e le considerazioni applicabili.

Regole e considerazioni generali per la nidificazione di blueprint

- Una procedura consigliata per ridurre al minimo la complessità dei blueprint consiste nel limitare i blueprint a una profondità di tre livelli, impostando il blueprint principale come uno dei tre livelli.
- Se un utente è autorizzato ad accedere al blueprint esterno, tale utente è autorizzato ad accedere ai relativi blueprint nidificati.

- È possibile applicare un criterio di approvazione a un blueprint. In seguito all'approvazione, l'elemento di catalogo del blueprint e tutti i relativi componenti, inclusi i blueprint nidificati, vengono sottoposti a provisioning. È anche possibile applicare criteri di approvazione differenti ai diversi componenti. Perché il blueprint richiesto venga sottoposto a provisioning è necessario che tutti i criteri di approvazione vengano approvati.
- Quando si modifica un blueprint pubblicato, non si modificano le distribuzioni già sottoposte a provisioning utilizzando tale blueprint. In questa fase, la distribuzione risultante legge i valori correnti del blueprint, inclusi quelli dei blueprint nidificati. Le uniche modifiche che è possibile convalidare a distribuzioni sottoposte a provisioning sono quelle apportate ai componenti software, ad esempio le modifiche per aggiornare o disinstallare script.
- Le impostazioni definite nel blueprint esterno sovrascrivono le impostazioni configurate nei blueprint nidificati con le seguenti eccezioni:
 - È possibile modificare il nome di un blueprint nidificato, ma non il nome di un componente macchina, o di qualsiasi altro componente, all'interno di un blueprint nidificato.
 - Non è possibile aggiungere o eliminare le proprietà personalizzate di un componente macchina in un blueprint nidificato. È tuttavia possibile modificare tali proprietà. Non è possibile aggiungere, modificare o eliminare i gruppi di proprietà di un componente macchina in un blueprint nidificato.
- Le modifiche apportate dall'utente o da un altro architetto alle impostazioni di blueprint nidificati vengono visualizzate nei blueprint esterni, a meno che tali impostazioni non siano state sovrascritte nel blueprint esterno.
- Limitare la durata massima del lease nel blueprint esterno al valore massimo del lease più basso del blueprint di un componente.

Mentre la durata del lease specificata in un blueprint nidificato e nel blueprint esterno può essere impostata su qualsiasi valore, la durata massima del lease nel blueprint esterno dovrebbe essere limitata al valore massimo del lease più basso di un blueprint nidificato. Questo consente all'architetto dell'applicazione di progettare un blueprint composito con valori di lease uniformi e variabili, ma all'interno dei vincoli individuati dall'architetto dell'infrastruttura. Se il valore massimo del lease definito in un blueprint nidificato è inferiore a quello definito nel blueprint esterno, la richiesta di provisioning non riesce.

- Quando si lavora in un blueprint esterno, è possibile sovrascrivere le impostazioni Risorse macchina configurate per un componente macchina in un blueprint nidificato.
- Quando si lavora in un blueprint esterno, è possibile trascinare un componente software in un componente macchina all'interno di un blueprint nidificato.
- Se si apre un blueprint in cui è stato rimosso un componente di una macchina in un blueprint nidificato o è stato modificato l'ID corrispondente e il componente della macchina era associato a componenti nel blueprint corrente, i componenti associati vengono rimossi e viene visualizzato un messaggio simile al seguente:

Il componente di una macchina in un blueprint nidificato associato a componenti nel blueprint corrente è stato rimosso oppure il relativo ID del componente della macchina è stato modificato. Tutti i componenti nel blueprint corrente associati all'ID del componente della macchina mancante o modificato sono stati rimossi. Fare clic su Annulla per mantenere la cronologia di associazioni tra l'ID del componente della macchina mancante o modificato nel blueprint nidificato e i componenti nel blueprint corrente, quindi risolvere il problema nel blueprint nidificato. Aprire il blueprint nidificato e aggiungere di nuovo il componente della macchina mancante con l'ID originale oppure modificare l'ID del componente della macchina riportandolo all'ID originale. Fare clic su Salva per rimuovere l'intera cronologia di associazioni tra l'ID del componente della macchina mancante o modificato nel blueprint nidificato e i componenti nel blueprint corrente.

- Quando si pubblica un blueprint, i dati del componente software vengono gestiti come uno snapshot. Se in un momento successivo si modificano le proprietà del componente software, solo le nuove proprietà vengono riconosciute dal blueprint in cui si trova il componente software. Le modifiche apportate alle proprietà presenti nel componente software al momento della pubblicazione del blueprint non vengono applicate nel blueprint. Solo le proprietà aggiunte dopo la pubblicazione del blueprint vengono ereditate dal blueprint. Tuttavia, è possibile apportare modifiche alle istanze del componente software nel blueprint in cui si trova il componente software per modificare tale blueprint specifico.

Regole e considerazioni dei servizi di rete e sicurezza per i blueprint nidificati

- Tutti i componenti dei servizi di rete e sicurezza nei blueprint esterni possono essere associati alle macchine definite nei blueprint nidificati.
- Rete, sicurezza e componenti di bilanciamento del carico di NSX e le loro impostazioni non sono supportati nei blueprint nidificati.
- Quando viene applicato l'isolamento app nel blueprint esterno, questo sovrascrive le impostazioni di isolamento app specificate nei blueprint nidificati.
- Le impostazioni della zona di trasporto definite nel blueprint esterno sovrascrivono le impostazioni della zona di trasporto specificate nei blueprint nidificati.
- Quando si lavora in un blueprint esterno, è possibile configurare le impostazioni di bilanciamento del carico relative alle impostazioni dei componenti di rete e dei componenti macchina che sono configurate in un blueprint interno o nidificato.
- Per un blueprint nidificato che contiene un componente di rete NAT su richiesta, gli intervalli IP specificati in tale componente non sono modificabili nel blueprint esterno.
- Il blueprint esterno non può contenere un blueprint interno contenente a sua volta delle impostazioni di rete su richiesta o delle impostazioni del bilanciamento del carico su richiesta. L'utilizzo di un blueprint interno contenente un componente di rete su richiesta NSX o un componente del bilanciamento del carico NSX non è supportato.

- Per un blueprint nidificato che contiene componenti di rete o sicurezza NSX, non è possibile modificare le informazioni sul profilo di rete o sui criteri di sicurezza specificate nel blueprint nidificato. È tuttavia possibile riutilizzare queste impostazioni per altri componenti della macchina vSphere aggiunti al blueprint esterno.
- Per garantire che i componenti di rete e di sicurezza NSX nei blueprint nidificati abbiano un nome univoco in un blueprint composito, vRealize Automation antepone l'ID dei blueprint nidificati ai nomi dei componenti di rete e sicurezza che non sono univoci. Se, ad esempio, si aggiunge un blueprint con il nome ID xbp_1 a un blueprint esterno ed entrambi i blueprint contengono un componente gruppo di sicurezza su richiesta chiamato OD_Security_Group_1, il componente nel blueprint nidificato viene rinominato xbp_1_OD_Security_Group_1 nella tela di progettazione del blueprint. Ai nomi dei componenti di rete e sicurezza nel blueprint esterno non viene aggiunto alcun prefisso.
- Le impostazioni dei componenti possono cambiare in base al blueprint in cui si trova il componente. Se ad esempio si includono gruppi di sicurezza, tag di sicurezza o reti su richiesta a entrambi i livelli del blueprint interno ed esterno, le impostazioni nel blueprint esterno sovrascrivono quelle del blueprint interno. I componenti rete e sicurezza sono supportati solo al livello del blueprint esterno, eccetto per le reti esistenti che funzionano al livello del blueprint interno. Per evitare problemi, aggiungere tutti i gruppi di sicurezza, i tag di sicurezza e le reti su richiesta solo al blueprint esterno.

Considerazioni dei componenti software per i blueprint nidificati

Nel caso di blueprint scalabili, si consiglia di creare singoli blueprint di layer che non riutilizzino altri blueprint. In genere, i processi di aggiornamento durante le operazioni di scalabilità vengono attivati da dipendenze implicite come le dipendenze create quando si associa una proprietà software a una proprietà di macchina. Tuttavia, le dipendenze implicite in un blueprint nidificato non attivano sempre processi di aggiornamento. Se è necessario utilizzare blueprint nidificati in un blueprint scalabile, è possibile tracciare manualmente dipendenze tra i componenti nel blueprint nidificato per creare dipendenze esplicite che attivano sempre un aggiornamento.

Utilizzo di componenti macchina e componenti Software durante l'assemblaggio di un blueprint

Per fornire i componenti di Software, è necessario collocarli sopra i componenti della macchina supportati quando si assemblano blueprint.

Per supportare i componenti Software, il blueprint della macchina selezionato deve contenere un componente macchina basato su un modello, uno snapshot o un'immagine della macchina Amazon che contiene l'agente guest e l'agente bootstrap del Software e deve utilizzare un metodo di provisioning supportato.

Poiché gli agenti Software non supportano il protocollo IP versione 6 (IPv6), utilizzare le impostazioni IPv4.

Nota I componenti software nel blueprint devono avere una dipendenza ordinata. Componenti software non ordinati possono infatti impedire il provisioning corretto del blueprint. Se per i componenti software non è presente alcuna dipendenza di ordine effettiva, è possibile soddisfare il requisito relativo all'ordine dei blueprint aggiungendo una dipendenza fittizia tra i componenti software.

Se si progettano blueprint in modo che siano scalabili, si consiglia di creare singoli blueprint di layer che non riutilizzino altri blueprint. Normalmente, i processi di aggiornamento utilizzati durante le operazioni di scalabilità vengono attivati da dipendenze implicite come i binding di proprietà. Tuttavia, le dipendenze implicite in un blueprint nidificato non attivano sempre processi di aggiornamento.

Mentre gli architetti IaaS, gli architetti delle applicazioni e gli architetti dei software possono tutti assemblare blueprint, solo gli architetti IaaS possono configurare i componenti macchina. Se l'utente non è un architetto IaaS, non può configurare i propri componenti macchina, ma può riutilizzare i blueprint delle macchine che l'architetto IaaS ha creato e pubblicato.

Per aggiungere correttamente componenti software alla tela di progettazione, è inoltre necessario poter accedere al catalogo target con ruolo di membro del gruppo di business, amministratore del gruppo di business o amministratore tenant.

Se è necessario utilizzare blueprint nidificati in un blueprint scalabile, è possibile tracciare manualmente dipendenze tra i componenti nel blueprint nidificato per creare dipendenze esplicite che attivano sempre un aggiornamento.

Nota Quando si pubblica un blueprint, i dati del componente software vengono gestiti come uno snapshot. Se in un momento successivo si modificano le proprietà del componente software, solo le nuove proprietà vengono riconosciute dal blueprint in cui si trova il componente software. Le modifiche apportate alle proprietà presenti nel componente software al momento della pubblicazione del blueprint non vengono applicate nel blueprint. Solo le proprietà aggiunte dopo la pubblicazione del blueprint vengono ereditate dal blueprint. Tuttavia, è possibile apportare modifiche alle istanze del componente software nel blueprint in cui si trova il componente software per modificare tale blueprint specifico.

Tabella 3-64. Metodi di provisioning che supportano Software

Tipo di macchina	Metodo di provisioning
vSphere	Clona
vSphere	Clone collegato
vCloud Director	Clona
vCloud Air	Clona
Amazon Web Services	Immagine macchina Amazon

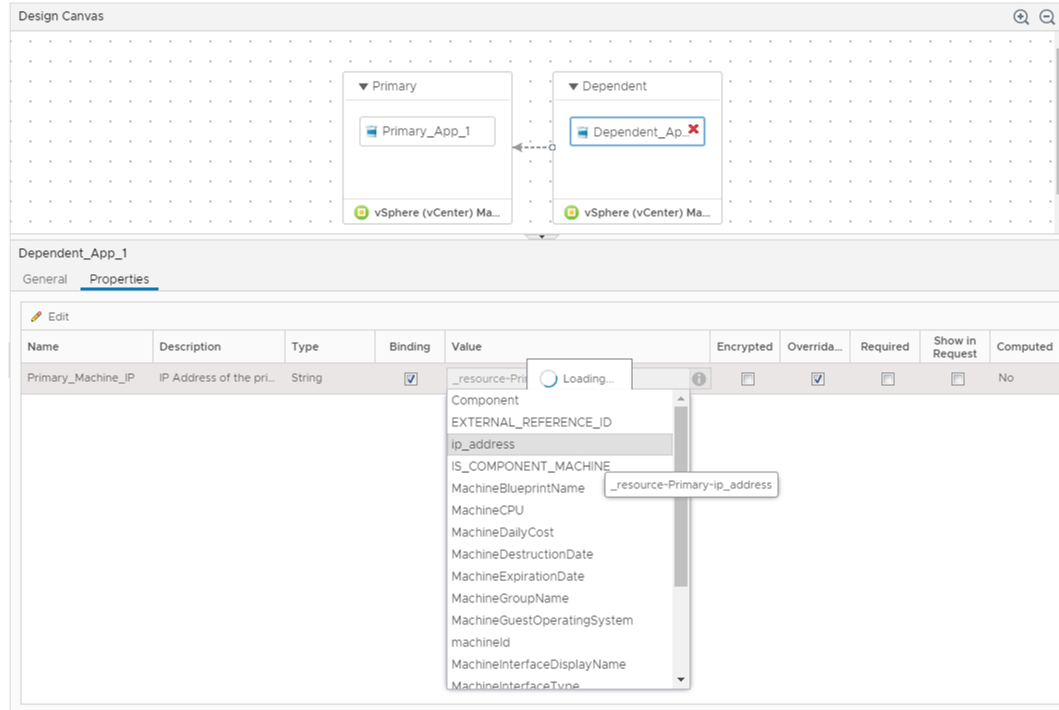
Creazione di binding di proprietà tra componenti di blueprint

In diversi scenari di distribuzione, per essere personalizzato, un componente deve avere il valore di proprietà di un altro componente. In un blueprint è possibile effettuare il binding di XaaS, macchine, Software e proprietà personalizzate ad altre proprietà.

Si supponga, ad esempio, che l'architetto del software modifichi le definizioni delle proprietà negli script del ciclo di vita di un componente WAR. Un componente WAR richiede il percorso di installazione del componente server Apache Tomcat. L'architetto del software configura quindi il componente WAR in modo che il valore della proprietà `server_home` sia impostato sul valore della proprietà `install_path` del server Apache Tomcat. Per il corretto provisioning del componente Software, l'architetto che assembla il blueprint deve eseguire il binding della proprietà `server_home` alla proprietà `install_path` del server Apache Tomcat.

I binding delle proprietà vengono impostati durante la configurazione dei componenti in un blueprint. Nella pagina Blueprint, trascinare il componente sulla tela e fare clic sulla scheda **Proprietà**. Per eseguire il binding di una proprietà a un'altra proprietà in un blueprint, selezionare la casella di controllo **Binding**. Immettere *ComponentName~PropertyName* nella casella di testo del valore, oppure utilizzare la freccia in giù per generare un elenco delle opzioni di binding disponibili. Utilizzare il carattere tilde (~) come delimitatore tra componenti e proprietà. Ad esempio, per eseguire il binding alla proprietà `dp_port` nel componente software MySQL, digitare `mysql~db_port`. Per eseguire il binding a proprietà configurate durante il provisioning, come l'indirizzo IP di una macchina o il nome host di un componente Software, immettere `_resource~ComponentName~PropertyName`. Ad esempio, per seguire il binding al nome della prenotazione di una macchina, immettere `_resource~vSphere_Machine_1~MachineReservationName`.

Figura 3-6. Binding di una proprietà software all'indirizzo IP di una macchina



Creazione di dipendenze e controllo dell'ordine di provisioning

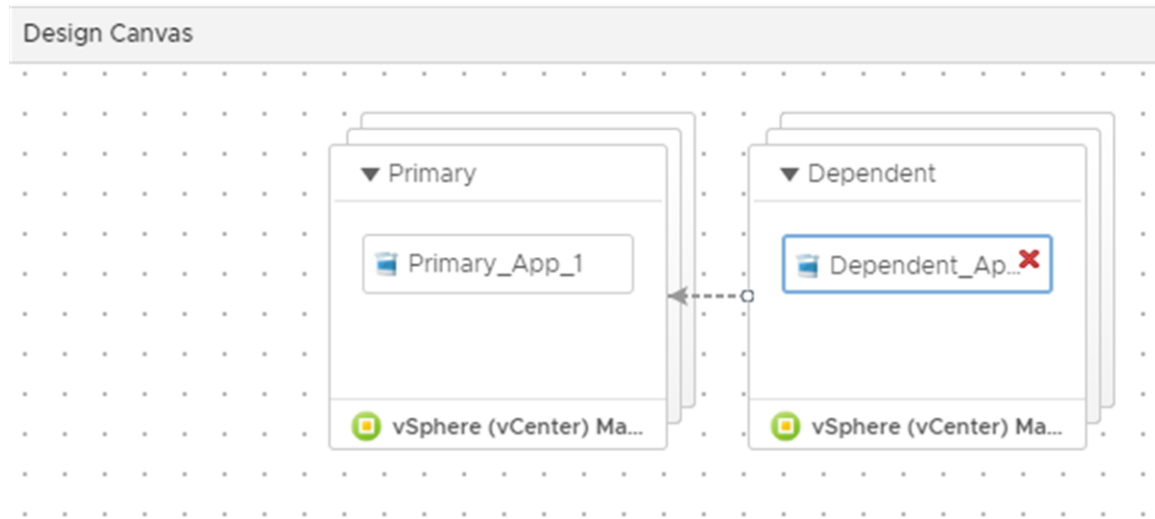
Se sono necessarie informazioni da uno dei componenti di blueprint per completare il provisioning di un altro componente, è possibile tracciare una dipendenza esplicita sulla tela di progettazione per scaglionare il provisioning in modo da non eseguire il provisioning prematuro del componente dipendente. Le dipendenze esplicite controllano l'ordine di build di una distribuzione e attivano aggiornamenti dipendenti durante un'operazione di scalabilità verticale o orizzontale. I componenti software in un blueprint devono essere ordinati.

Quando si progettano blueprint con più macchine e applicazioni, potrebbero essere presenti proprietà che è necessario ottenere da una macchina per terminare l'installazione di un'applicazione in un'altra. Ad esempio, se si sta generando un server Web, potrebbe essere necessario il nome host del server di database prima di poter installare l'applicazione e creare istanze delle tabelle del database. Se si mappa una dipendenza esplicita, il server di database avvia il provisioning quando il server Web termina il provisioning.

Nota I componenti software nel blueprint devono avere una dipendenza ordinata. Componenti software non ordinati possono infatti impedire il provisioning corretto del blueprint. Se per i componenti software non è presente alcuna dipendenza di ordine effettiva, è possibile soddisfare il requisito relativo all'ordine dei blueprint aggiungendo una dipendenza fittizia tra i componenti software.

Per mappare una dipendenza nelle tele di progettazione, è necessario tracciare una riga dal componente dipendente al componente dal quale si dipende. Al termine, il componente che si desidera generare per secondo presenterà una freccia che punta al componente che si desidera generare per primo. Ad esempio, nella figura Controllo dell'ordine di creazione mediante mappatura delle dipendenze, il provisioning della macchina dipendente viene eseguito solo dopo la creazione della macchina principale. In alternativa, è possibile configurare entrambe le macchine in modo che il provisioning venga eseguito simultaneamente ma tracciando una dipendenza tra i componenti software.

Figura 3-7. Controllo dell'ordine di creazione mediante mappatura delle dipendenze



Se si progettano blueprint in modo che siano scalabili, si consiglia di creare singoli blueprint di layer che non riutilizzino altri blueprint. In genere, i processi di aggiornamento durante le operazioni di scalabilità vengono attivati da dipendenze implicite come le dipendenze create quando si associa una proprietà software a una proprietà di macchina. Tuttavia, le dipendenze implicite in un blueprint nidificato non attivano sempre processi di aggiornamento. Se è necessario utilizzare blueprint nidificati in un blueprint scalabile, è possibile tracciare manualmente dipendenze tra i componenti nel blueprint nidificato per creare dipendenze esplicite che attivano sempre un aggiornamento.

Personalizzazione dei moduli di richiesta di blueprint

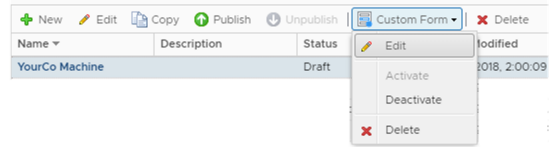
Ogni blueprint creato e pubblicato visualizza un modulo quando gli utenti richiedono il blueprint nel catalogo. È possibile utilizzare il modulo predefinito oppure personalizzare i moduli di richiesta di blueprint quando si crea o si modifica un blueprint. È consigliabile personalizzare un modulo quando le informazioni specificate o necessarie nel modulo predefinito non sono quelle che si desidera fornire agli utenti.

Personalizzazione dei moduli di richiesta

È possibile accedere al designer dei moduli di richiesta personalizzati dalla griglia dati del blueprint o dalla tela del blueprint.

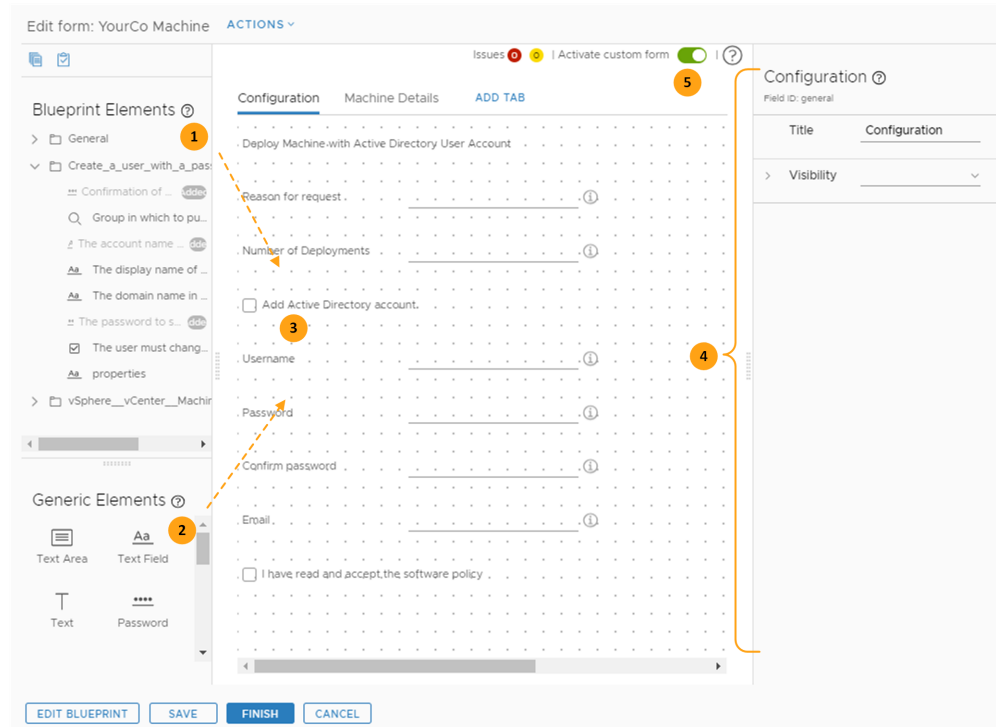
Blueprints

Create and manage blueprints. Publish a blueprint to allow architects to reuse your blueprint, administrators to entitle users to request your blueprint from the catalog.



Designer dei moduli di richiesta personalizzati

Utilizzare il designer dei moduli per creare il modulo personalizzato.



Per creare un modulo personalizzato:

- 1 Trascinare gli elementi (1 e 2) nella tela di progettazione (3).
- 2 Configurare ciascun elemento utilizzando il riquadro delle proprietà (4).
- 3 Attivare il modulo (5).

A meno che non sia configurata una proprietà che vieti la sovrascrittura, l'elenco degli elementi del blueprint include proprietà personalizzate. Se l'opzione di sovrascrittura della proprietà è impostata su no, il campo non è idoneo per la personalizzazione.

Convalida e vincoli

Il designer dei moduli personalizzati supporta la convalida dei dati aggiungendo vincoli a un campo o utilizzando un'origine di convalida esterna. Per le opzioni dei vincoli che vengono applicate quando si crea un modulo, vedere [Proprietà personalizzate dei campi di designer modulo](#).

- Per un esempio di vincolo, vedere [Creazione di un modulo di richiesta personalizzato con opzioni di Active Directory](#).
- Per la convalida esterna, vedere [Utilizzo della convalida esterna nel designer di moduli personalizzati](#).

Quando si aggiungono la convalida e le dipendenze nei moduli, l'utente richiedente deve fornire oppure il sistema deve convalidare i campi; in caso contrario, i campi dipendenti potrebbero non essere visualizzati nel modulo.

Ad esempio, se sono presenti campi nella prima scheda da cui dipendono i campi successivi, è possibile che i campi dipendenti non vengano visualizzati nelle schede successive finché non si specifica il valore dipendente nelle schede precedenti.

Azioni dei moduli di richiesta personalizzati

Utilizzare le voci del menu Azioni per popolare i moduli e condividerli con altri sistemi.

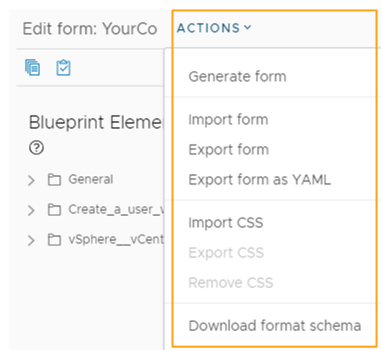


Tabella 3-65. Voci del menu Azioni del modulo di richiesta personalizzato

Voce del menu Azioni	Descrizione
Genera modulo	<p>Consente di aggiungere al designer modulo tutti i campi associati a ciascun componente del blueprint. Ciascun componente viene aggiunto a una scheda. Se si utilizza questa voce di menu dopo aver creato o modificato un modulo, il modulo generato sovrascrive il modulo corrente.</p> <p>Se si utilizza questa voce di menu, è possibile nascondere o rimuovere i campi che non si desidera fornire agli utenti nel catalogo. Se non si genera il modulo, è comunque possibile aggiungere e configurare le caselle di testo che si desidera siano visibili per gli utenti.</p>
Importa modulo	Importa un file JSON o YAML di modulo personalizzato.

Tabella 3-65. Voci del menu Azioni del modulo di richiesta personalizzato (continua)

Voce del menu Azioni	Descrizione
Esporta modulo	Esporta il modulo personalizzato corrente come file JSON. Esportare il file quando si desidera utilizzarne la parte che corrisponde a un componente utilizzato in un altro blueprint.
Esporta modulo come YAML	Esporta il modulo personalizzato corrente come file YAML. Esportare il file come file YAML quando si desidera spostare un modulo personalizzato da un'istanza di vRealize Automation a un'altra, ad esempio dall'ambiente di prova all'ambiente di produzione. Se si preferisce modificare il modulo come file YAML, è possibile esportare il modulo, modificarlo e quindi importarlo nuovamente nel blueprint.
Importa CSS	<p>Importa un file CSS che migliora il modulo di richiesta del catalogo.</p> <p>Questo file può essere simile all'esempio seguente. In questo esempio viene modificata la dimensione del carattere e il testo viene reso grassetto. Il campo a cui si fa riferimento è Distribuisci macchina con account utente di Active Directory visualizzato nell'immagine che si trova nella sezione Designer dei moduli di richiesta personalizzati precedente.</p> <pre>#<field-ID> .grid-item { font-size: 16px; font-weight: bold; width: 600px; }</pre> <p>In questo esempio, <field-ID> è l'ID per il campo nella tela. Per individuare il valore, selezionare il campo nella tela. Il valore si trova nel riquadro a destra, sotto al nome. Nell'immagine precedente, il valore è text_d947bc97. Per importare il file: Salvarlo come <filename>.css.</p>
Esporta CSS	Esporta il file CSS importato.
Rimuovi CSS	Elimina il file CSS personalizzato. Il file CSS eliminato non può essere recuperato.
Scarica schema formato	<p>Scarica un file JSON che contiene la struttura e la descrizione dei controlli, nonché gli stati utilizzati in un modulo personalizzato.</p> <p>È possibile utilizzare questo schema per creare un modulo o modificare un modulo esistente. È possibile importare il file JSON modificato come modulo personalizzato.</p>

Creazione di un modulo di richiesta personalizzato con opzioni di Active Directory

L'utente che effettua la richiesta crea un modulo personalizzato nel caso in cui il modulo predefinito contenga un numero eccessivo o insufficiente di informazioni. Nel modulo è possibile aggiungere o nascondere campi, oppure precompilare i campi e scegliere di mostrarli o nasconderli.

Questo caso d'uso si basa su un blueprint contenente un tipo di macchina virtuale vSphere e un blueprint XaaS che configura un account amministratore di Active Directory nella macchina virtuale. Il blueprint XaaS si basa sul workflow di creazione di un utente con una password in un gruppo.

L'obiettivo in questo caso d'uso è:

- Fornire all'utente la possibilità di configurare la password amministratore.
- Preconfigurare i dettagli della macchina in modo che i valori di CPU e memoria siano entrambi espressi in GB.

Questo caso d'uso include esempi delle seguenti personalizzazioni del modulo:

- Aggiunta di campi specifici a un modulo vuoto.
- Configurazione di una casella di controllo Mostra/Nascondi.
- Come nascondere i campi finché l'utente che effettua la richiesta non seleziona una casella di controllo.
- Aggiunta della convalida ai campi.
- Visualizzazione di un campo della memoria in GB anche se il campo del blueprint è espresso in MB.
- Utilizzo di espressioni regolari.

Prerequisiti

- Accedere a vRealize Automation come **architetto dell'applicazione, architetto del software o architetto dell'infrastruttura**.
- Creare un blueprint della macchina e dell'utente dell'azienda che includa un blueprint vSphere e un blueprint XaaS per creare un account utente di Active Directory con una password in un gruppo. Per un esempio, vedere [Creazione di un blueprint di XaaS per la creazione di un utente](#).

Procedura

- 1 Scegliere **Progettazione > Blueprint**.
- 2 Evidenziare la riga contenente il blueprint della macchina e dell'utente dell'azienda, quindi fare clic su **Modulo personalizzato > Modifica**.

- 3 Rinominare la scheda Generale.
 - a Fare clic sulla scheda.
 - b Nella proprietà **Titolo** nel riquadro a destra, immettere **Configuration**.
- 4 Nella nuova scheda Configuration, aggiungere i seguenti campi e configurarli con i valori specificati.

The screenshot shows the vRealize Automation form editor. The main window is titled "Edit form: YourCo Machine". On the left, there are two panels: "Blueprint Elements" and "Generic Elements". The "Blueprint Elements" panel shows a tree structure with "General" and "vSphere_vCenter_Machine" folders. The "Generic Elements" panel shows a list of form elements: Text Area, Text Field, Text, and Password. The main area displays a form with the following fields: "Deploy Machine with Active Directory User Account", "Reason for request", "Number of Deployments", "Add Active Directory account", "Username", "Password", "Confirm password", "Email", and a checkbox for "I have read and accept the software policy". The right sidebar shows the "Configuration" tab with a "Title" field set to "Configuration" and a "Visibility" dropdown.

Nei campi Aspetto, Valori e Vincoli, utilizzare i valori specificati.

In questo modo, è possibile evitare eventuali errori durante la creazione del modulo.

Campo nella screenshot	Origine dell'elemento blueprint	Aspetto	Valori	Vincoli
Deploy Machine with Active Directory User Account (Distribuisci macchina con account utente di Active Directory)	Elementi generici > Testo	Etichetta e tipo <ul style="list-style-type: none"> ■ Tipo di visualizzazione = Testo Visibilità <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Visibile = Sì 	Valore predefinito <ul style="list-style-type: none"> ■ Valore predefinito = Deploy Machine with Active Directory User Account (Distribuisci macchina con account utente di Active Directory) ■ Origine valore = Costante 	
Reason for Request (Motivo della richiesta)	Elementi blueprint > vSphere_vCenter_Machine > Descrizione	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Motivo della richiesta ■ Tipo di visualizzazione = Campo testo Visibilità <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Visibile = Sì Sola lettura <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Sola lettura = No Guida personalizzata <ul style="list-style-type: none"> ■ Guida indicazioni = Specificare il motivo della richiesta. 		Obbligatorio <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Obbligatorio = Sì

Campo nella screenshot	Origine dell'elemento blueprint	Aspetto	Valori	Vincoli
Number of Deployments (Numero di distribuzioni)	Elementi blueprint > Generale > Numero di distribuzioni	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Numero di distribuzioni ■ Tipo di visualizzazione = Intero Visibilità <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Visibile = Sì Sola lettura <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Sola lettura = No Guida personalizzata <ul style="list-style-type: none"> ■ Guida indicazioni = Selezionare il numero di istanze del blueprint da distribuire. 	Valore predefinito <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Valore predefinito = 1 	Obbligatorio <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Obbligatorio = Sì Valore minimo <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Valore minimo = 1
Casella di controllo Add Active Directory account (Aggiungi account di Active Directory)	Elementi generici > Casella di controllo	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Aggiungi account di Active Directory ■ Tipo di visualizzazione = Casella di controllo Visibilità <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Visibile = Sì 		

Campo nella screenshot	Origine dell'elemento blueprint	Aspetto	Valori	Vincoli
Username	Elementi blueprint > Crea utente con una password in un gruppo > Nome dell'account utente	<p>Etichetta e tipo</p> <ul style="list-style-type: none"> ■ Etichetta = Nome utente ■ Tipo di visualizzazione = Campo testo <p>Visibilità</p> <hr/> <p>Nota Questa proprietà di visibilità, configurata nello stesso modo nei campi successivi, consente di nascondere il campo a meno che non sia selezionata la casella di controllo Aggiungi account di Active Directory.</p> <hr/> <ul style="list-style-type: none"> ■ Origine valore = Valore condizionale ■ Espressione = Impostare il valore = Sì <p>Se Aggiungi account di Active Directory è uguale a Sì</p> <p>Guida personalizzata</p> <ul style="list-style-type: none"> ■ Guida indicazioni = Specificare il nome utente dell'amministratore. 	<p>Valore predefinito</p> <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Valore predefinito = admin 	<p>Obbligatorio</p> <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Obbligatorio = Sì <p>Espressione regolare</p> <hr/> <p>Nota Le espressioni regolari devono utilizzare la sintassi JavaScript.</p> <hr/> <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Espressione regolare = "[a-z]*\$" ■ Messaggio di errore convalida = Il nome utente non può contenere caratteri speciali o numeri.

Campo nella screenshot	Origine dell'elemento blueprint	Aspetto	Valori	Vincoli
Password	Elementi blueprint > Crea utente con una password in un gruppo > Password da impostare per il nuovo account creato	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Password ■ Tipo di visualizzazione = Password Visibilità <ul style="list-style-type: none"> ■ Origine valore = Valore condizionale ■ Espressione = Impostare il valore = Sì Se Aggiungi account di Active Directory è uguale a Sì Guida personalizzata <ul style="list-style-type: none"> ■ Guida indicazioni = Specificare la password dell'account amministratore. 		Obbligatorio <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Obbligatorio = Sì Espressione regolare <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Espressione regolare = <code>"^(?=.*[A-Z])(?=.*[0-9])(?=.*[a-z]).{8,}\$"</code> ■ Messaggio = La password amministratore deve includere almeno otto caratteri e può contenere caratteri alfanumerici e speciali.
Confirm password (Conferma password)	Elementi blueprint > Crea utente con una password in un gruppo > Conferma della password	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Conferma password Tipo di visualizzazione = Password Visibilità <ul style="list-style-type: none"> ■ Origine valore = Valore condizionale ■ Espressione = Imposta valore su Sì Se Aggiungi account di Active Directory è uguale a Sì Guida personalizzata <ul style="list-style-type: none"> ■ Guida indicazioni = Immettere nuovamente la password dell'account amministratore. 		Obbligatorio <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Obbligatorio = Sì Trova una corrispondenza per il campo <ul style="list-style-type: none"> ■ Trova una corrispondenza per il campo = Password

Campo nella screenshot	Origine dell'elemento blueprint	Aspetto	Valori	Vincoli
Email	Elementi generici > Campo testo	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Email ■ Tipo di visualizzazione = Campo testo Visibilità <ul style="list-style-type: none"> ■ Origine valore = Valore condizionale ■ Espressione = Impostare il valore = Sì Se Aggiungi account di Active Directory è uguale a Sì Guida personalizzata <ul style="list-style-type: none"> ■ Guida indicazioni = Specificare l'indirizzo email dell'amministratore. 	Valore predefinito <ul style="list-style-type: none"> ■ Origine valore = Valore elaborato ■ Operatore = Concatena ■ Aggiungi valore = Campo Selezionare il nome utente ■ Aggiungi valore = Costante Immettere @yourco.com 	Espressione regolare <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Espressione regolare = "[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$" ■ Messaggio di errore convalida = Specificare un indirizzo email valido.
Casella di controllo I have read and accept the software policy (Ho letto e accetto i termini di utilizzo del software)	Elementi generici > Casella di controllo	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta elemento = Ho letto e accetto i termini di utilizzo del software ■ Tipo di visualizzazione = Casella di controllo Visibilità <ul style="list-style-type: none"> ■ Origine valore = Valore condizionale ■ Espressione = Impostare il valore = Sì Se Aggiungi account di Active Directory è uguale a Sì 		

- 5 Fare clic su **Aggiungi scheda** e immettere **Machine Details** nella proprietà **Titolo** sulla destra.

6 Nella scheda Machine Details, configurare i campi illustrati di seguito.

The screenshot shows the 'Machine Details' configuration form in vRealize Automation. The form is titled 'Machine Details' and has a 'Field ID: page_039f8ffc'. The 'Storage (GB)' field is highlighted. The form also includes a 'Visibility' dropdown set to 'Yes'. The left sidebar shows 'Blueprint Elements' and 'Generic Elements'.

Nei campi Aspetto, Valori e Vincoli, utilizzare i valori specificati.

Campo nella screenshot	Origine elementi blueprint	Aspetto	Valori	Vincoli
Storage (GB)	Elementi blueprint > vSphere_vCenter_Machine > Storage (GB)	Etichetta e tipo <ul style="list-style-type: none"> Etichetta = Storage (GB) Tipo di visualizzazione = Intero Visibilità <ul style="list-style-type: none"> Origine valore = Costante Visibilità = Sì Sola lettura <ul style="list-style-type: none"> Origine valore = Costante Sola lettura = No 	Valore predefinito <ul style="list-style-type: none"> Origine valore = Costante Valore predefinito = 4 	Valore minimo <ul style="list-style-type: none"> Origine valore = Costante Valore minimo = 2
Number of CPUs (Numero di CPU)	Elementi blueprint > vSphere_vCenter_Machine > CPU	Etichetta e tipo <ul style="list-style-type: none"> Etichetta = Numero di CPU Tipo di visualizzazione = Intero Visibilità <ul style="list-style-type: none"> Origine valore = Costante Visibilità = Sì 	Valore predefinito <ul style="list-style-type: none"> Origine valore = Costante Valore predefinito = 1 	Valore minimo <ul style="list-style-type: none"> Origine valore = Costante Valore minimo = 1

Campo nella screenshot	Origine elementi blueprint	Aspetto	Valori	Vincoli
Memoria (GB)	Elementi generici > Intero	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Memoria (GB) ■ Tipo di visualizzazione = Intero Visibilità <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Visibilità = Sì 	Valore predefinito <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Valore predefinito = 1 	Valore minimo <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Valore minimo = 1
Memoria (MB)	Elementi blueprint > vSphere_vCenter_Machine > Memoria (MB)	Etichetta e tipo <ul style="list-style-type: none"> ■ Etichetta = Memoria (MB) ■ Tipo di visualizzazione = Intero Visibilità <ul style="list-style-type: none"> ■ Origine valore = Costante ■ Visibilità = No 	Valore predefinito <ul style="list-style-type: none"> ■ Origine valore = Valore elaborato ■ Operatore = Moltiplica ■ Aggiungi valore = Campo Seleziona memoria (GB) ■ Aggiungi valore = Costante Immettere 1024 	

- 7 Correggere eventuali errori. È possibile salvare il modulo, ma non è possibile attivarlo finché sono presenti errori.
- 8 Per salvare il modulo e chiudere il designer modulo, fare clic su **Fine**.
- 9 Selezionare il blueprint e fare clic su **Pubblica**.
- 10 Per rendere disponibile il modulo personalizzato quando gli utenti richiedono l'elemento nel catalogo dei servizi, nella barra degli strumenti della pagina Blueprint, selezionare **Modulo personalizzato > Attiva**.

Operazioni successive

- Rendere disponibile il blueprint nel catalogo dei servizi. Vedere [Gestione del catalogo dei servizi](#).
- Nel catalogo, verificare che il modulo di richiesta sia simile a quello illustrato nell'esempio seguente.

Two overlapping screenshots of the vRealize Automation configuration interface. The top screenshot shows the 'Machine Details' tab with fields for Storage (GB) set to 4, Number of CPUs set to 1, and Memory (GB) set to 1. The bottom screenshot shows the 'Configuration' tab with fields for Reason for request, Number of Deployments (set to 1), Username (set to admin), Password, Confirm password, and Email (set to admin@yourco.com). A checkbox 'Add Active Directory account' is checked. Both screenshots have 'SUBMIT' and 'CANCEL' buttons at the bottom.

Proprietà personalizzate dei campi di designer modulo

Le proprietà dei campi determinano l'aspetto del campo selezionato e i valori predefiniti che vengono visualizzati. Inoltre, determinano le regole da applicare al campo per garantire che l'utente specifichi una voce valida nel modulo di richiesta del catalogo in vRealize Automation.

Ciascun campo deve essere configurato singolarmente. Selezionare il campo e modificarne le proprietà.

Aspetto del campo

Le proprietà dell'aspetto consentono di determinare se il campo verrà visualizzato nel modulo, nonché l'etichetta e la guida personalizzata da fornire agli utenti del catalogo.

Alcuni Blueprint potrebbe includere campi che contengono un valore fisso. Quando si aggiunge questo tipo di campi a un modulo personalizzato, sono disponibili solo le opzioni Aspetto e il campo è sempre in sola lettura.

Tabella 3-66. Opzioni della scheda Aspetto

Opzione	Descrizione
Etichetta e tipo	<p>Questa opzione consente di specificare un'etichetta e selezionare un tipo di visualizzazione.</p> <p>I tipi di visualizzazione disponibili variano in base al campo. Alcuni campi supportano più tipi di testo, alcuni supportano alcuni tipi e alcuni supportano solo un singolo tipo. Valori possibili in tutti i tipi:</p> <ul style="list-style-type: none"> ■ Casella combinata ■ Decimale ■ Menu a discesa ■ Elenco doppio ■ Immagine ■ Integer ■ Collegamento ■ Selezione multipla ■ Selettore multivalore ■ Password ■ Gruppo di pulsanti di opzione ■ Text ■ Area testo ■ Campo testo <p>I tipi di campi a selezione multipla e a doppio elenco forniscono la stessa funzionalità, con l'elenco doppio che rappresenta un'opzione più intuitiva quando l'utente può selezionare più di un elemento in un elenco.</p> <p>I campi Menu a discesa e Griglia dati includono un'impostazione Segnaposto. Il valore immesso viene visualizzato come un'etichetta o un'istruzione interna nel menu a discesa oppure come un'etichetta o un'istruzione generica nella griglia dati.</p> <p>I campi del selettore del valore e del selettore dell'albero includono l'impostazione Tipo di riferimento. Il tipo di riferimento è il tipo di risorsa di vRealize Orchestrator utilizzato per limitare la ricerca del selettore del valore o dell'albero all'inventario del server vRealize Orchestrator che supporta il tipo. È quindi possibile limitare ulteriormente la ricerca selezionando un'azione che supporta il tipo di riferimento. Per ulteriori informazioni sui due selettori, vedere Utilizzo degli elementi del selettore del valore e del selettore della struttura nel designer moduli personalizzati.</p>
Visibilità	<p>Consente di mostrare o nascondere un campo nel modulo di richiesta.</p> <ul style="list-style-type: none"> ■ Costante. Selezionare Sì per visualizzare il campo nel modulo. Selezionare No per nascondere il campo.

Tabella 3-66. Opzioni della scheda Aspetto (continua)

Opzione	Descrizione
	<ul style="list-style-type: none"> ■ Valore condizionale. La visibilità è determinata dalla prima espressione che risulta vera. Ad esempio, un campo di un modulo è visibile se è selezionata una casella di testo. ■ Origine esterna. La visibilità è determinata dai risultati dell'azione di vRealize Orchestrator selezionata.
Sola lettura	<p>Consente di impedire agli utenti di modificare i valori del campo.</p> <ul style="list-style-type: none"> ■ Costante. Selezionare Sì per visualizzare il valore, ma per impedire eventuali modifiche. Selezionare No per consentire le modifiche. ■ Valore condizionale. Lo stato è determinato dalla prima espressione che risulta vera. Ad esempio, un campo è di sola lettura se il valore di un campo Storage è maggiore di 2 GB. ■ Origine esterna. Lo stato è determinato dai risultati dell'azione di vRealize Orchestrator selezionata.
Righe per pagina	<p>Solo per gli elementi della griglia dati.</p> <p>Consente di immettere il numero di righe.</p>
Guida personalizzata	<p>Consente di fornire agli utenti informazioni relative al campo. Queste informazioni vengono visualizzate nella Guida indicazioni del campo.</p> <p>È possibile utilizzare testo semplice o HTML, includendo collegamenti href. Ad esempio <code>vRealize Automation documentation</code>.</p>

Valori dei campi

Le proprietà dei valori consentono di specificare qualsiasi valore predefinito.

Tabella 3-67. Opzioni della scheda Valori

Opzione	Descrizione
Colonne	<p>Solo per l'elemento griglia dati.</p> <p>Consente di specificare l'etichetta, l'ID e il tipo di valore di ciascuna colonna nella tabella.</p> <p>Il valore predefinito della griglia dati deve includere dati dell'intestazione corrispondenti alle colonne definite. Ad esempio, se una colonna contiene l'ID user_name e un'altra l'ID user_role, la prima riga sarà user_name,user_role.</p> <p>Per alcuni esempi di configurazione, vedere Utilizzo dell'elemento Griglia dati nel designer di moduli personalizzati.</p>
Valore predefinito	<p>Consente di compilare il campo con un valore predefinito in base all'origine del valore.</p> <p>Per molte delle proprietà, è possibile selezionare varie opzioni relative all'origine dei valori. Non tutte le opzioni relative all'origine sono disponibili per tutti i tipi o le proprietà dei campi. Le origini dei valori possibili dipendono dal campo.</p> <ul style="list-style-type: none"> ■ Costante. La stringa immessa. Il valore non cambia. A seconda della proprietà, il valore potrebbe essere una stringa, un numero intero, un'espressione regolare oppure un valore selezionato da un elenco limitato, ad esempio Sì o No. <p>Ad esempio, è possibile specificare 1 come valore intero predefinito, selezionare No per la proprietà di sola lettura o fornire l'espressione regolare per convalidare una voce del campo.</p> <ul style="list-style-type: none"> ■ Valore condizionale. Il valore si basa su una o più condizioni. Le condizioni vengono elaborate nell'ordine in cui sono elencate. Se più condizioni sono vere, l'ultima condizione vera determina il comportamento del campo per tale proprietà. Ad esempio, è possibile creare una condizione che determina se un campo è visibile in base al valore in un altro campo. <p>Ad esempio, il valore predefinito di un campo Storage è 1 GB se il campo Memoria è minore di 512 MB. L'operatore <code>contains</code> verifica che il campo selezionato contenga il valore specificato. L'operatore <code>within</code> verifica che nei campi selezionati sia presente la stringa specificata. Ad esempio, se l'espressione è Field A within development, l'espressione è true se Field A = dev o lop o ment, ma è false se Field A = prod o test.</p> <ul style="list-style-type: none"> ■ Origine esterna. Il valore si basa sui risultati di un'azione di vRealize Orchestrator. Ad esempio, il calcolo del costo in base a un'azione di vRealize Orchestrator con script.

Tabella 3-67. Opzioni della scheda Valori (continua)

Opzione	Descrizione
	<p>Per un esempio, vedere Utilizzo delle azioni di vRealize Orchestrator nel designer di moduli personalizzati.</p> <ul style="list-style-type: none"> ■ Associa campo. Il valore corrisponde a quello del campo selezionato a cui è associato. I campi disponibili sono limitati allo stesso tipo di campo. <p>Ad esempio, è possibile associare il valore predefinito del campo di una casella di controllo con autenticazione necessaria al campo di un'altra casella di controllo. Quando viene selezionata una casella di controllo di un campo di destinazione nel modulo di richiesta, viene selezionata anche la casella di controllo nel campo corrente.</p> <ul style="list-style-type: none"> ■ Valore elaborato. Il valore dipende dai risultati dei valori dei campi specificati e dall'operatore selezionato. Per i campi di testo viene utilizzato l'operatore Concatena. Per i campi numero intero vengono utilizzate le operazioni di aggiunta, sottrazione, moltiplicazione o divisione selezionate. <p>Ad esempio, è possibile configurare un campo numero intero per convertire i megabyte in gigabyte utilizzando l'operazione di moltiplicazione. Il valore predefinito di Memoria in MB di basa sul valore di Memoria in GB moltiplicato per 1024.</p>
Opzione valore	<p>Consente di compilare un campo Menu a discesa, Selezione multipla, Gruppo di pulsanti di opzione o Selezione valore.</p> <ul style="list-style-type: none"> ■ Costante. Il formato dell'elenco è Valore Etichetta,Valore Etichetta,Valore Etichetta. Ad esempio 2 Small,4 Medium,8 Large. ■ Origine esterna. Il valore è basato sui risultati dell'azione di vRealize Orchestrator selezionata.
Passaggio	<p>Consente di definire valori incrementali o decrementali per i campi numero intero o decimale.</p> <p>Ad esempio, se il valore predefinito è 1 e il valore di Passaggio è impostato su 3, i valori consentiti saranno 4, 7, 10 e così via.</p>

Vincoli dei campi

Le proprietà di vincolo consentono di garantire che l'utente che effettua la richiesta specifichi valori validi nel modulo di richiesta.

Come metodo alternativo per garantire l'immissione di valori validi, è inoltre possibile utilizzare la convalida esterna. Vedere [Utilizzo della convalida esterna nel designer di moduli personalizzati](#).

Tabella 3-68. Opzioni della scheda Vincoli

Opzione	Descrizione
Obbligatorio	<p>L'utente che effettua la richiesta deve specificare un valore per questo campo.</p> <ul style="list-style-type: none"> ■ Costante. Selezionare Sì per obbligare l'utente che effettua la richiesta a specificare un valore. Selezionare No se si desidera che il campo sia facoltativo. ■ Valore condizionale. L'obbligatorietà del campo è determinata dalla prima espressione che risulta vera. Ad esempio, questo campo è obbligatorio se la famiglia del sistema operativo inizia con Darwin in un altro campo. ■ Origine esterna. Lo stato si basa sui risultati dell'azione di vRealize Orchestrator selezionata.
Espressione regolare	<p>Consente di specificare un'espressione regolare che convalida il valore e un messaggio che viene visualizzato quando la convalida non riesce.</p> <p>Le espressioni regolari devono seguire la sintassi JavaScript. Per una panoramica, vedere Creazione di un'espressione regolare. Per istruzioni più dettagliate, vedere Sintassi.</p> <ul style="list-style-type: none"> ■ Costante. Consente di specificare un'espressione regolare. Ad esempio, per un indirizzo email l'espressione regolare potrebbe essere <code>^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$</code> e il messaggio di errore di convalida <code>Il formato dell'indirizzo email non è valido. Riprovare.</code> ■ Valore condizionale. L'espressione regolare che viene utilizzata è determinata dalla prima espressione che risulta vera.
Valore minimo	<p>Specificare un valore numerico minimo. Ad esempio, una password deve includere almeno 8 caratteri.</p> <p>Specificare un messaggio di errore. Ad esempio, <code>La password deve includere almeno 8 caratteri.</code></p> <ul style="list-style-type: none"> ■ Costante. Immettere il numero intero. ■ Valore condizionale. Il valore minimo è determinato dalla prima espressione che risulta vera. Ad esempio, il valore minimo di una CPU è 4 se il sistema operativo è diverso da Linux. ■ Origine esterna. Il valore è basato sui risultati dell'azione di vRealize Orchestrator selezionata.

Tabella 3-68. Opzioni della scheda Vincoli (continua)

Opzione	Descrizione
Valore massimo	<p>Valore numerico massimo. Ad esempio, un campo ha un limite di 50 caratteri.</p> <p>Specificare un messaggio di errore. Ad esempio, La descrizione non può superare i 50 caratteri.</p> <ul style="list-style-type: none"> ■ Costante. Immettere il numero intero. ■ Valore condizionale. Il valore massimo è determinato dalla prima espressione che risulta vera. Ad esempio, il valore massimo di Storage è 2 GB se Posizione della distribuzione è uguale ad AMEA. ■ Origine esterna. Il valore è basato sui risultati dell'azione di vRealize Orchestrator selezionata.
Trova una corrispondenza per il campo	<p>Il valore di questo campo deve corrispondere al valore del campo selezionato.</p> <p>Ad esempio, il valore del campo di conferma della password deve corrispondere al valore del campo Password.</p>

Utilizzo delle azioni di vRealize Orchestrator nel designer di moduli personalizzati

Quando si personalizza il modulo di richiesta di un blueprint di vRealize Automation, è possibile basare il comportamento di alcuni campi sui risultati di un'azione di vRealize Orchestrator.

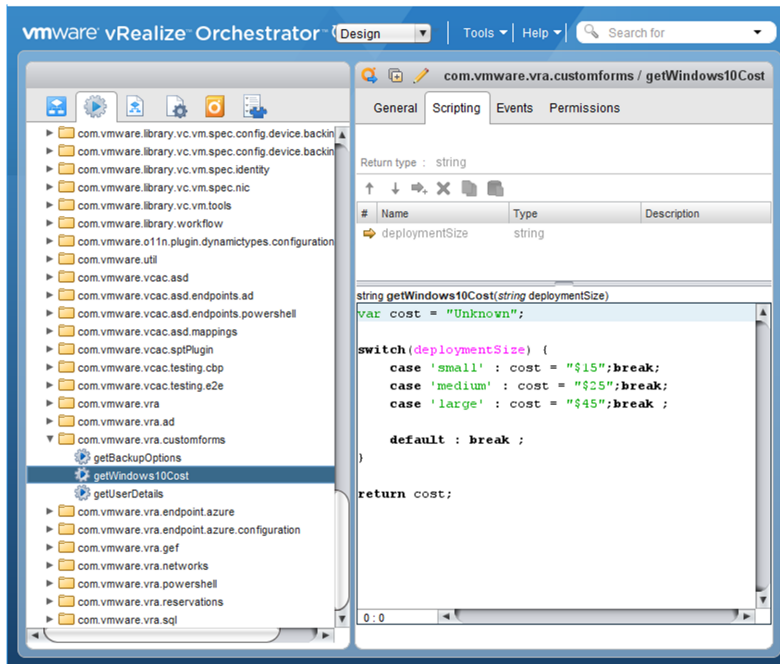
Esistono diversi metodi di utilizzo delle azioni di vRealize Orchestrator. È possibile utilizzare un'azione che estrae i dati da un'origine di terze parti oppure usare uno script che definisce le dimensioni e il costo. In questo esempio viene utilizzato uno script.

Quando si crea uno script per popolare i campi utilizzando un'azione, non utilizzare un tipo Array [Any].

Esempio: Esempi di campi Dimensioni e Costo

In questo caso d'uso, si desidera che l'utente del catalogo selezioni determinate dimensioni di macchina virtuale e quindi visualizzi il costo di tale macchina al giorno. Per eseguire l'operazione di questo esempio, è disponibile un'azione di vRealize Orchestrator che mette in relazione le dimensioni e il costo. Si aggiunge inoltre un campo Dimensioni e un campo Costo nel modulo personalizzato del blueprint. Il campo Dimensioni determina il valore visualizzato nel campo Costo.

- 1 In vRealize Orchestrator, configurare l'azione `getWindows10Cost` con uno script `deploymentSize` simile a quello riportato nell'esempio seguente.



Di seguito è riportato uno script di esempio.

```

var cost = "Unknown";

switch(deploymentSize) {
  case 'small' : cost = "$15";break;
  case 'medium' : cost = "$25";break;
  case 'large' : cost = "$45";break ;

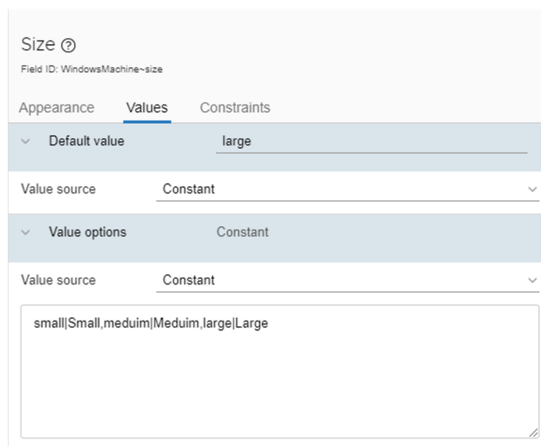
  default : break ;
}

return cost;

```

- 2 In vRealize Automation, aggiungere e configurare un campo Dimensioni e un campo Costo nel modulo personalizzato del blueprint.

Configurare il campo Dimensioni come selezione multipla, con i valori Small, Medium e Large.



In vRealize Automation, aggiungere e configurare un campo Dimensioni e un campo Costo nel modulo personalizzato del blueprint.

Nella scheda Valori, configurare i valori delle proprietà seguenti.

- Valore predefinito = **Large**
- Opzioni valore
 - Origine valore = **Constant**
 - Definizione valore = **small|Small,medium|Medium,large|Large**

- 3 Configurare il campo Costo per visualizzare il costo come definito nell'azione di vRealize Orchestrator in base al valore selezionato nel campo Dimensioni.

Cost ⓘ
Field ID: cost

Appearance **Values** Constraints

▼ Default value External source

Value source External source ▼

Select action com.vmware.vra.customforms/getWindows10Cost

Action inputs

deploymentSize Field ▼ Size ▼

Nella scheda Valori, configurare i valori delle proprietà seguenti.

- Valore predefinito = Origine esterna
- Seleziona azione = <cartella azioni vRealize Orchestrator>/getWindows10Cost
- Input azioni
 - deploymentSize. Questo valore è stato configurato nell'azione.
 - Campo
 - Dimensioni

Utilizzo degli elementi del selettore del valore e del selettore della struttura nel designer moduli personalizzati

Quando si personalizza il modulo di richiesta, è possibile fornire elementi in cui l'utente può selezionare i risultati di ricerca da un elenco o cercare una struttura per individuare un valore corrispondente.

Il selettore del valore e il selettore della struttura operano con il tipo di riferimento definito nella scheda Aspetto del modulo personalizzato. Il tipo di riferimento è una risorsa di vRealize Orchestrator. Ad esempio, AD:UserGroup o VC:Datastore. Con la definizione del tipo di riferimento, quando l'utente immette una stringa di ricerca, i risultati o le opzioni della struttura sono limitate alle risorse che dispongono di parametri corrispondenti.

Per il selettore del valore, è possibile quindi limitare ulteriormente i valori possibili configurando una fonte esterna. Per il selettore della struttura, è possibile fornire un valore predefinito configurando una fonte esterna.

Utilizzo del selettore del valore

Il selettore del valore viene visualizzato nel modulo del catalogo come opzione di ricerca. L'utente immette una stringa e il selettore fornisce opzioni in base a come è configurata. È possibile utilizzare il selettore in base ai seguenti casi di utilizzo. L'utilizzo più efficiente del selettore del valore consiste nell'associarlo a un valore di origine esterna.

- Selettore del valore con un'origine del valore costante. Utilizzare questo metodo quando si desidera che l'utente richiedente selezioni da un elenco statico di valori predefiniti. Come per una casella combinata, un menu a discesa, una selezione multipla ed elementi di gruppo di opzione, questo metodo fornisce risultati della ricerca in un elenco basato su etichette e valori costanti definiti.
- Selettore del valore senza origine di valore definita. Utilizzare questo metodo quando si desidera che l'utente richiedente effettui la ricerca nell'inventario di vRealize Orchestrator per un oggetto specifico con il tipo di riferimento configurato. Ad esempio, il tipo di riferimento è VC:Datastore e si desidera che gli utenti selezionino il datastore dall'elenco recuperato.
- Selettore del valore con un'origine del valore esterna. Utilizzare questo metodo quando si desidera che l'utente richiedente selezioni dai risultati in base a un'azione di vRealize Orchestrator. Per un'origine esterna del selettore del valore, l'azione deve restituire un array di proprietà, non un array di stringhe. Ad esempio, è presente un'azione che recupera due o più valori da un database integrato e si desidera che gli utenti selezionino un valore dall'elenco recuperato. L'azione deve includere il filtro `var filter = System.getContext().getParameter("__filter");` e deve restituire un array di proprietà, non un array di stringhe. Se si desidera un array di stringhe, utilizzare il tipo di campo casella combinata.

Utilizzo del selettore della struttura

Il selettore della struttura viene visualizzato nel modulo del catalogo come opzione di ricerca. L'utente immette una stringa e viene visualizzato il selettore della struttura. La struttura consente agli utenti di selezionare i valori che corrispondono al tipo di riferimento. Ad esempio, se il tipo di riferimento è VC:Datastore, l'utente richiedente può selezionare gli oggetti del datastore. Se il tipo di riferimento è VC:VirtualMachine, l'utente può selezionare macchine virtuali.

- Selettore della struttura senza origine di valore definita. Utilizzare questo metodo quando si desidera che l'utente richiedente visualizzi la struttura gerarchica per un oggetto specifico con il tipo di riferimento configurato. Ad esempio, il tipo di riferimento è VC:Datastore e si desidera che gli utenti selezionino un datastore dalla struttura recuperata.

- Selettore della struttura con un'origine del valore esterna. Utilizzare questo metodo quando si desidera fornire una selezione predefinita nella struttura. L'utente richiedente può selezionare il valore predefinito o cercare un valore diverso. Ad esempio, per tipo di riferimento VC:Datastore, si desidera preimpostare il datastore nella struttura a un datastore specifico in base ai risultati del valore di input dell'azione che specifica una rete.

Utilizzo dell'elemento Griglia dati nel designer di moduli personalizzati

Quando si personalizza il modulo di richiesta per un blueprint, è possibile aggiungere informazioni in formato tabella. L'utente richiedente può popolare le righe con i dati inclusi nella richiesta di provisioning.

È possibile aggiungere una tabella e popolarla in base ai dati forniti manualmente o in base a un'origine esterna. Alcuni elementi del blueprint vengono visualizzati come una griglia dati. Ad esempio, dischi della macchina virtuale o NIC.

Oltre ad aggiungere campi alla griglia dati, è possibile aggiungere vincoli per garantire che l'utente fornisca valori accettabili.

Negli esempi seguenti viene utilizzata la griglia dati, ma è possibile utilizzare il selettore multivalore come modalità alternativa di presentazione dell'opzione agli utenti nel modulo di richiesta. È possibile verificare le differenze modificando la proprietà del campo **Aspetto > Etichetta e tipo > Tipo di visualizzazione**.

Esempio: Esempio di dati CSV forniti

In questo esempio, è presente una tabella di valori forniti nel modulo di richiesta personalizzato. Fornire le informazioni nella tabella come origine di valori costante. L'origine è basata su una struttura di dati CSV in cui la prima riga è l'intestazione. Le intestazioni sono gli identificatori di colonna separati da virgole. Ogni riga aggiuntiva contiene i dati che vengono visualizzati in ogni riga nella tabella.

- 1 Aggiungere l'elemento generico Griglia dati alla tela di progettazione.
- 2 Selezionare la griglia dati e definire i valori nel riquadro delle proprietà.



Data Grid ?



Field ID: datagrid_ecdf4fe3



Appearance **Values** Constraints

Columns

ADD COLUMN

Label	Username	 
Id	username	
Type	String	▼

Label	Employee ID	 
Id	employeeid	
Type	Integer	▼

Label	Manager	 
Id	manager	
Type	String	▼

Default value Constant

Value Constant ▼

source

CSV

```
username,employeeid,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

Label	ID	Tipo
Username	nome utente	Stringa
ID dipendente	employeeid	Integer
Manager	manager	Stringa

Definire i valori CSV.

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

- 3 Verificare che la griglia dati visualizzi i dati previsti nel modulo di richiesta del blueprint.

<input type="checkbox"/>	Username	Employee ID	Manager
<input type="checkbox"/>	leonardo	95621	Farah
<input type="checkbox"/>	vindhya	15496	Farah
<input type="checkbox"/>	martina	52648	Nikolai

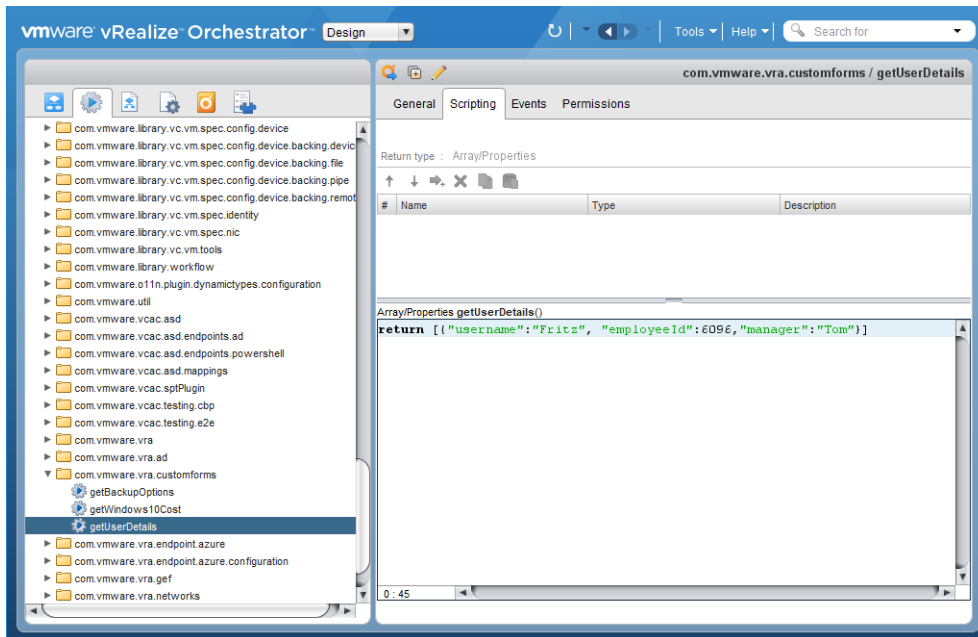
1 - 3 of 3

Esempio: Esempio di origine esterna

Questo esempio utilizza l'esempio precedente, ma i valori sono basati su un'azione di vRealize Orchestrator. Anche se questo è un esempio di azione semplice, è possibile utilizzare un'azione più complessa che consente di recuperare le informazioni da un database o un sistema locale.

L'azione utilizzata come convalida deve avere un parametro di input Array/Properties.

- 1 In vRealize Orchestrator, configurare un'azione, `getUserDetails`, con un array simile all'esempio seguente.



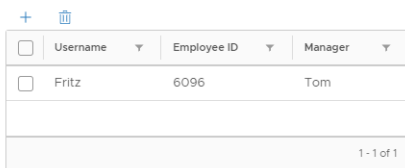
Utilizzare lo script di esempio seguente.

```
return [{"username": "Fritz", "employeeId": 6096, "manager": "Tom"}]
```

- In vRealize Automation, aggiungere la griglia dati e configurare le colonne della griglia dati con i valori seguenti.

Label	ID	Tipo
Username	nome utente	Stringa
ID dipendente	employeeid	Integer
Manager	manager	Stringa

- Nell'elenco Origine valore, selezionare **Origine esterna**.
- In Seleziona azione immettere getUserDetails e selezionare l'azione creata in vRealize Orchestrator.
- Salvare e verificare la tabella nel modulo di richiesta.



<input type="checkbox"/>	Username ▼	Employee ID ▼	Manager ▼
<input type="checkbox"/>	Fritz	6096	Tom
1 - 1 of 1			

Esempio: Esempio di elemento del blueprint

È possibile aggiungere alcuni elementi del blueprint al modulo e visualizzarli come griglia dati quando l'utente richiede il blueprint. I dischi e le NIC vengono visualizzati come griglie dati.

In questo esempio, si aggiunge un elemento disco al modulo in modo che gli utenti possano aggiungere altri dischi quando richiedono l'elemento del catalogo. È possibile aggiungere vincoli per controllare meglio ciò che l'utente può richiedere. Ad esempio, è possibile limitare la capacità a 5 GB.

I valori degli elementi definiti nel blueprint, ad esempio i dischi, non sono visibili nel modulo personalizzato. Ciò impedisce all'utente di modificare una configurazione necessaria per il corretto provisioning della richiesta.

- Creare un blueprint con una macchina con un disco di storage definito da 6 GB.
- Aggiungere l'elemento disco alla tela.
- Selezionare la griglia dati e definire i vincoli nel riquadro delle proprietà.

In questo esempio, la capacità minima è impostata su 2 e quella massima su 5.

Disks ⓘ

Field ID: vSphere__vCenter__Machine_1-disks

Appearance	Values	Constraints
> Drive letter / Mount path		
> Volume ID		
> ID		
> Label		
> custom_properties		
> User Created		
> Storage Reservation policy		
▼ Capacity		
> Required	No	▼
> Regular expression	Regular expression	
> Minimum value	2	
> Maximum value	5	

4 Salvare e verificare i vincoli della tabella nel modulo di richiesta.

5 Nel modulo di richiesta, fare clic sul segno più nella griglia dati.

Tenere presente che il vincolo di capacità si attiva se si immette un valore maggiore di 5.

☐ Is Clone

Drive letter / Mount path

Volume ID



ID

Label

custom_properties

☐ User Created

Storage Reservation policy

Capacity  

Utilizzo della convalida esterna nel designer di moduli personalizzati

Per accertarsi che gli utenti forniscano valori validi al momento della richiesta, è possibile personalizzare un modulo di richiesta aggiungendo vincoli ai campi o utilizzando un'origine di convalida esterna.

Alcune proprietà dei campi, come minimo, massimo, espressioni regolari, corrispondenza campi o non vuoto, possono essere configurate con vincoli per garantire l'immissione di valori validi. Vedere [Proprietà personalizzate dei campi di designer modulo](#).

Controlli di convalida di valori validi da un'origine esterna mediante azioni di vRealize Orchestrator.

Se si sta convalidando un valore della griglia dati, l'azione utilizzata come convalida deve avere un parametro di input array/proprietà.

La convalida esterna può essere utilizzata, ad esempio, nei seguenti casi:

- Se i valori validi vengono definiti in un'origine esterna. Ad esempio vRealize Orchestrator.
- Se la convalida coinvolge più campi. Ad esempio, un'azione di vRealize Orchestrator consente di raccogliere i dati relativi alle dimensioni del disco e alla capacità del pool di archiviazione e di convalidare i valori specificati in base allo spazio disponibile.

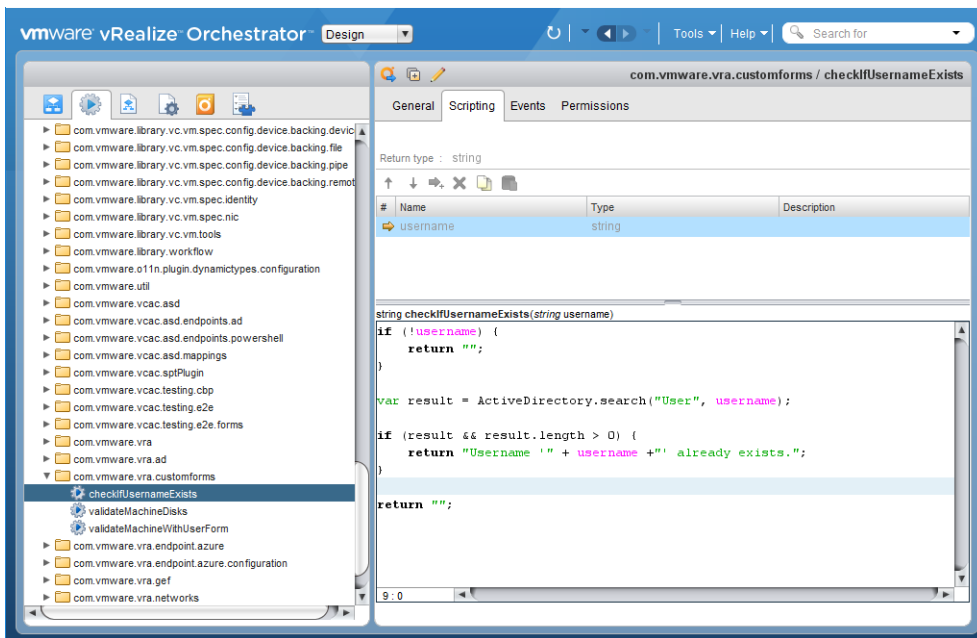
Come è possibile ordinare più operazioni di convalida esterna in un blueprint? Le operazioni di convalida vengono elaborate nell'ordine in cui sono visualizzate sulla tela Convalida esterna. Se sono presenti due operazioni di convalida per lo stesso campo, i risultati della seconda convalida sovrascriveranno quelli della prima. Per riordinare le convalide, è possibile fare clic e trascinare le schede sulla tela.

Esempio: Caso d'uso di vRealize Orchestrator

In questo caso d'uso, si desidera che l'utente del catalogo fornisca solo un nuovo nome utente. Per eseguire l'operazione descritta in questo esempio, è disponibile un'azione di vRealize Orchestrator che consente di controllare se il nome utente specificato nel modulo esiste nel database di Active Directory. Se il nome esiste, nel modulo di richiesta viene visualizzato un messaggio di errore.

Questo caso d'uso è applicato all'esempio di [Creazione di un modulo di richiesta personalizzato con opzioni di Active Directory](#).

- 1 In vRealize Orchestrator, configurare l'azione `checkIfUsernameExists` con uno script simile a quello riportato nell'esempio seguente.



Di seguito è riportato uno script di esempio. In questo esempio, `return` è il messaggio che viene visualizzato se la convalida non riesce.

```
if (!username) {
    return "";
}

var result = ActiveDirectory.search("User", username);

if (result && result.length > 0) {
```

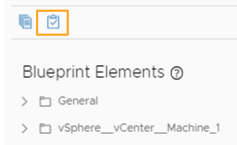
```

    return "Username '" + username + "' already exists.";
}

return "";

```

- In vRealize Automation, aprire il designer del modulo predefinito per il blueprint, fare clic su **Convalida esterna** e trascinare il tipo **Convalida Orchestrator** sulla tela.



- Configurare le opzioni di convalida esterna.

- Etichetta convalida = Controlla se il nome utente esiste
- Seleziona azione = <cartella azioni di vRealize Orchestrator>/checkIfUsernameExists
- Input azioni
 - nome utente = Campo e Nome utente
- Campi evidenziati
 - Fare clic su **Aggiungi campo** e selezionare Nome utente.

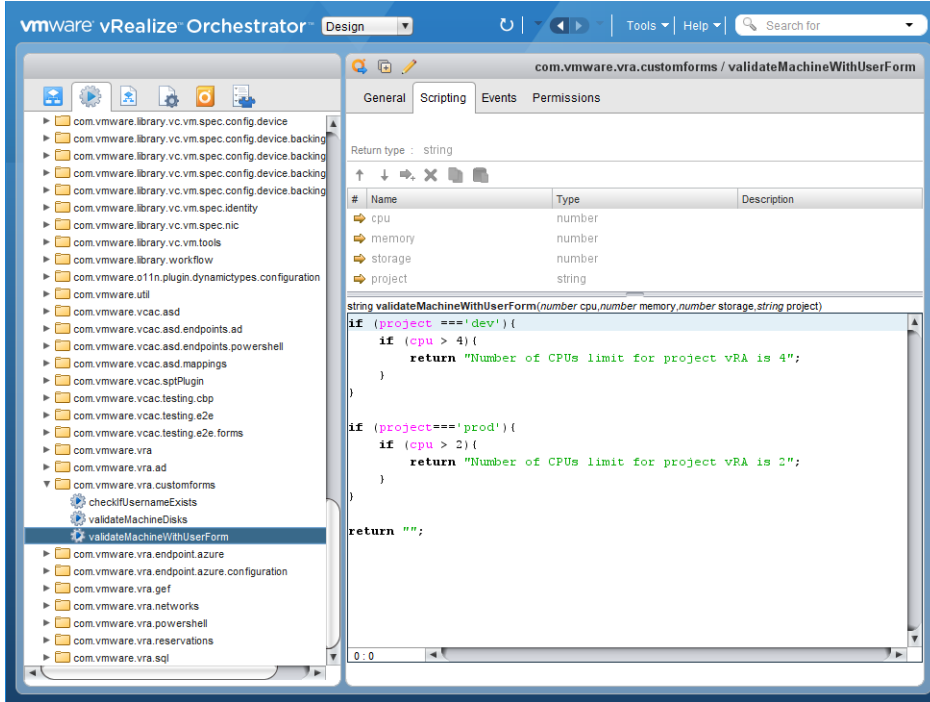
Se il valore immesso causa l'esito negativo della convalida, nel modulo di richiesta del catalogo viene visualizzato un errore di convalida a livello di campo. Se si desidera che venga visualizzato un errore globale, non configurare il campo evidenziato.

Esempio: Esempio relativo a più campi di vRealize Orchestrator

In questo caso d'uso, si desidera basare la convalida dei valori di CPU, memoria e storage sul valore del progetto. Ad esempio, se gli utenti selezionano il progetto Dev, il numero massimo di CPU sarà 4. Se selezionano Prod, il valore massimo sarà 2.

Per questo caso d'uso, aggiungere un campo del progetto all'esempio di [Creazione di un modulo di richiesta personalizzato con opzioni di Active Directory](#). Configurare il progetto come menu a discesa contenente Dev e Prod.

- 1 In vRealize Orchestrator, configurare l'azione `validateMachineWithUserForm` con uno script simile a quello riportato nell'esempio seguente.



Per il controllo della CPU, utilizzare lo script di esempio indicato di seguito. Continuare ad aggiungere i valori di memoria e storage allo script, se necessario. In questo esempio, return è il messaggio che viene visualizzato se la convalida non riesce.

```

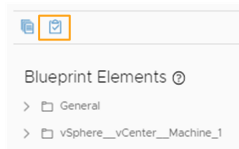
if (project === 'dev'){
    if (cpu > 4){
        return "Number of CPUs limit for project vRA is 4";
    }
}

if (project==='prod'){
    if (cpu > 2){
        return "Number of CPUs limit for project vRA is 2";
    }
}

return "";

```

- 2 In vRealize Automation, aprire il designer del modulo predefinito per il blueprint, fare clic su **Convalida esterna** e trascinare il tipo **Convalida Orchestrator** sulla tela.



3 Configurare le opzioni di convalida esterna.

- Etichetta convalida = Convalida dettagli macchina
- Seleziona azione = <cartella azioni di vRealize Orchestrator>/validateMachineWithUserForm
- Input azioni
 - cpu = Campo e Numero di CPU
 - memoria = Campo e Memoria (GB)
 - storage = Campo e Storage (GB)
 - Progetto = Campo e Progetto
- Campi evidenziati
 - Fare clic su **Aggiungi campo** e selezionare **Progetto**.

Nel catalogo, potrebbe venire visualizzato un errore di convalida simile a quello dell'esempio seguente.

Richieste di provisioning non riuscite per test e risoluzione dei problemi

Come architetti o amministratori di blueprint, si desidera assicurarsi di fornire blueprint di lavoro all'utente.

Le richieste del catalogo possono non riuscire per diversi motivi. Ciò può avvenire a causa del traffico di rete, risorse insufficienti dell'endpoint o una specifica di blueprint difettosa. Oppure, è possibile che la richiesta di provisioning sia stata completata, ma la distribuzione non sembra funzionare. Come architetti di blueprint, si desidera evitare di fornire blueprint che gli utenti non possano distribuire con successo.

È possibile creare un servizio e un permesso di testing in modo da poter distribuire il blueprint dal catalogo. Vedere [Elenco di controllo per la configurazione del catalogo dei servizi](#).

Se le risorse non vengono effettuate correttamente, è possibile utilizzare vRealize Automation per la risoluzione dei problemi nella distribuzione non riuscita.

Possibili stati di errore

Se una richiesta di provisioning non riesce, viene visualizzato uno degli stati seguenti.

- **Non riuscito** Una richiesta può non riuscire per diversi motivi. Un motivo può essere che il processo di provisioning non ha funzionato a causa della mancanza di risorse nell'endpoint di destinazione, risorse insufficienti per supportare il blueprint o un blueprint progettato in modo errato che deve essere corretto. Un altro motivo è che la richiesta necessita l'approvazione di un utente dell'organizzazione, ma l'approvatore rifiuta la richiesta. È inoltre possibile che un'azione eseguita in una distribuzione non sia riuscita. L'errore può essere causato dai motivi relativi all'ambiente o all'approvazione già indicati.

Utilizzare il workflow per la risoluzione dei problemi seguente per individuare la causa del problema. Se si è in grado di risolvere il problema, esaminare le opzioni delle azioni **Ignora** e **Invia di nuovo**. Vedere [Comandi del menu Azione per le risorse di cui è stato eseguito il provisioning](#).

- **Parzialmente completata.** Una richiesta può essere parzialmente riuscita, il che significa che alcuni componenti sono stati distribuiti, ma non tutti i passaggi del provisioning sono stati completati correttamente.

Utilizzare il workflow di risoluzione dei problemi seguente per determinare quali componenti sono riusciti solo parzialmente e individuare la causa del problema. Se si è in grado di risolvere il problema, esaminare le opzioni dell'azione **Ignora** e verificare se è possibile utilizzare **Riprendi**. Vedere [Comandi del menu Azione per le risorse di cui è stato eseguito il provisioning](#) e [Funzionamento dell'azione Riprendi](#).

Workflow di risoluzione dei problemi

È possibile utilizzare questo workflow per iniziare l'analisi di una distribuzione non riuscita. Se l'analisi rivela che l'errore si è verificato a causa di un problema ambientale temporaneo, è possibile correggere l'errore e inviare di nuovo la richiesta. Se il problema riguarda la specifica della richiesta, è possibile aggiornare il blueprint e inviare una nuova richiesta.

Tabella 3-69. Come iniziare a risolvere i problemi

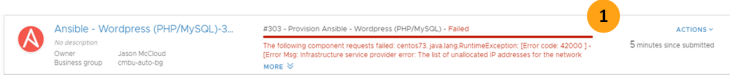
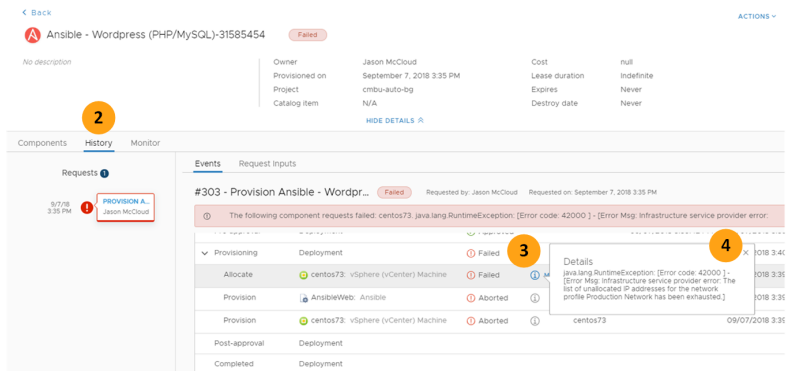
Workflow	Passaggio di risoluzione dei problemi	Esempio
1	Nella scheda Distribuzioni , le distribuzioni non riuscite sono indicate nella barra di stato. La scheda include l'ultimo messaggio di errore. Per ulteriori informazioni, fare clic sul nome della distribuzione o sulla barra di avanzamento.	
2	Nella scheda Cronologia dei dettagli della distribuzione, è possibile utilizzare il workflow degli eventi per verificare dove il processo di provisioning non è riuscito. Questo workflow è inoltre utile quando si esegue un'azione in una distribuzione, ma la modifica non riesce.	
3	Lo stato di errore indica dove il workflow non è riuscito.	

Tabella 3-69. Come iniziare a risolvere i problemi (continua)

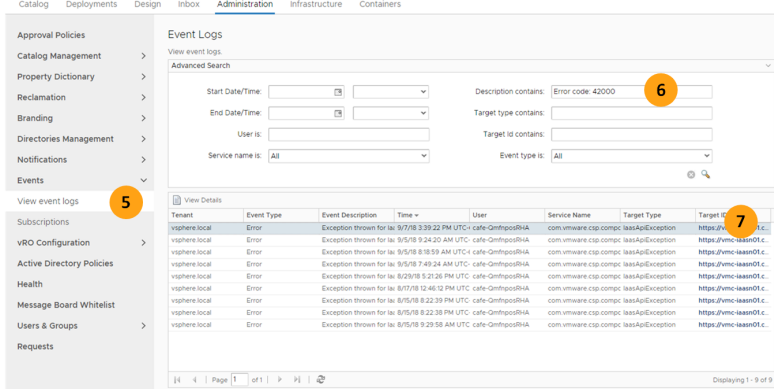
Workflow	Passaggio di risoluzione dei problemi	Esempio
4	Le informazioni forniscono una versione più dettagliata del messaggio di errore. Se queste informazioni non sono sufficienti per identificare e risolvere il problema, è possibile eseguire ricerche aggiuntive nei registri eventi.	
5	I passaggi seguenti richiedono un ruolo di amministratore. Per individuare un errore nel contesto di altri errori e avvisi, selezionare Amministrazione > Eventi > Visualizza registri eventi .	
6	È possibile utilizzare la ricerca avanzata per individuare l'errore in base al messaggio nei dettagli della distribuzione.	
7	Per visualizzare i dettagli dell'evento, fare clic sul collegamento ID target.	

Tabella 3-69. Come iniziare a risolvere i problemi (continua)

Workflo w	Passaggio di risoluzione dei problemi	Esempio
8	I dettagli dell'evento forniscono informazioni aggiuntive sul provisioning che potrebbero risultare utili per la risoluzione dei problemi.	
9	In qualità di amministratore, è inoltre possibile visualizzare la richiesta nel contesto di altre richieste degli utenti. Selezionare Amministrazione > Richieste e fare clic sul numero di richiesta per esaminare gli input e gli eventi della richiesta.	

Funzionamento dell'azione Riprendi

Per le distribuzioni non riuscite è possibile riprendere il processo di provisioning dal punto di errore e in circostanze specifiche. Se è attivata, l'azione Riprendi è disponibile per le richieste di provisioning non riuscite o per altre azioni applicabili.

Per utilizzare l'azione di ripresa nelle richieste di provisioning, è necessario aggiungere la proprietà personalizzata `_debug_deployment = true` al blueprint. Per impostazione predefinita, per le distribuzioni non riuscite viene effettuato il rollback. Tali distribuzioni vengono inoltre eliminate in modo da recuperare le risorse. La proprietà `_debug_deployment = true` mantiene la distribuzione al punto di errore e, laddove supportato e in base al funzionamento, consente un'azione di ripresa. Se si utilizza la ripresa solo per le azioni supportate, non è necessario abilitare la proprietà `_debug_deployment`.

Per ulteriori informazioni su `_debug_deployment`, vedere *Guida di riferimento alle proprietà personalizzate*.

Per utilizzare l'azione di ripresa per una richiesta di provisioning o per un'azione disponibile, è necessario autorizzare gli utenti all'esecuzione dell'azione di ripresa. Vedere [Autorizzazione degli utenti per servizi, elementi di catalogo e azioni](#).

È possibile autorizzare gli utenti all'esecuzione dell'azione di ripresa per le seguenti attività di provisioning.

- Richieste di provisioning
- Azione di ripresa
- Azione di scalabilità verticale
- Azione di scalabilità orizzontale
- Azione di eliminazione

Vincoli dell'azione di ripresa

Quando si decide se utilizzare l'azione di ripresa anziché richiedere una nuova istanza di blueprint, è consigliabile considerare i vincoli.

- Il blueprint non è modificabile dall'ora della richiesta.

Al momento della richiesta, una versione non modificabile del blueprint viene associata alla richiesta del catalogo. Questa versione statica contiene tutte le specifiche, inclusi gli attributi, le proprietà personalizzate, le impostazioni e così via, relative al momento dell'avvio del provisioning. Se nel blueprint è presente un errore che crea problemi, la correzione dell'errore e l'utilizzo dell'azione di ripresa non consentono di risolvere la situazione perché fanno riferimento alla versione associata alla richiesta. In questo scenario, è necessario eseguire il provisioning di una nuova istanza.

Esempi

- Il blueprint A richiede 5 GB di RAM, ma la richiesta non riesce perché sono presenti solo prenotazioni per 3 GB. Se si aggiorna il blueprint in modo che necessiti di soli 3 GB e quindi si esegue l'azione Riprendi, tale azione non riesce. Quando viene eseguita, l'azione di ripresa verifica infatti la richiesta originale e cerca ancora 5 GB. Tuttavia, se si aumenta la prenotazione del sistema fino a 5 GB per il gruppo di business e si esegue l'azione Riprendi, tale azione viene effettuata correttamente.
- Quando si richiede il blueprint B, che include una specifica personalizzata guest, l'azione non viene eseguita correttamente. Un'indagine determina che la specifica personalizzata guest è stata rinominata nell'istanza di vCenter Server. Se si aggiorna il blueprint con il nuovo nome e si esegue la ripresa, tale azione non viene effettuata correttamente. Il blueprint è stato aggiornato, ma per l'azione di ripresa viene utilizzata la versione originale. Se il nuovo nome è quello che si desidera utilizzare da ora in poi, distribuire una nuova istanza del blueprint anziché utilizzare l'azione di ripresa. In caso contrario, è necessario modificare il nome della specifica personalizzata guest nell'istanza di vCenter Server riutilizzando il nome previsto dalla versione originale e quindi eseguire l'azione di ripresa. Se si desidera evitare che la successiva richiesta di provisioning non riesca, non dimenticare di aggiornare il blueprint con la specifica personalizzata guest corretta.

L'azione di ripresa funziona se è possibile aggiornare l'ambiente di distribuzione di destinazione in modo che supporti le specifiche del blueprint esistenti al momento della richiesta.

- Il nuovo tentativo viene eseguito solo dal punto di errore.

L'azione di ripresa ripete le attività dei componenti dal punto di errore. Non viene inviata nuovamente l'intera richiesta di provisioning.

Esempi

- Il blueprint C crea una macchina virtuale dell'applicazione e una macchina virtuale del database. La macchina virtuale del database viene distribuita correttamente, ma il provisioning non riesce nella macchina virtuale dell'applicazione. Se si esegue l'azione di ripresa, viene ripetuto solo il provisioning della macchina virtuale dell'applicazione.

Se un componente viene contrassegnato come non riuscito, viene considerato come se non fosse mai stato eseguito. Se l'installazione non riesce durante la fase di configurazione nella macchina virtuale del database, ad esempio a causa di un errore di scripting, ma il database è integro, il database esiste ancora quando viene eseguito lo script durante un'azione di ripresa. Lo script di installazione, che include lo script di configurazione, non viene eseguito nuovamente. L'azione di ripresa non riesce. È necessario correggere lo script ed effettuare il provisioning di una nuova istanza.

- Un'altra variante da prendere in considerazione è quella in cui il passaggio di allocazione riesce, ma il provisioning no. In questo esempio, quando si esegue l'azione di ripresa, che effettua un nuovo tentativo dal punto del provisioning non riuscito, la richiesta di ripresa elabora informazioni di allocazione obsolete e pertanto tale azione non riesce.

Utilizzo dell'azione di ripresa e delle sottoscrizioni ai workflow

Se la sottoscrizione a un workflow non riesce, non è possibile eseguire un'azione di ripresa per riprendere tale workflow. L'azione di ripresa può essere eseguita solo quando si verificano eventi di provisioning non riusciti, in presenza dei quali viene eseguito un nuovo workflow.

Ad esempio, se si sottoscrive l'evento Richiesta catalogo ricevuta, la richiesta di provisioning non riuscita e la nuova richiesta di ripresa soddisfano entrambe in modo indipendente le condizioni di sottoscrizione, ma la sottoscrizione non è a conoscenza della richiesta non riuscita e della richiesta di ripresa come attività correlate.

Eliminazione forzata di una distribuzione dopo una richiesta di eliminazione non riuscita

È possibile forzare l'eliminazione di una distribuzione che presenta uno stato incoerente a causa di una richiesta di eliminazione non riuscita.

Quando vRealize Automation non riesce a eliminare una risorsa di distribuzione durante un'operazione di eliminazione della distribuzione, l'operazione si interrompe subito senza eliminare le restanti risorse di distribuzione. Questo errore lascia la distribuzione in uno stato incoerente, consumando risorse senza la possibilità effettiva di eliminare la distribuzione. Gli amministratori del gruppo di business possono forzare l'eliminazione delle distribuzioni che presentano questo stato incoerente.

Prerequisiti

- Verificare di aver effettuato l'accesso a vRealize Automation come **amministratore del gruppo di business**.
- Prima di eseguire l'azione Forza eliminazione, controllare la descrizione dell'azione Elimina in [Comandi del menu Azione per le risorse di cui è stato eseguito il provisioning](#).

Procedura

- 1 Nella scheda **Distribuzioni**, individuare la distribuzione da eliminare.
- 2 Fare clic su **Azioni**, quindi su **Elimina**.
- 3 Immettere una descrizione e il motivo della richiesta.
- 4 Selezionare **Forza eliminazione** e fare clic su **Invia**.

Risultati

vRealize Automation tenta di eliminare completamente la distribuzione, comprese tutte le risorse al suo interno. Se vRealize Automation non riesce a eliminare una risorsa di distribuzione, la salta e continua a eliminare le restanti risorse nella distribuzione.

Operazioni successive

Verificare che tutte le risorse nella distribuzione siano state eliminate correttamente. Le risorse che non vengono eliminate durante un'operazione di eliminazione forzata devono essere eliminate manualmente. Assicurarsi inoltre che tutti gli oggetti della macchina virtuale con provisioning vengano eliminati, perché vRealize Automation potrebbe tentare di riutilizzare i nomi host, gli indirizzi IP e altri dettagli sulla configurazione durante le operazioni di provisioning successive.

Risoluzione dei problemi relativi a una distribuzione non riuscita che include un workflow vRealize Orchestrator

Se una distribuzione blueprint non riuscita include un workflow vRealize Orchestrator, è possibile utilizzare l'ID del token per risolvere eventuali problemi con il workflow. L'ID del token consente di individuare i registri in vRealize Orchestrator.

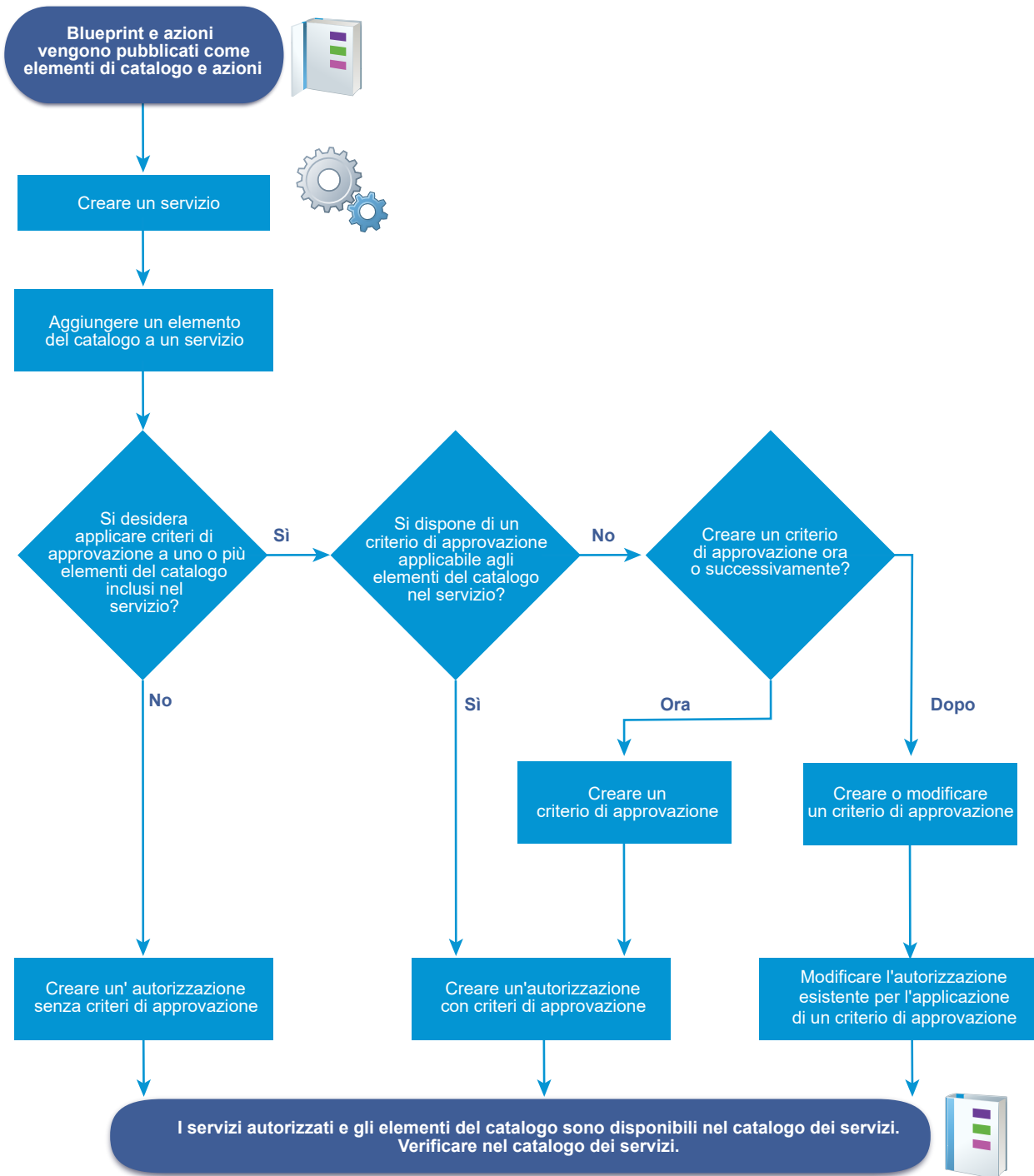
Soluzione

- 1 Individuare l'ID del token per il workflow non riuscito.
 - a In vRealize Automation, fare clic sulla scheda **Distribuzioni** e individuare la distribuzione o l'azione.
 - b Fare clic sul nome della distribuzione.
La richiesta può essere una distribuzione o un'azione.
 - c Fare clic su scheda **Cronologia** e quindi sulla scheda **Richiesta input**.
Se il blueprint si basa su un workflow vRealize Orchestrator, il titolo della pagina è Dettagli esecuzione workflow vRealize Orchestrator.
 - d Individuare l'ID del token e copiarlo negli Appunti o in un file di testo.
Ad esempio, ff8080815a685352015a6c8d450801ee.
- 2 Individuare i registri del workflow in vRealize Orchestrator utilizzando il Centro di controllo
 - a Immettere l'URL di base per vRealize Automation nella casella di ricerca di un browser.
Viene visualizzata la pagina dell'appliance VMware vRealize Automation .
 - b Fare clic su **vRealize Orchestrator Control Center**.
 - c Accedere come utente con privilegi root.
 - d Fare clic su **Analizza workflow**.
 - e Fare clic su **Workflow completati**.
 - f Incollare il token del workflow nella casella di testo ID token.
Viene visualizzato l'elenco corrispondente all'ID del token.
 - g Fare clic sulla riga e analizzare i registri per individuare la causa dell'errore.

Gestione del catalogo dei servizi

Il catalogo dei servizi è il punto in cui i clienti richiedono il provisioning delle macchine e degli altri elementi da utilizzare. È possibile gestire l'accesso degli utenti agli elementi del catalogo dei servizi in base alla modalità di creazione dei servizi, autorizzare gli utenti a uno o più elementi e applicare governance.

Il workflow seguito per aggiungere elementi al catalogo dei servizi cambia varia in base a se sono creati e applicati criteri di approvazione.



Elenco di controllo per la configurazione del catalogo dei servizi

Dopo la creazione e pubblicazione di blueprint e azioni, è possibile creare un servizio vRealize Automation, configurare gli elementi del catalogo e assegnare permessi e approvazioni.

L'elenco di controllo per la configurazione del catalogo dei servizi è una panoramica ad alto livello della sequenza di passaggi necessari per configurare il catalogo e contiene i collegamenti ai punti di decisione e alle istruzioni dettagliate per ogni passaggio.

Tabella 3-70. Elenco di controllo Configurazione del catalogo dei servizi

Attività	Ruolo richiesto	Dettagli
<input type="checkbox"/> Aggiunta di un servizio.	amministratore tenant o del catalogo	Vedere Aggiunta di un servizio .
<input type="checkbox"/> Aggiunta di un elemento del catalogo a un servizio.	amministratore tenant o del catalogo	Vedere Aggiunta di elementi del catalogo a un servizio .
<input type="checkbox"/> Configurazione dell'elemento del catalogo nel servizio.	amministratore tenant o del catalogo	Vedere Configurazione di un elemento del catalogo .
<input type="checkbox"/> Creazione e applicazione di permessi all'elemento del catalogo.	amministratore tenant o manager del gruppo di business	Vedere Autorizzazione degli utenti per servizi, elementi di catalogo e azioni .
<input type="checkbox"/> Creazione e applicazione di criteri di approvazione all'elemento del catalogo.	amministratore tenant o amministratore approvazioni per la creazione di criteri di approvazione. amministrazione tenant o manager di gruppo di business per l'applicazione dei criteri di approvazione	Vedere Creazione di un criterio di approvazione .

Creazione di un servizio

Un servizio è un gruppo di elementi di catalogo che si desidera includere nel catalogo dei servizi. È possibile autorizzare il servizio, operazione che trasmette agli utenti del gruppo di business l'autorizzazione per tutti gli elementi di catalogo associati, ed è possibile applicare un criterio di approvazione al servizio.

Un servizio funziona come un gruppo dinamico di elementi di catalogo. Se si autorizza un servizio, tutti gli elementi del catalogo associati al servizio diventano disponibili nel catalogo del servizio per gli utenti specificati, e tutti gli elementi del catalogo aggiunti o rimossi da un servizio influiscono sul catalogo del servizio.

Quando si crea il servizio, è possibile utilizzarlo come categoria di servizi in modo che sia possibile assemblare le offerte dei servizi per i propri utenti del catalogo del servizio. Ad esempio, un servizio desktop Windows che include elementi di catalogo sistemi operativi Windows 7, 8 e 10 o un servizio Linux che include gli elementi di catalogo sistemi operativi CentOS e RHEL.

Aggiunta di un servizio

Per rendere elementi di catalogo disponibili agli utenti del catalogo dei servizi, aggiungere un servizio. Tutti gli elementi del catalogo devono essere associati a un servizio, in modo da poter autorizzare l'accesso agli elementi da parte degli utenti.

Quando un servizio viene autorizzato per gli utenti, gli elementi del catalogo compaiono tutti insieme nel catalogo dei servizi. È possibile anche autorizzare l'accesso da parte degli utenti ai singoli elementi del catalogo.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.

Procedura

1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.

2 Fare clic sull'icona **Nuovo** (+).

3 Immettere un nome e una descrizione.

Questi valori vengono visualizzati nel catalogo dei servizi per gli utenti del catalogo.

4 Per aggiungere un'icona specifica per il servizio all'interno del catalogo dei servizi, fare clic su **Sfoglia** e scegliere un'immagine.

I tipi di file immagine supportati sono GIF, JPG e PNG. Le dimensioni dell'immagine visualizzata sono 40 x 40 pixel. Se non viene selezionata un'immagine personalizzata, nel catalogo dei servizi comparirà l'icona predefinita.

5 Selezionare uno stato dal menu a discesa **Stato**.

Opzione	Descrizione
Inattivo	Il servizio non è disponibile nel catalogo dei servizi. Quando un servizio è in questo stato, è possibile associare a esso elementi del catalogo, ma non è possibile autorizzare l'accesso al servizio da parte degli utenti. Se si seleziona Inattivo per un servizio che è attivo e autorizzato, questo viene rimosso dal catalogo dei servizi fino alla sua riattivazione.
Attivo	(Impostazione predefinita) Il servizio e gli elementi del catalogo associati sono disponibili per essere autorizzati per gli utenti. Una volta concessa l'autorizzazione, gli utenti interessati potranno accedervi dal catalogo dei servizi.
Eliminato	Rimuove il servizio da vRealize Automation. Tutti gli elementi del catalogo associati sono ancora presenti, ma gli elementi associati al servizio nel catalogo dei servizi non sono disponibili per gli utenti del catalogo.

6 Configurare le impostazioni del servizio.

Le impostazioni seguenti forniscono informazioni agli utenti del catalogo dei servizi. Le impostazioni non influiscono sulla disponibilità del servizio.

Opzione	Descrizione
Ore	Configurare l'orario in modo che coincida con la disponibilità del team di supporto. L'orario è basato sul fuso orario locale. Le ore di servizio non possono iniziare in un giorno e terminare nel giorno successivo. Ad esempio non è possibile impostare un orario di servizio che inizia alle 16:00 e finisce alle 04:00. In questi casi è necessario creare due permessi. In questo esempio, se ne crea uno per la fascia dalle 16:00 alle 23:59 e un altro dalle 00:00 alle 04:00.
Proprietario	Specificare l'utente o il gruppo di utenti che riveste il ruolo di proprietario principale del servizio e degli elementi del catalogo associati.
Team di supporto	Specificare l'utente o il gruppo di utenti personalizzato che è disponibile a fornire assistenza nel caso in cui gli utenti del catalogo dei servizi incontrino problemi quando effettuano il provisioning degli elementi utilizzando il servizio.
Finestra per le modifiche	Selezionare la data e l'ora in cui si pianifica di apportare una modifica al servizio. La data e l'ora specificate sono dati informativi e non influiscono sulla disponibilità del servizio.

7 Fare clic su **Aggiungi**.

Operazioni successive

Associare gli elementi del catalogo a un servizio, in modo da poter autorizzare gli utenti ad accedervi. Vedere [Aggiunta di elementi del catalogo a un servizio](#).

Aggiunta di elementi del catalogo a un servizio

Aggiungendo elementi del catalogo ai servizi è possibile autorizzare gli utenti a richiedere gli elementi nel catalogo dei servizi. Un elemento del catalogo può essere associato a un solo servizio.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.
- Verificare che esista un servizio. Vedere [Aggiunta di un servizio](#).
- Verificare che siano pubblicati uno o più elementi del catalogo. Vedere [Configurazione di un elemento del catalogo](#).

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.
- 2 Selezionare il servizio a cui aggiungere gli elementi del catalogo e fare clic su **Gestisci elementi del catalogo**.

3 Fare clic sull'icona **Elementi del catalogo** (+).

- a Selezionare gli elementi del catalogo da includere nel servizio.

Nella finestra di dialogo Seleziona elementi del catalogo vengono visualizzati solo gli elementi che non sono già associati a un servizio.

- b Fare clic su **Aggiungi**.

4 Fare clic su **Chiudi**.

Operazioni successive

- È possibile aggiungere un'icona personalizzata all'elemento del catalogo che accompagnerà la visualizzazione dell'elemento nel catalogo dei servizi. Vedere [Configurazione di un elemento del catalogo](#).
- Autorizzare gli utenti ai servizi o agli elementi del catalogo in modo che possano richiederli nel catalogo dei servizi. Vedere [Creazione di permessi](#).

Funzionamento di elementi del catalogo e azioni

Gli elementi del catalogo sono blueprint pubblicati di macchine, componenti software e altri oggetti. Le azioni nell'area di gestione del catalogo sono azioni pubblicate che è possibile eseguire sugli elementi del catalogo con provisioning. È possibile utilizzare gli elenchi per determinare quali sono i blueprint e le azioni pubblicati, così da poterli rendere disponibili agli utenti del catalogo dei servizi.

Elementi del catalogo pubblicati

Un elemento del catalogo è un blueprint pubblicato. I blueprint pubblicati possono essere utilizzati anche in altri blueprint. Il riutilizzo dei blueprint in altri blueprint non è mostrato nell'elenco degli elementi del catalogo.

Gli elementi del catalogo pubblicati possono anche includere elementi che sono solo componenti di blueprint. Ad esempio, i componenti software pubblicati sono elencati come elementi del catalogo, ma sono disponibili solo come parte di una distribuzione.

Gli elementi del catalogo di distribuzione devono essere associati a un servizio, così da poterli rendere disponibili agli utenti autorizzati nel catalogo dei servizi. Nel catalogo dei servizi compaiono solo elementi attivi. È possibile configurare gli elementi del catalogo in un servizio differente, disattivare se si desidera rimuoverlo temporaneamente dal catalogo dei servizi e aggiungere un'icona personalizzata che verrà mostrata nel catalogo.

Azioni pubblicate

Le azioni sono cambiamenti apportati agli elementi del catalogo di cui viene eseguito il provisioning. È possibile ad esempio riavviare una macchina virtuale.

Le azioni possono includere azioni integrate o azioni create utilizzando XaaS. Le azioni integrate si aggiungono quando si include una macchina o altro blueprint fornito in provisioning. Le azioni di XaaS devono essere create e pubblicate.

Le azioni non sono associate ai servizi. È necessario includere un'azione nel permesso che contiene l'elemento del catalogo sul quale viene eseguita. Nel catalogo dei servizi non compaiono le azioni che sono state autorizzati agli utenti. Se applicabili all'elemento e al suo stato corrente, le azioni vengono rese disponibili per l'elemento fornito in provisioning nella scheda **Distribuzioni** dell'utente del catalogo dei servizi.

È possibile aggiungere un'icona personalizzata all'azione mostrata nella scheda **Distribuzioni**.

Configurazione di un elemento del catalogo

Un elemento del catalogo è un blueprint pubblicato che gli utenti sono autorizzati a richiedere. Le opzioni degli elementi del catalogo consentono di cambiare lo stato o il servizio associato. È inoltre possibile visualizzare i permessi relativi all'elemento del catalogo selezionato.

Nel catalogo dei servizi vengono inclusi solo gli elementi del catalogo associati a un servizio e per i quali è stato concesso agli utenti il relativo permesso. Un elemento del catalogo può essere associato a un solo servizio.

Se non si desidera che un elemento del catalogo venga visualizzato nel catalogo dei servizi senza rimuoverlo da un permesso o dall'elenco degli elementi del catalogo pubblicato, è possibile disattivarlo. Lo stato di un elemento del catalogo disattivato viene ritirato nella griglia e reso inattivo nei dettagli della configurazione. Potrà essere attivato in un secondo momento.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.
- Accertarsi che almeno un blueprint sia stato pubblicato come elemento del catalogo. Vedere [Pubblicazione di un blueprint](#).

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Elementi del catalogo**.
- 2 Selezionare l'elemento del catalogo e fare clic su **Configura**.

3 Configurare le impostazioni dell'elemento del catalogo.

Opzione	Descrizione
Icona	Selezionare un'immagine. I tipi di file immagine supportati sono GIF, JPG e PNG. Le dimensioni dell'immagine visualizzata sono 40 x 40 pixel. Se non viene selezionata un'immagine personalizzata, nel catalogo dei servizi viene visualizzata l'icona di catalogo predefinita.
Stato	<p>I possibili valori sono Attivo, Inattivo e Gestione temporanea.</p> <ul style="list-style-type: none"> ■ Attivo. L'elemento del catalogo è disponibile nel catalogo dei servizi e gli utenti autorizzati possono utilizzarlo per il provisioning di risorse. Nell'elenco degli elementi del catalogo, l'elemento è indicato come Pubblicato. ■ Inattivo. L'elemento del catalogo non è disponibile nel catalogo dei servizi. Nell'elenco degli elementi del catalogo è indicato come Ritirato. ■ Gestione temporanea. L'elemento del catalogo non è disponibile nel catalogo dei servizi. Selezionare questa voce del menu per un elemento inattivo che si intende riattivare mediante la gestione temporanea. Nell'elenco degli elementi del catalogo l'elemento è indicato come Gestione temporanea.
Quota	<p>Impostare il numero di istanze di questo elemento del catalogo che un utente può distribuire.</p> <p>Se l'utente supera il numero, alla richiesta di catalogo viene visualizzata una notifica e la richiesta non viene inviata.</p>
Servizio	Selezionare un servizio. Affinché possano essere disponibili nel catalogo dei servizi per gli utenti autorizzati, gli elementi del catalogo devono essere associati a un servizio. L'elenco include i servizi attivi e inattivi.

4 Per visualizzare i permessi che rendono l'elemento del catalogo disponibile per gli utenti, fare clic sulla scheda **Permessi**.

5 Fare clic su **Aggiorna**.

Operazioni successive

- Per rendere un elemento del catalogo disponibile nel catalogo dei servizi, è necessario autorizzare gli utenti per il servizio associato all'elemento o per il singolo elemento. Vedere [Creazione di permessi](#).
- Per specificare l'ordine di elaborazione dei permessi per la corretta applicazione dei criteri di approvazione per i singoli utenti, impostare l'ordine di priorità per più permessi per lo stesso gruppo di business. Vedere [Assegnare priorità ai permessi](#).

Configurazione di un'azione per il catalogo dei servizi

Un'azione è una modifica o un workflow eseguibile su elementi con provisioning eseguito. È possibile aggiungere un'icona o visualizzare i permessi che comprendono l'azione selezionata.

Un'azione può essere integrata per una macchina fornita in provisioning, una rete e altri componenti di un blueprint, oppure può essere un'azione XaaS pubblicata.

Per l'icona, i tipi di file immagine supportati sono GIF, JPG e PNG. Le dimensioni dell'immagine visualizzata sono 40 x 40 pixel. Se non viene selezionata un'immagine personalizzata, nella scheda **Distribuzioni** compare l'icona di azione predefinita.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.
- Assicurarsi che sia disponibile almeno un'azione pubblicata. Vedere [Pubblicazione di un blueprint](#) e [Pubblicazione di un'azione risorsa](#).

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Azioni**.
- 2 Selezionare l'azione condivisa e fare clic su **Visualizza dettagli** oppure, per le azioni XaaS, **Configura**.
- 3 Selezionare un'immagine.
- 4 Per visualizzare i permessi per cui l'azione è stata resa disponibile agli utenti, fare clic sulla scheda **Permessi**.
- 5 Fare clic su **Fine**.

Operazioni successive

[Autorizzazione degli utenti per servizi, elementi di catalogo e azioni](#).

Creazione di permessi

I permessi controllano quali elementi e azioni sono disponibili nel catalogo dei servizi per i membri del gruppo di business selezionato. Affinché gli elementi compaiano nel catalogo dei servizi, per questi deve essere attivo un permesso. Se si hanno elementi che richiedono governance, è possibile utilizzare i permessi per applicare criteri di approvazione ai diversi elementi.

Per configurare un permesso, gli elementi del catalogo devono essere inclusi in un servizio. I permessi possono comprendere più servizi, elementi del catalogo dai servizi che sono compresi in altri permessi e azioni che è possibile eseguire sugli elementi del catalogo distribuiti.

Comprensione delle interazioni delle opzioni di permesso

La modalità di configurazione di un permesso determina i contenuti visualizzati nel catalogo dei servizi. L'interazione dei servizi, gli elementi e i componenti del catalogo, l'azione e i criteri di approvazione influiscono su ciò che l'utente del catalogo dei servizi può richiedere e le modalità di applicazione dei criteri di approvazione.

Quando si crea un permesso, è necessario considerare le interazioni dei servizi, gli elementi di catalogo, le azioni e le approvazioni.

■ Servizi nei permessi

Un servizio autorizzato funziona come un gruppo dinamico di elementi di catalogo. Se dopo essere stato autorizzato un elemento di catalogo viene aggiunto a un servizio, il nuovo elemento di catalogo sarà disponibile agli utenti specificati senza alcuna configurazione aggiuntiva.

■ Elementi e componenti del catalogo nei permessi

Gli elementi del catalogo autorizzati sono blueprint che è possibile richiedere nel catalogo di servizi. I componenti autorizzati fanno parte dei blueprint, ma non è possibile richiederli in modo specifico nel catalogo dei servizi.

■ Azioni nei permessi

Azioni eseguite sugli elementi del catalogo distribuiti. Gli elementi del catalogo con provisioning e le azioni che l'utente è autorizzato ad eseguire su di essi vengono visualizzati nella scheda Distribuzioni. Per eseguire azioni su un elemento distribuito, l'azione deve essere inclusa nello stesso permesso dell'elemento di catalogo che ha eseguito il provisioning dell'elemento dal catalogo dei servizi.

■ Criteri di approvazione nei permessi

I criteri di approvazione vengono applicati nei permessi in modo da consentire la gestione delle risorse nel proprio ambiente.

Servizi nei permessi

Un servizio autorizzato funziona come un gruppo dinamico di elementi di catalogo. Se dopo essere stato autorizzato un elemento di catalogo viene aggiunto a un servizio, il nuovo elemento di catalogo sarà disponibile agli utenti specificati senza alcuna configurazione aggiuntiva.

Se si applica un criterio di approvazione a un servizio, tutti gli elementi, quando richiesto, sono soggetti allo stesso criterio di approvazione.

Elementi e componenti del catalogo nei permessi

Gli elementi del catalogo autorizzati sono blueprint che è possibile richiedere nel catalogo di servizi. I componenti autorizzati fanno parte dei blueprint, ma non è possibile richiederli in modo specifico nel catalogo dei servizi.

Gli elementi e i componenti del catalogo autorizzati possono includere gli elementi elencati di seguito:

Elementi del catalogo

- Elementi provenienti da qualsiasi servizio che si desidera fornire a utenti autorizzati, persino servizi non inclusi nel permesso corrente.

Si consideri il seguente esempio: un amministratore di un catalogo ha associato svariate versioni di Red Hat Enterprise Linux a un servizio Red Hat e autorizzato il servizio agli ingegneri di qualità del prodotto A. Egli riceve la richiesta di creare elementi del catalogo dei servizi che include solo l'ultima versione di sistemi operativi basati su Linux per il team di formazione. L'amministratore crea un permesso per il team di formazione che include le ultime versioni degli altri sistemi operativi in un servizio. Egli dispone già dell'ultima versione di Red Hat Enterprise Linux associata a un altro servizio, pertanto aggiunge Red Hat Enterprise Linux come elemento di catalogo invece di aggiungere l'intero servizio Red Hat.

- Elementi inclusi in un servizio incluso nel permesso corrente, ma si desidera applicare un criterio di approvazione al singolo elemento di catalogo diverso dal criterio applicato al servizio.

Ad esempio, un manager gruppo di business autorizza il team di sviluppo per un servizio che include tre elementi di catalogo macchina virtuale. Egli applica un criterio di approvazione che richiede l'approvazione dell'amministratore di infrastruttura virtuale per le macchine con più di quattro CPU. Una delle macchine virtuali è utilizzata per testare le prestazioni, così il manager la aggiunge come elemento del catalogo e applica un criterio di approvazione meno restrittivo per lo stesso gruppo di utenti.

Componenti

- I componenti non sono disponibili per nome nel catalogo di servizi in quanto fanno parte di un elemento del catalogo. Devono essere autorizzati singolarmente in modo da poter applicare un criterio di approvazione specifico che differisca dall'elemento del catalogo nel quale è incluso.

Si consideri ad esempio un elemento che include una macchina e software. La macchina è disponibile come elemento di cui è possibile eseguire il provisioning e presenta un criterio di approvazione che richiede l'approvazione del manager del sito. Il software non è disponibile come elemento autonomo di cui è possibile eseguire il provisioning, ma solo come parte di una richiesta di macchina, tuttavia il criterio di approvazione per il software richiede l'approvazione da parte dell'amministratore delle licenze software dell'organizzazione. Quando la macchina viene richiesta nel catalogo dei servizi, deve essere approvata dall'amministratore del sito e dall'amministratore delle licenze software prima che venga fornita in provisioning. Dopo che è stato eseguito il provisioning, la macchina, con la voce relativa al software, compare nella scheda Distribuzioni del richiedente come parte della macchina.

Azioni nei permessi

Azioni eseguite sugli elementi del catalogo distribuiti. Gli elementi del catalogo con provisioning e le azioni che l'utente è autorizzato ad eseguire su di essi vengono visualizzati nella scheda Distribuzioni. Per eseguire azioni su un elemento distribuito, l'azione deve essere inclusa nello stesso permesso dell'elemento di catalogo che ha eseguito il provisioning dell'elemento dal catalogo dei servizi.

Si consideri come esempio un permesso 1, che include una macchina virtuale vSphere e un'azione di creazione snapshot, e un permesso 2 che include solo una macchina virtuale vSphere. Quando si distribuisce una macchina vSphere dal permesso 1, l'azione di creazione snapshot è disponibile. Quando si distribuisce una macchina vSphere dal permesso 2, non c'è alcuna azione. Per rendere l'azione disponibile agli utenti del permesso 2, aggiungere l'azione di creazione snapshot al permesso 2.

Se si seleziona un'azione non applicabile ad alcun elemento del catalogo nel permesso, essa non comparirà come azione nella scheda Distribuzioni. Si consideri il seguente esempio: il permesso include una macchina vSphere e si autorizza un'azione di eliminazione per una macchina cloud. L'azione di eliminazione non è disponibile per l'esecuzione sulla macchina fornita in provisioning.

È possibile applicare un criterio di approvazione a un'azione diversa dal criterio applicato all'elemento di catalogo nel permesso.

Se l'utente del catalogo dei servizi è membro di più gruppi di business, uno dei quali è autorizzato solo all'accensione e allo spegnimento mentre un altro alla sola eliminazione, per l'utente saranno disponibili tre azioni per la macchina fornita in provisioning applicabile.

Procedure consigliate quando si autorizzano utenti per le azioni

I blueprint sono complessi e autorizzare l'esecuzione di azioni sui blueprint di cui è stato eseguito il provisioning può causare comportamenti imprevisti. Attenersi alle seguenti procedure consigliate quando si autorizzano utenti del catalogo dei servizi a eseguire azioni sui loro elementi con provisioning eseguito.

- Quando si autorizzano utenti all'azione Elimina Macchina, autorizzarli per Elimina Distribuzione. Un blueprint di cui è stato eseguito il provisioning è di fatto una distribuzione. Una distribuzione può contenere una macchina. Se l'utente del catalogo dei servizi è autorizzato a eseguire l'azione Elimina Macchina e non è autorizzato a eseguire l'azione Elimina Distribuzione, quando l'utente esegue l'azione Elimina Macchina sull'ultima o sull'unica macchina in una distribuzione, viene visualizzato un messaggio in cui si informa l'utente che non dispone dell'autorizzazione necessaria per eseguire l'azione. Il permesso per entrambe le azioni garantisce l'eliminazione della distribuzione dall'ambiente. Per gestire la governance sull'azione Elimina Distribuzione è possibile creare un criterio di pre-approvazione e applicarlo all'azione. Il criterio consentirà all'approvatore designato di convalidare la richiesta Elimina Distribuzione prima che venga eseguita.
- Quando si autorizzano utenti del catalogo dei servizi per Modifica lease, Cambia proprietario, Scadenza, Riconfigura e altre azioni che possono applicarsi a macchine e distribuzioni, prevedere l'autorizzazione per entrambe le azioni.

Criteri di approvazione nei permessi

I criteri di approvazione vengono applicati nei permessi in modo da consentire la gestione delle risorse nel proprio ambiente.

Per applicare un criterio di approvazione quando si crea il permesso, è necessario che il criterio esista già. Se non esiste, è comunque possibile creare il permesso e lasciarlo nello stato di bozza o inattivo finché non si creano i criteri di approvazione necessari per gli elementi del catalogo e le azioni in questo permesso, per poi applicare i criteri successivamente.

Non è necessario applicare un criterio di approvazione a tutti gli elementi o le azioni. Se non viene applicato alcun criterio di approvazione, gli elementi e le azioni vengono distribuiti quando richiesti, senza attivare una richiesta di approvazione.

Autorizzazione degli utenti per servizi, elementi di catalogo e azioni

Quando si aggiunge un servizio, un elemento di catalogo o un'azione a un permesso, si consente agli utenti identificati nel permesso di richiedere gli elementi nel catalogo dei servizi di cui è possibile eseguire il provisioning. Le azioni sono associate agli elementi e sono elencate nella scheda **Distribuzioni** per l'utente richiedente.

Sono disponibili diversi ruoli utente dotati dell'autorizzazione a creare permessi per i gruppi di business.

- Gli amministratori tenant possono creare permessi per qualsiasi gruppo di business nei relativi tenant.
- I manager dei gruppi di business possono creare permessi per i gruppi da essi gestiti.
- Gli amministratori dei cataloghi possono creare permessi per qualsiasi gruppo di business nei relativi tenant.

Quando si crea un permesso, è necessario selezionare un gruppo di business e i relativi membri per tale permesso.

Per ulteriori dettagli su come creare un permesso in modo da poter utilizzare le interazioni dei servizi, elementi del catalogo e azioni con approvazioni vedere [Creazione di permessi](#)

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.
- Verificare che gli elementi del catalogo, per cui si stanno autorizzando gli utenti, siano associati a un servizio. Vedere [Aggiunta di elementi del catalogo a un servizio](#).
- Verificare l'esistenza del gruppo di business per cui si sta definendo il permesso e assicurarsi che gli utenti membri e i gruppi di utenti siano definiti. Vedere [Creazione di un gruppo di business](#).
- Verificare l'esistenza dei criteri di approvazione se si intende aggiungere approvazioni quando si crea questo permesso. Vedere [Creazione di un criterio di approvazione](#). Se si desidera autorizzare gli utenti per gli elementi nel catalogo dei servizi senza approvazioni, è possibile modificare il permesso in un secondo momento per aggiungere le approvazioni.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.

2 Fare clic sull'icona **Nuovo** (+).

3 Configurare le opzioni in **Dettagli**.

I dettagli determinano come viene mostrato il permesso nell'elenco dei permessi e quali utenti hanno accesso agli elementi nel catalogo dei servizi.

Opzione	Descrizione
Nome e descrizione	Informazioni sul permesso riportate nell'elenco dei permessi.
Data di scadenza	Impostare la data e l'ora se si desidera che il permesso diventi inattivo a una data particolare.
Stato	<p>I valori possibili sono Attivo, Inattivo e Eliminato.</p> <ul style="list-style-type: none"> ■ Attivo. Gli elementi sono disponibili nel catalogo dei servizi. Questa opzione viene visualizzata quando si aggiungono o modificano i permessi. ■ Inattivo: gli elementi non sono disponibili nel catalogo dei servizi. Il permesso è stato disattivato a causa di una data di scadenza o da un utente. ■ Eliminato. Elimina il permesso.
Gruppo di business	<p>Selezionare un gruppo di business. È possibile creare permessi per un solo gruppo di business e gli utenti autorizzati devono essere membri del gruppo di business.</p> <p>Se si desidera rendere un permesso disponibile per tutti gli utenti è necessario disporre di un gruppo di business denominato Tutti gli utenti oppure creare permessi per ciascun gruppo di business.</p> <p>Se si è eseguito l'accesso come manager del gruppo di business, è possibile creare permessi solo per il proprio gruppo di business.</p>
Utenti e gruppi	<p>Selezionare Tutti gli utenti e i gruppi per concedere il permesso per gli elementi del catalogo e le azioni a tutti i membri del gruppo di business. In alternativa, è possibile concedere il permesso a singoli utenti o gruppi. Per attivare un permesso è necessario selezionare almeno un utente di un gruppo di business o un gruppo.</p>

4 Fare clic su **Avanti**.

- 5 Fare clic sull'icona **Nuovo** (+) per autorizzare utenti alla richiesta di servizi, elementi di catalogo o azioni con questo permesso.

È possibile creare un permesso con varie combinazioni di servizi, elementi e azioni.

Opzione	Descrizione
Servizi autorizzati	<p>Aggiungere un servizio quando si desidera autorizzare gli utenti ad accedere a tutti gli elementi del catalogo pubblicati e associati al servizio.</p> <p>Un servizio autorizzato è un permesso dinamico. Se in un secondo momento si aggiunge un elemento al servizio, l'elemento verrà aggiunto al catalogo dei servizi per gli utenti autorizzati. I permessi possono includere sia servizi che singoli elementi di catalogo.</p>
Elementi e componenti del catalogo autorizzati	<p>Aggiungere singoli elementi disponibili agli utenti autorizzati.</p> <p>I permessi possono includere sia servizi che singoli elementi di catalogo. Per applicare un criterio di approvazione diverso a un elemento incluso nel servizio, aggiungerlo a un elemento del catalogo. In uno stesso permesso, il criterio di approvazione applicato a un elemento ha la precedenza rispetto al criterio di approvazione applicato al servizio a cui l'elemento appartiene. In permessi diversi, l'ordine dipende dall'ordine di precedenza impostato.</p> <p>Gli elementi del catalogo devono essere associati a un servizio per essere disponibili nel catalogo dei servizi. L'elemento del catalogo può essere associato a qualsiasi servizio, non solo a un servizio nel permesso corrente.</p> <p>I componenti sono una parte di un elemento del catalogo ma non sono disponibili per nome nel catalogo dei servizi. Ad esempio, il software MySQL è un componente dell'elemento del catalogo della macchina virtuale CentOS. I componenti sono autorizzati con l'elemento del catalogo. Se si desidera applicare un criterio di approvazione specifico per il software, è necessario autorizzare l'elemento singolarmente. Altrimenti, non è necessario autorizzare un componente per la sua distribuzione con l'elemento principale.</p>
Azioni autorizzate	<p>Aggiungere azioni quando si desidera permettere agli utenti di eseguire le azioni per un elemento fornito in provisioning.</p> <p>Le azioni che si desidera eseguire sugli elementi sottoposti a provisioning da questo permesso devono essere inclusi nello stesso permesso.</p> <p>Le azioni consentite non vengono visualizzate nel catalogo dei servizi. Vengono visualizzate nella scheda Distribuzioni per un elemento con provisioning.</p>
Le azioni si applicano solo agli elementi definiti in questo permesso	<p>Determina se le azioni sono autorizzate per tutti gli elementi del catalogo dei servizi applicabili o solo per gli elementi in questo permesso.</p> <p>Se questa opzione è selezionata, i membri del gruppo di business vengono autorizzati a eseguire le azioni per gli elementi applicabili inclusi nel permesso. Questo metodo di concedere l'autorizzazione per le azioni consente di specificare le azioni per i singoli elementi.</p> <p>Se l'opzione non è selezionata, gli utenti specificati nel permesso vengono autorizzati a eseguire le azioni per tutti gli elementi del catalogo applicabili, indipendentemente dalla loro inclusione nel permesso. Sono inoltre attivi eventuali criteri di approvazione applicati a queste azioni.</p>

- 6 Utilizzare i menu a discesa di ogni sezione per filtrare gli elementi disponibili.
- 7 Selezionare le caselle di controllo per includere elementi nel permesso.

- 8** Per aggiungere un criterio di approvazione al servizio, elemento o azione selezionata, selezionare un criterio di approvazione dal menu a discesa **Applicare questo criterio agli elementi selezionati**.

Se si applica un criterio di approvazione a un servizio, tutti gli elementi nel servizio avranno lo stesso criterio di approvazione. Per applicare un criterio diverso a un elemento, aggiungerlo come voce di catalogo e applicare il criterio appropriato.

- 9** Fare clic su **OK**.

Il servizio, l'azione o l'elemento viene aggiunto al permesso.

- 10** Fare clic su **Fine** per salvare il permesso.

Risultati

Se lo stato del permesso è attivo, il servizio e gli elementi vengono aggiunti al catalogo dei servizi.

Operazioni successive

Verificare che i servizi e gli elementi di catalogo autorizzati appaiano nel catalogo dei servizi per gli utenti autorizzati e che gli elementi richiesti eseguano il provisioning degli oggetti di destinazione come previsto. È possibile richiedere l'elemento a nome degli utenti selezionati.

Assegnare priorità ai permessi

Se esistono più permessi per lo stesso gruppo di business, è possibile assegnare priorità ai permessi. In questo modo, alla richiesta da parte di un utente di un catalogo di servizi, l'elaborazione del permesso e del criterio di approvazione associato verrà eseguita seguendo l'ordine specificato.

Se si configura un criterio di approvazione per un gruppo di utenti e si desidera che un membro del gruppo abbia un criterio unico per uno o più servizi, elementi del catalogo o azioni, assegnare al permesso del membro una priorità precedente rispetto al permesso del gruppo. Quando il membro richiede un elemento nel catalogo dei servizi, il criterio di approvazione applicato si basa sull'ordine di priorità dei permessi per il gruppo di business. Il criterio di approvazione applicato corrisponderà alla prima volta che viene trovato il nome del membro, ovvero come parte di un gruppo di utenti personalizzato o come utente individuale.

Supponiamo, ad esempio, che vengano creati due permessi per lo stesso elemento di catalogo, in modo da poter applicare un criterio di approvazione per il gruppo di utenti della contabilità e un criterio di approvazione differente per Chris, un membro di quel gruppo.

Tabella 3-71. Permessi di esempio

Permesso 1	Permesso 2
Gruppo di business: Finanze	Gruppo di business: Finanze
Utenti e gruppi: gruppo Contabilità	Utenti e gruppi: Chris
Elemento di catalogo 1: Criterio A	Elemento di catalogo 1: Criterio C

Chris richiede l'Elemento di catalogo 1 nel catalogo dei servizi. Alla richiesta di Chris viene applicato un criterio differente a seconda dell'ordine di priorità dei permessi del gruppo di business Finanze.


Tabella 3-72. Risultati dell'esempio

Configurazione e risultato	Ordine di priorità	Ordine di priorità
Ordine di priorità	1: Permesso 1 2: Permesso 2	1: Permesso 2 2: Permesso 1
Criterio applicato	Viene applicato il Criterio A. Chris è membro del gruppo di utenti Contabilità. La ricerca di Chris come utente autorizzato si interrompe al Permesso 1 e viene applicato il criterio di approvazione.	Viene applicato il Criterio C. La ricerca di Chris come utente autorizzato si interrompe al Permesso 2 e viene applicato il criterio di approvazione.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.
- 2 Fare clic sull'icona **Assegna priorità** ().
- 3 Selezionare un gruppo di business dall'elenco a discesa **Gruppo di business**.
- 4 Trascinare un permesso in una nuova posizione dell'elenco per cambiarne la priorità.
- 5 Selezionare un metodo di aggiornamento.

Opzione	Descrizione
Aggiorna	Salva le modifiche.
Aggiorna e chiudi	Salva le modifiche e chiude la finestra Assegna priorità elementi .

Utilizzo dei criteri di approvazione

I criteri di approvazione sono strumenti di governance che è possibile aggiungere alle richieste del catalogo dei servizi per poter gestire le risorse nell'ambiente. Ogni criterio è un set di condizioni definito che può essere applicato a servizi, elementi di catalogo e azioni quando si autorizzano utenti ad accedervi.

Processo dei criteri di approvazione

Come prima fase, un amministratore tenant o un amministratore approvazioni crea i criteri di approvazione dove occorre mantenere la governance sul provisioning.

I criteri di approvazione vengono creati per tipologie di criteri di approvazione o per elementi specifici. Se il criterio è basato su un tipo di criterio, è possibile applicarlo ai tipi di elementi di catalogo corrispondenti. Ad esempio, se un criterio è basato su un tipo di criterio software, è possibile definirlo per e applicarlo a qualsiasi elemento software presente nei permessi. Se il criterio è relativo a un elemento specifico, è applicabile solo a quell'elemento. Ad esempio, se l'elemento è un elemento software specifico, il criterio è applicabile solo a quello specifico elemento software di database nel permesso.

I criteri possono includere requisiti di pre-approvazione e di post-approvazione. Per la fase prima dell'approvazione, la richiesta deve essere approvata prima del provisioning dell'elemento richiesto. I criteri di post-approvazione devono invece essere approvati dall'utente approvatore prima che l'elemento con provisioning eseguito venga reso disponibile all'utente che lo richiede.

Le configurazioni prima e dopo l'approvazione sono costituite da uno o più livelli che definiscono quando deve essere attivato il criterio di approvazione e chi approva la richiesta o in che modo. È possibile includere più livelli. Ad esempio, un criterio di approvazione può avere un livello per l'approvazione da parte del manager, seguito da un livello per l'approvazione finanziaria.

In seconda fase, un amministratore tenant o un manager di un gruppo di business applica i criteri di approvazione a servizi, elementi di catalogo e azioni, secondo necessità.

Infine, quando un utente del catalogo dei servizi richiede un elemento a cui è applicato un criterio di approvazione, gli approvatori devono approvare o rifiutare la richiesta nella rispettiva scheda **Posta in arrivo**. L'utente richiedente può tenere traccia dello stato di approvazione di una specifica richiesta dalla propria scheda **Distribuzioni**.

Esempi di criteri di approvazione basati sul tipo di criterio macchina virtuale

È possibile creare un criterio di approvazione da applicare allo stesso tipo di elemento di catalogo, ma che produce risultati differenti quando un elemento è richiesto nel catalogo dei servizi. In base a come il criterio di approvazione è definito e applicato, l'effetto sull'utente del catalogo dei servizi e sull'approvatore cambia.

Nella tabella seguente sono riportati alcuni esempi di criteri di approvazione diversi, ma tutti basati sullo stesso tipo di criterio di approvazione. Gli esempi illustrano alcune modalità di configurazione dei criteri di approvazione per realizzare tipologie di governance differenti.

Tabella 3-73. Esempi di criteri di approvazione e risultati

Obiettivi governance	Tipo di criterio selezionato	Prima o dopo l'approvazione	Quando è richiesta l'approvazione	Chi sono gli approvatori	Come viene applicato il criterio nel permesso	Risultati alla richiesta dell'elemento nel catalogo dei servizi
Il manager del gruppo di business deve approvare tutte le richieste di macchine virtuali. Il criterio di approvazione deve essere applicabile per più gruppi di business in più permessi.	Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale	Aggiungere alla scheda Prima dell'approvazione	Selezionare Sempre necessaria	Selezionare Determina approvatori della richiesta. Selezionare la condizione Gruppo di business > Manager > Utenti > manager. Selezionare Chiunque può approvare.	I permessi si basano sui gruppi di business. Questa approvazione può essere utilizzata in qualsiasi permesso in cui è richiesta l'approvazione e del manager per la macchina virtuale.	Quando l'utente del catalogo dei servizi richiede una macchina virtuale a cui è stata applicata questa approvazione, il manager del gruppo di business deve approvare la richiesta prima che venga eseguito il provisioning della macchina.
L'amministratore dell'infrastruttura virtuale deve verificare la correttezza del provisioning della macchina virtuale e approvare la richiesta prima che la macchina virtuale venga rilasciata all'utente richiedente.	Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale	Aggiungere alla scheda Dopo l'approvazione	Selezionare Sempre necessaria	Selezionare Gruppi e utenti specifici. Selezionare il gruppo di utenti personalizzati degli amministratori dell'infrastruttura virtuale. Selezionare Chiunque può approvare.	Questa approvazione può essere utilizzata in qualsiasi permesso in cui si desidera che l'amministratore dell'infrastruttura controlli la macchina virtuale su vCenter Server dopo che è stato eseguito il provisioning.	Quando l'utente del catalogo dei servizi richiede una macchina virtuale a cui è stata applicata questa approvazione, viene eseguito il provisioning della macchina virtuale. Se tutti i membri del gruppo di amministrazione dell'infrastruttura virtuale approvano la richiesta, la macchina viene rilasciata all'utente.

Tabella 3-73. Esempi di criteri di approvazione e risultati (continua)

Obiettivi governance	Tipo di criterio selezionato	Prima o dopo l'approvazione	Quando è richiesta l'approvazione	Chi sono gli approvatori	Come viene applicato il criterio nel permesso	Risultati alla richiesta dell'elemento nel catalogo dei servizi
Per gestire le risorse dell'infrastruttura virtuale e controllare i prezzi, è possibile aggiungere due livelli di pre-approvazione, uno per le risorse della macchina e l'altro per il prezzo giornaliero della macchina.	Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale	Aggiungere alla scheda Prima dell'approvazione	Livello 1 Selezionare Necessaria in base alle condizioni. Configurare le condizioni in cui CPU > 6 o Memoria > 8 o Storage > 100 GB.	Selezionare Determina approvatori della richiesta. Selezionare la condizione Autore richiesta > manager. Selezionare . Fare clic su Proprietà di sistema e CPU Memoria e Storage in modo che l'approvatore possa cambiare il valore in un livello accettabile.	Questo criterio di approvazione può essere utilizzato in un permesso in cui si desidera che la richiesta venga approvata dal manager dell'utente e da un membro del reparto finanze.	Quando l'utente del catalogo dei servizi richiede una macchina virtuale, la richiesta viene valutata per determinare se le quantità di CPU, memoria o storage richieste superano le quantità specificate nel livello 1. In caso contrario, viene valutata la condizione di livello 2. Se le richieste superano almeno una delle condizioni di livello 1, il manager deve approvare la richiesta. Il manager può ridurre le quantità della configurazione richieste e approvarle oppure rifiutare la richiesta.

Tabella 3-73. Esempi di criteri di approvazione e risultati (continua)

Obiettivi governance	Tipo di criterio selezionato	Prima o dopo l'approvazione	Quando è richiesta l'approvazione	Chi sono gli approvatori	Come viene applicato il criterio nel permesso	Risultati alla richiesta dell'elemento nel catalogo dei servizi
			Livello 2 Selezionare Necessaria in base alle condizioni. Configurare la condizione Prezzo > 15,00 al giorno.	Selezionare Gruppi e utenti specifici. Selezionare il gruppo di utenti personalizzati delle finanze. Selezionare Chiunque può approvare.		
Per gli elementi del catalogo di blueprint con parametri, è necessario che un amministratore e cloud approvi le richieste di distribuzione in cui il profilo size di un componente della macchina vSphere è impostato su Large.	Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale	Aggiungere alla scheda Prima dell'approvazione	Livello 1 Selezionare Necessaria in base alle condizioni. Livello 2 Selezionare Condizione singola. Selezionare Profilo componente > Dimensione macchina vSphere. Configurare la dimensione della condizione su "large" (grande).	Selezionare Gruppi e utenti specifici. Selezionare gli utenti e i gruppi che possono approvare la richiesta. Selezionare Chiunque può approvare.	Questo criterio di approvazione può essere utilizzato in un permesso in cui si desidera che un amministratore cloud approvi la richiesta di provisioning.	Quando l'utente del catalogo dei servizi richiede una macchina virtuale a cui è stata applicata questa approvazione, un amministratore e cloud deve approvare la richiesta prima che venga eseguito il provisioning della macchina.

Esempio di azioni con criteri di approvazione applicati in una distribuzione composita

Quando si applicano criteri di approvazione ad azioni che possono essere eseguite su vari componenti in un blueprint composito, il processo di approvazione varia a seconda della configurazione del permesso e della modalità di applicazione dei criteri di approvazione.

Questo esempio utilizza dettagli specifici per creare il blueprint e applicare quindi criteri di approvazione alle azioni che possono essere eseguite dal catalogo dei servizi sul blueprint di cui viene eseguito il provisioning in diversi permessi. Il blueprint è composito e include un altro blueprint. Con le azioni utilizzate vengono eliminati gli elementi di cui è stato eseguito il provisioning, una distribuzione per i blueprint e una macchina virtuale per la macchina. Il comportamento risultante include ciò che viene eliminato e quando i criteri di approvazione applicati attivano richieste di approvazione.

Blueprint di esempio

In questo esempio, viene configurato un blueprint che include un blueprint nidificato con una macchina virtuale.

- Blueprint 1 - Blueprint di integrazione continua
 - Blueprint 2 - Blueprint di pre-produzione
 - Macchina virtuale 1 - Macchina virtuale TestAsAService di vSphere

Criteri di approvazione per azioni di eliminazione

Vengono configurati due criteri di approvazione per l'eliminazione degli elementi di cui è stato eseguito il provisioning. In questo esempio un'azione Elimina - Distribuzione può essere eseguita su Blueprint 1 o Blueprint 2. Un'azione Elimina - Macchina virtuale può essere eseguita su Macchina virtuale 1. Si creano quindi i criteri di approvazione da applicare alle azioni nel permesso.

Nome criterio di approvazione	Tipo criterio di approvazione
Criterio di approvazione A	Catalogo dei servizi - Richiesta azione risorsa - Elimina - Distribuzione
Criterio di approvazione B	Catalogo dei servizi - Richiesta azione risorsa - Elimina - Macchina virtuale

Permessi e criteri di approvazione applicati alle azioni

Si devono configurare tre permessi. Ogni permesso include il blueprint composito. In ogni permesso si aggiungono le azioni di eliminazione e si applicano i criteri di approvazione.

Nome permesso	Azione autorizzata sulla macchina di cui è stato eseguito il provisioning	Criterio di approvazione applicato
Permesso 1	Elimina - Distribuzione	Criterio di approvazione A
Permesso 2	Elimina - Macchina virtuale	Criterio di approvazione B
Permesso 3	Elimina - Distribuzione	Criterio di approvazione A
	Elimina - Macchina virtuale	Criterio di approvazione B

Azioni utente nel catalogo dei servizi

Quando l'utente del catalogo dei servizi esegue l'azione, le macchine o i blueprint vengono eliminati in base all'elemento sul quale l'utente ha eseguito l'azione.

Azione utente nel catalogo dei servizi	Azione selezionata	Macchine o blueprint eliminati
Azione 1	Azione Elimina - Distribuzione eseguita su Blueprint 1 - Blueprint integrazione continua	Blueprint 1, Blueprint 2 e Macchina virtuale 1
Azione 2	Azione Elimina - Distribuzione eseguita su Blueprint 2 - Blueprint di pre-produzione	Blueprint 2 e Macchina virtuale 1
Azione 3	Azione Elimina - Macchina virtuale eseguita sulla macchina nella distribuzione, Macchina virtuale 1 - Macchina virtuale TestAsAService di vSphere	Macchina virtuale 1

Criteri di approvazione applicati ad azioni nei permessi

Si applicano i criteri di approvazione. Gli approvatori ricevono una richiesta di approvazione in base al blueprint o alla macchina su cui l'utente del catalogo dei servizi esegue l'azione.

Nome permesso	Criterio di approvazione su azioni	Azione dell'utente	Richiesta di approvazione attivata	In caso di approvazione, blueprint o macchine eliminati
Permesso 1 - Criterio di approvazione per Elimina distribuzione	Criterio A (Criterio di approvazione per Elimina distribuzione) solo sull'azione Elimina - Distribuzione	Azione 1 (Esegue l'azione Elimina - Distribuzione su Blueprint 1)	Le richieste di approvazione sono attivate solo per Blueprint 1	Blueprint 1, Blueprint 2 e Macchina virtuale 1
		Azione 2 (Esegue l'azione Elimina - Distribuzione su Blueprint 2)	Le richieste di approvazione sono attivate solo per Blueprint 2	Blueprint 2 e Macchina virtuale 1
		Azione 3 (Azione Elimina - Macchina virtuale eseguita su Macchina virtuale 1)	Non viene attivata alcuna richiesta di approvazione	Macchina virtuale 1
Permesso 2	Criterio B (Criterio Elimina - Macchina virtuale) solo sull'azione Elimina - Macchina virtuale	Azione 1 (Esegue l'azione Elimina - Distribuzione su Blueprint 1)	Non viene attivata alcuna richiesta di approvazione	Blueprint 1, Blueprint 2 e Macchina virtuale 1
		Azione 2 (Esegue l'azione Elimina - Distribuzione su Blueprint 2)	Non viene attivata alcuna richiesta di approvazione	Blueprint 2 e Macchina virtuale 1
		Azione 3 (Azione Elimina - Macchina virtuale eseguita su Macchina virtuale 1)	Le richieste di approvazione sono attivate solo per Macchina virtuale 1	Macchina virtuale 1

Nome permesso	Criterio di approvazione su azioni	Azione dell'utente	Richiesta di approvazione attivata	In caso di approvazione, blueprint o macchine eliminati
Permesso 3	Criterio A (Criterio di approvazione per Elimina distribuzione) sull'azione Elimina - Distribuzione e Criterio B (Criterio Elimina - Macchina virtuale) sull'azione Elimina - Macchina virtuale	Azione 1 (Esegue l'azione Elimina - Distribuzione su Blueprint 1)	Le richieste di approvazione sono attivate solo per Blueprint 1	Blueprint 1, Blueprint 2 e Macchina virtuale 1
		Azione 2 (Esegue l'azione Elimina - Distribuzione su Blueprint 2)	Le richieste di approvazione sono attivate solo per Blueprint 2	Blueprint 2 e Macchina virtuale 1
		Azione 3 (Azione Elimina - Macchina virtuale eseguita su Macchina virtuale 1)	Le richieste di approvazione sono attivate solo per Macchina virtuale 1	Macchina virtuale 1

Esempio di criterio di approvazione in permessi multipli

Se si applica un criterio di approvazione a un elemento utilizzato in più permessi rilasciati agli stessi utenti di un gruppo di business, il criterio di approvazione viene attivato sull'elemento anche nel servizio in cui il criterio di approvazione non sia stato applicato esplicitamente nel permesso.

Si supponga ad esempio che vengano creati i seguenti blueprint, servizi, criteri di approvazione e permessi.

Blueprint

- Macchina virtuale RHEL di vSphere
- QE Testing con macchina virtuale RHEL di vSphere
- QE Training con macchina virtuale RHEL di vSphere

Servizi

- Il blueprint QE Testing è associato al servizio Testing
- Il blueprint QE Training è associato al servizio Training

Permessi

- Permesso 1
- Permesso 2

Tabella 3-74. Configurazioni dei permessi

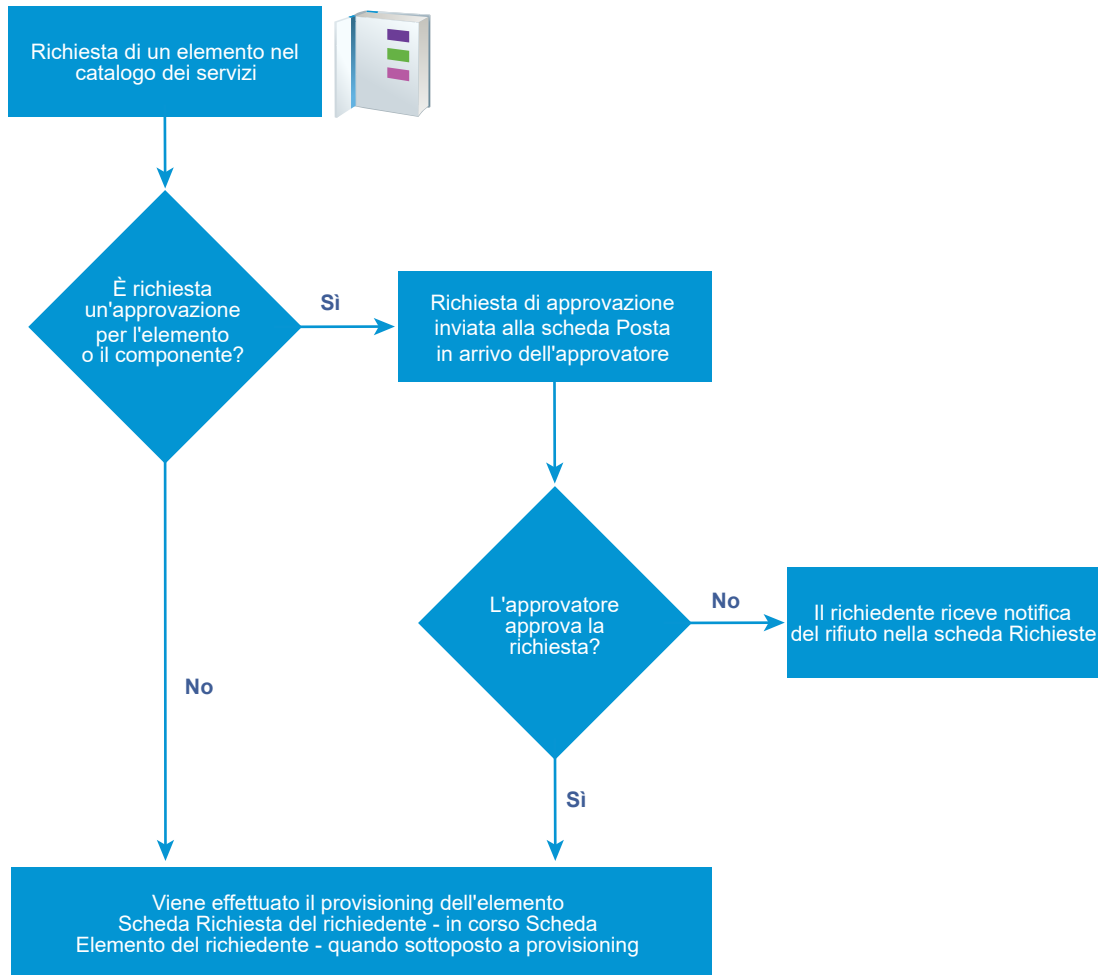
Nome permesso	Gruppo di business	Servizio autorizzato	Elemento autorizzato
Permesso 1	QE	Testing	Richiesta di elemento del catalogo - Macchina virtuale applicata al componente Macchina virtuale
Permesso 2	QE	Training	

Risultati

Quando l'utente seleziona QE Training nel catalogo dei servizi, il criterio di approvazione viene attivato per la macchina virtuale RHEL di vSphere, perché si tratta di un blueprint basato su un componente macchina virtuale utilizzato nel blueprint QE Training.

Elaborazione dei criteri di approvazione nel catalogo dei servizi

Quando un utente richiede un elemento del catalogo dei servizi al quale è applicato un criterio di approvazione, la richiesta viene elaborata dall'approvatore e dall'utente richiedente in base a un workflow simile a quello mostrato di seguito.



Creazione di un criterio di approvazione

Gli amministratori tenant o amministratori approvazioni possono definire i criteri di approvazione e utilizzarli nei permessi. I criteri di approvazione possono essere configurati con più livelli per eventi di pre-approvazione e post-approvazione.

Se si modifica un'impostazione in un blueprint di componente software e un criterio di approvazione utilizza tale impostazione per attivare una richiesta di approvazione, il criterio di approvazione potrebbe non funzionare correttamente. Qualora sia necessario modificare un'impostazione di un componente, accertarsi che le modifiche non influiscano su eventuali criteri di approvazione.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant** o **amministratore approvazioni**.

Procedura

1 Definizione di informazioni sui criteri di approvazione

Quando si crea un criterio di approvazione, definire il tipo, il nome, la descrizione e lo stato del criterio di approvazione.

2 Creazione di un livello di approvazione

Quando si crea un criterio di approvazione, è possibile aggiungere livelli di pre-approvazione e post-approvazione.

3 Configurazione del modulo di approvazione con proprietà di sistema e personalizzate

È possibile aggiungere proprietà di sistema e personalizzate da visualizzare sul modulo di approvazione. Prima di completare una richiesta di approvazione, gli approvatori potranno quindi cambiare i valori delle proprietà di sistema per le impostazioni delle risorse della macchina quali CPU o memoria, nonché le proprietà personalizzate.

4 Impostazioni dei criteri di approvazione

Quando si crea un criterio di approvazione, si configurano varie opzioni che determinano se un elemento richiesto dagli utenti di un catalogo di servizi debba essere approvato o meno. L'approvazione può essere richiesta prima che la richiesta avvii il provisioning oppure dopo il provisioning dell'elemento ma prima che questo venga rilasciato al richiedente.

Definizione di informazioni sui criteri di approvazione

Quando si crea un criterio di approvazione, definire il tipo, il nome, la descrizione e lo stato del criterio di approvazione.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant** o **amministratore approvazioni**.

Procedura

- 1 Selezionare **Amministrazione > Criteri di approvazione**.
- 2 Fare clic sull'icona **Nuovo** (+).

3 Selezionare un tipo di criterio o un componente software.

Opzione	Descrizione
Seleziona un tipo di criterio di approvazione	<p>Consente di creare un criterio di approvazione in base al tipo di richiesta di criterio.</p> <p>Selezionare questa opzione per definire un criterio di approvazione applicabile a tutti gli elementi del catalogo di quel tipo. La richiesta può essere di tipo generico, elemento di catalogo o azione su risorsa.</p> <p>Le opzioni disponibili per la configurazione delle condizioni dipendono dal tipo di richiesta. Più è specifico il tipo, più sono specifici i campi della configurazione. Ad esempio, Catalogo dei servizi - Richiesta di elemento del catalogo fornisce solo i campi comuni a tutte le richieste di elementi del catalogo. Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale include le opzioni comuni e quelle specifiche per le macchine virtuali.</p> <p>Il tipo di richiesta limita gli elementi di catalogo o le azioni a cui è possibile applicare il criterio di approvazione.</p>
Seleziona un elemento	<p>Consente di creare un criterio di approvazione basato su un elemento specifico.</p> <p>Selezionare questa opzione per definire un criterio di approvazione applicabile a elementi specifici non disponibili come elementi singoli nel catalogo dei servizi, ma solo come parte di una macchina o di un'altra distribuzione. Un esempio di tali elementi sono i componenti software.</p> <p>I campi disponibili per la configurazione delle condizioni sono specifici dell'elemento e possono essere più dettagliati rispetto ai criteri disponibili per un elemento di tipo criterio.</p>
Elenco	<p>Elenco dei tipi di criteri o degli elementi di catalogo disponibili.</p> <p>Per individuare un elemento o un tipo specifico, effettuare una ricerca oppure ordinare le colonne.</p>

4 Fare clic su **OK**.

5 Immettere un nome e, facoltativamente, una descrizione.

6 Selezionare lo stato del criterio dal menu a discesa **Stato**.

Opzione	Descrizione
Bozza	Salva il criterio di approvazione in uno stato modificabile.
Attivo	Salva il criterio di approvazione in uno stato di sola lettura che è possibile utilizzare in un permesso.
Inattivo	Salva il criterio di approvazione in uno stato di sola lettura che non è possibile utilizzare in un permesso finché non si attiva il criterio.

Operazioni successive

Creare i livelli Prima dell'approvazione e Dopo l'approvazione.

Creazione di un livello di approvazione

Quando si crea un criterio di approvazione, è possibile aggiungere livelli di pre-approvazione e post-approvazione.

È possibile creare più livelli di approvazione per un criterio di approvazione. Quando un utente del catalogo dei servizi richiede un elemento a cui è stato applicato un criterio di approvazione con più livelli, ogni approvazione di primo livello deve essere accettata prima che la richiesta possa essere trasmessa all'approvatore successivo. Vedere [Utilizzo dei criteri di approvazione](#).

Se si configura un criterio di approvazione attivato da una richiesta di durata di lease, è necessario selezionare **Sempre necessaria** come richiesta di approvazione.

Prerequisiti

[Definizione di informazioni sui criteri di approvazione](#).

Procedura

- 1 Nella scheda **Prima dell'approvazione** o **Dopo l'approvazione**, fare clic sull'icona **Nuovo** (+).
- 2 Immettere un nome e, facoltativamente, una descrizione.
- 3 Selezionare un requisito di approvazione.

Opzione	Descrizione
Sempre necessaria	Il criterio di approvazione viene attivato per ogni richiesta.
Necessaria in base alle condizioni	<p>Il criterio di approvazione si basa su una o più clausole di condizioni.</p> <p>Se si seleziona questa opzione, è necessario creare le relative condizioni. Quando si applica questo criterio di approvazione a servizi, azioni o elementi di catalogo idonei in un permesso, le condizioni vengono valutate. Se le condizioni sono soddisfatte, prima del provisioning la richiesta deve essere approvata tramite il metodo di approvazione specificato. Se le condizioni non sono soddisfatte, viene eseguito il provisioning della richiesta senza che sia necessaria alcuna approvazione. Ad esempio, tutte le richieste per una macchina virtuale con 4 o più CPU devono essere approvate dall'amministratore dell'infrastruttura virtuale.</p> <p>I campi disponibili per la definizione delle condizioni dipendono dal tipo di criterio di approvazione o dall'elemento di catalogo selezionato.</p> <p>Nei valori immessi per le condizioni viene fatta distinzione tra maiuscole e minuscole.</p> <p>Per configurare più clausole di condizioni, selezionare l'operazione booleana desiderata.</p>

4 Selezionare gli approvatori.

Opzione	Azione
Gruppi e utenti specifici	La richiesta di approvazione viene inviata agli utenti selezionati.
Determina approvatori della richiesta	<p>La richiesta di approvazione viene inviata agli utenti in base alla condizione specificata.</p> <p>Nota Assicurarsi che tutti gli utenti che saranno determinati dinamicamente dalla richiesta e dal richiedente esistano in vRealize Automation, che siano sincronizzati in Active Directory e che siano presenti in Amministrazione > Utenti e gruppi > Utenti e gruppi della directory.</p> <p>Se un utente non è sincronizzato nel provider di identità di Gestione directory e durante la richiesta del catalogo si fa in qualche modo riferimento a questo utente, la richiesta avrà esito negativo e terminerà con un errore di runtime correlato all'approvazione dell'elemento richiesto.</p>
Usa sottoscrizione evento	<p>Consente di elaborare la richiesta di approvazione in base alle sottoscrizioni evento definite.</p> <p>La sottoscrizione del workflow deve essere definita in Amministrazione > Eventi > Sottoscrizioni. Le sottoscrizioni dei workflow applicabili sono Prima dell'approvazione e Dopo l'approvazione.</p>

5 Indicare chi deve approvare la richiesta o azione.

Opzione	Descrizione
Chiunque può approvare	<p>Per poter essere elaborata, è sufficiente che la richiesta venga approvata da uno solo degli approvatori.</p> <p>Quando l'elemento viene richiesto nel catalogo dei servizi, la richiesta di approvazione viene inviata a tutti gli approvatori. Una volta approvata da un approvatore, la richiesta è considerata approvata e viene rimossa dalla Posta in arrivo degli altri approvatori.</p>
Tutti devono approvare	Per poter essere elaborata, la richiesta deve essere approvata da tutti gli approvatori specificati.

6 Aggiungere le proprietà a un modulo di approvazione o salvare il livello.

- Per aggiungere proprietà al modulo di approvazione, fare clic su **Proprietà di sistema** o **Proprietà personalizzate**.
- Per salvare il livello, fare clic su **OK**.

Operazioni successive

Per aggiungere proprietà al modulo di approvazione, vedere [Configurazione del modulo di approvazione con proprietà di sistema e personalizzate](#).

Configurazione del modulo di approvazione con proprietà di sistema e personalizzate

È possibile aggiungere proprietà di sistema e personalizzate da visualizzare sul modulo di approvazione. Prima di completare una richiesta di approvazione, gli approvatori potranno quindi

cambiare i valori delle proprietà di sistema per le impostazioni delle risorse della macchina quali CPU o memoria, nonché le proprietà personalizzate.

Le proprietà di sistema disponibili dipendono dal tipo di criterio di approvazione e dalla configurazione del blueprint. Per alcune proprietà, il campo configurato nel blueprint deve includere un valore massimo e uno minimo prima che la proprietà venga elencata tra le proprietà di sistema.

Le proprietà personalizzate possono essere aggiunte quando si definisce il livello di approvazione. Se una proprietà personalizzata viene configurata e aggiunta a un blueprint, le proprietà personalizzate aggiunte al modulo di approvazione sovrascrivono ogni eventuale altra istanza di tale proprietà personalizzata, ad esempio in blueprint, gruppi di proprietà o endpoint.

L'approvatore può modificare le proprietà selezionate o configurate nel modulo di approvazione.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **amministratore approvazioni**.
- [Creazione di un livello di approvazione](#).

Procedura

- 1 Nella scheda **Prima dell'approvazione** o **Dopo l'approvazione**, fare clic sull'icona **Nuovo** (+).
- 2 Fare clic sulla scheda **Proprietà di sistema**.
- 3 Selezionare la casella di controllo di ciascuna proprietà di sistema che l'approvatore potrà configurare durante il processo di approvazione.
- 4 Configurare le proprietà personalizzate.

Aggiungere una o più proprietà personalizzate che l'approvatore potrà configurare durante il processo di approvazione.

- a Fare clic sulla scheda **Proprietà personalizzate**.
- b Fare clic sull'icona **Nuovo** (+).
- c Immettere i valori delle proprietà personalizzate.

Opzione	Descrizione
Nome	Specificare il nome della proprietà.
Etichetta	Immettere l'etichetta che viene presentata all'approvatore nel modulo di approvazione.
Descrizione	Immettere informazioni estese per l'approvatore. Queste verranno visualizzate come una descrizione di comando del campo nel modulo.

d Fare clic su **Salva**.

e Per eliminare più proprietà personalizzate, selezionare le righe corrispondenti e fare clic su **Elimina**.

5 Fare clic su **OK**.

Operazioni successive

- Aggiungere livelli di pre-approvazione o post-approvazione aggiuntivi.
- Salvare il criterio di approvazione. Il criterio deve essere attivo per poter essere applicato a servizi, elementi o azioni nei **Permessi**.

Impostazioni dei criteri di approvazione

Quando si crea un criterio di approvazione, si configurano varie opzioni che determinano se un elemento richiesto dagli utenti di un catalogo di servizi debba essere approvato o meno.

L'approvazione può essere richiesta prima che la richiesta avvii il provisioning oppure dopo il provisioning dell'elemento ma prima che questo venga rilasciato al richiedente.

Selezionare **Amministrazione > Criteri di approvazione**. Fare clic su **Nuovo**.

■ [Impostazioni dei tipi di criteri di approvazione](#)

Il tipo di un criterio di approvazione determina il modo in cui il criterio di approvazione viene configurato e a quali elementi o azioni può essere applicato nel permesso. Quando si aggiungono dei livelli di approvazione, i campi disponibili per la creazione delle condizioni per i livelli di approvazione dipendono dal tipo di criterio o elemento.

■ [Aggiunta di impostazioni dei criteri di approvazione](#)

È possibile gestire un criterio di approvazione dopo averne configurato le informazioni di base, incluso lo stato.

■ [Aggiunta di informazioni sui livelli alle impostazioni dei criteri di approvazione](#)

Un livello di approvazione contiene le condizioni che attivano un processo di approvazione quando l'utente del catalogo dei servizi richiede l'elemento, insieme a tutte le proprietà di sistema e le proprietà personalizzate che si desidera includere. Quante attivate, le richieste di approvazione vengono inviate agli approvatori designati.

■ [Aggiunta di proprietà di sistema alle impostazioni dei criteri di approvazione](#)

È possibile selezionare proprietà di sistema da aggiungere al modulo di approvazione e permettere così all'approvatore di modificarne i valori.

■ [Aggiunta di proprietà personalizzate alle impostazioni dei criteri di approvazione](#)

È possibile configurare proprietà personalizzate da aggiungere al modulo di approvazione e permettere così all'approvatore di modificarne i valori.

Impostazioni dei tipi di criteri di approvazione

Il tipo di un criterio di approvazione determina il modo in cui il criterio di approvazione viene configurato e a quali elementi o azioni può essere applicato nel permesso. Quando si aggiungono

dei livelli di approvazione, i campi disponibili per la creazione delle condizioni per i livelli di approvazione dipendono dal tipo di criterio o elemento.

Selezionare **Amministrazione > Criteri di approvazione**. Fare clic su **Nuovo**.

Tabella 3-75. Opzioni dei tipi di criteri di approvazione

Opzione	Descrizione
Seleziona un tipo di criterio di approvazione	<p>Consente di creare un criterio di approvazione in base al tipo di richiesta di criterio.</p> <p>Selezionare questa opzione per definire un criterio di approvazione applicabile a tutti gli elementi del catalogo di quel tipo. La richiesta può essere di tipo generico, elemento di catalogo o azione su risorsa.</p> <p>Le opzioni disponibili per la configurazione delle condizioni dipendono dal tipo di richiesta. Più è specifico il tipo, più sono specifici i campi della configurazione. Ad esempio, Catalogo dei servizi - Richiesta di elemento del catalogo fornisce solo i campi comuni a tutte le richieste di elementi del catalogo. Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale include le opzioni comuni e quelle specifiche per le macchine virtuali.</p> <p>Il tipo di richiesta limita gli elementi di catalogo o le azioni a cui è possibile applicare il criterio di approvazione.</p>
Seleziona un elemento	<p>Consente di creare un criterio di approvazione basato su un elemento specifico.</p> <p>Selezionare questa opzione per definire un criterio di approvazione applicabile a elementi specifici non disponibili come elementi singoli nel catalogo dei servizi, ma solo come parte di una macchina o di un'altra distribuzione. Un esempio di tali elementi sono i componenti software.</p> <p>I campi disponibili per la configurazione delle condizioni sono specifici dell'elemento e possono essere più dettagliati rispetto ai criteri disponibili per un elemento di tipo criterio.</p>
Elenco	<p>Elenco dei tipi di criteri o degli elementi di catalogo disponibili.</p> <p>Per individuare un elemento o un tipo specifico, effettuare una ricerca oppure ordinare le colonne.</p>

Aggiunta di impostazioni dei criteri di approvazione

È possibile gestire un criterio di approvazione dopo averne configurato le informazioni di base, incluso lo stato.

Per definire le informazioni di base dei criteri di approvazione, selezionare **Amministrazione > Criteri di approvazione**. Fare clic su **Nuovo**. Selezionare il tipo di criterio e scegliere **OK**.

Tabella 3-76. Opzioni dei criteri di approvazione

Opzione	Descrizione
Nome	Nome visualizzato quando si applica il criterio di approvazione in un permesso.
Descrizione	Immettere una descrizione dettagliata sulle caratteristiche del criterio di approvazione. Queste informazioni saranno utili nelle attività di gestione dei criteri di approvazione.
Stato	<p>I valori possibili includono:</p> <ul style="list-style-type: none"> ■ Bozza. Il criterio di approvazione non è disponibile per l'applicazione nei permessi. Per un criterio attivo non può più essere impostato lo stato Bozza. ■ Attivo. Il criterio di approvazione è disponibile per l'applicazione nei permessi. ■ Inattivo. Il criterio di approvazione non è disponibile per l'applicazione nei permessi. Se un criterio che non è stato applicato ad alcun permesso viene reso inattivo, sarà possibile eliminarlo ma non riattivarlo. Se il criterio è stato applicato e lo si rende inattivo, gli elementi ai quali si applica devono essere collegati a un criterio diverso o risulteranno scollegati. Le azioni e gli elementi scollegati risultano comunque accessibili per gli utenti, ma ad essi non è applicato alcun criterio di approvazione.
Tipo di criterio	<p>Visualizza il tipo di richiesta del criterio di approvazione.</p> <p>Se è stato selezionato un elemento di catalogo su cui basare il criterio di approvazione, viene visualizzato il tipo di richiesta associato.</p>
Elemento	<p>Visualizza l'elemento del catalogo selezionato.</p> <p>Se è stato selezionato un tipo di richiesta su cui basare il criterio di approvazione, questo campo è vuoto.</p>
Autore ultimo aggiornamento	Nome dell'utente che ha apportato modifiche al criterio di approvazione.
Data ultimo aggiornamento	Data dell'ultima modifica al criterio di approvazione.
Livello Prima dell'approvazione	Per richiedere l'approvazione prima che venga eseguito il provisioning degli elementi richiesti o che vengano eseguite le azioni, configurare una o più condizioni che attivino un processo di approvazione quando l'utente del catalogo dei servizi richiede l'elemento.

Tabella 3-76. Opzioni dei criteri di approvazione (continua)

Opzione	Descrizione
Livello Dopo l'approvazione	<p>Per richiedere l'approvazione dopo che è stato eseguito il provisioning dell'elemento ma prima che l'elemento di cui è stato eseguito il provisioning o che è stato modificato venga rilasciato all'utente del catalogo dei servizi richiedente, configurare una o più condizioni che attivino un processo di approvazione.</p> <p>Ad esempio, l'amministratore dell'infrastruttura virtuale verifica che la macchina virtuale sia in uno stato operativo prima di rilasciarla all'utente del catalogo dei servizi.</p>
Visualizza permessi collegati	<p>Visualizza tutti i permessi in cui il criterio di approvazione è applicato a servizi, elementi di catalogo o azioni. È possibile collegare gli elementi in un permesso a un criterio differente.</p> <p>Questa opzione è disponibile solo quando si visualizza un criterio di approvazione attivo.</p>

Aggiunta di informazioni sui livelli alle impostazioni dei criteri di approvazione

Un livello di approvazione contiene le condizioni che attivano un processo di approvazione quando l'utente del catalogo dei servizi richiede l'elemento, insieme a tutte le proprietà di sistema e le proprietà personalizzate che si desidera includere. Quante attivate, le richieste di approvazione vengono inviate agli approvatori designati.

Per definire le informazioni di base dei criteri di approvazione, selezionare **Amministrazione > Criteri di approvazione**. Fare clic su **Nuovo**. Selezionare il tipo di criterio e scegliere **OK**. Nella scheda Prima dell'approvazione o nella scheda Dopo l'approvazione, fare clic sull'icona **Nuovo** (+).

È possibile definire le priorità dei livelli in base all'ordine in cui si desidera che vengano elaborati. All'attivazione del criterio di approvazione, se il primo livello dell'approvazione viene rifiutato, la richiesta viene rifiutata.

Tabella 3-77. Opzioni per le informazioni sul livello

Opzione	Descrizione
Nome	<p>Immettere un nome.</p> <p>Il nome del livello viene visualizzato durante la revisione delle richieste con criteri di approvazione.</p>
Descrizione	<p>Immettere una descrizione del livello.</p> <p>Esempio: CPU>4 a VI Admin.</p>
Quando è richiesta l'approvazione?	Selezionare quando deve essere attivato il criterio di approvazione.

Tabella 3-77. Opzioni per le informazioni sul livello (continua)

Opzione	Descrizione
Sempre necessaria	<p>Il criterio di approvazione viene attivato per ogni richiesta. Se si seleziona questa opzione e si applica questo criterio di approvazione a servizi, elementi di catalogo o azioni idonei in un permesso, prima del provisioning la richiesta dovrà essere approvata tramite il metodo di approvazione specificato. Ad esempio, tutte le richieste devono essere approvate dal manager dell'utente che ha inoltrato la richiesta.</p>
Necessaria in base alle condizioni	<p>Il criterio di approvazione si basa su una o più clausole di condizioni.</p> <p>Se si seleziona questa opzione, è necessario creare le relative condizioni. Quando si applica questo criterio di approvazione a servizi, azioni o elementi di catalogo idonei in un permesso, le condizioni vengono valutate. Se le condizioni sono soddisfatte, prima del provisioning la richiesta deve essere approvata tramite il metodo di approvazione specificato. Se le condizioni non sono soddisfatte, viene eseguito il provisioning della richiesta senza che sia necessaria alcuna approvazione. Ad esempio, tutte le richieste per una macchina virtuale con 4 o più CPU devono essere approvate dall'amministratore dell'infrastruttura virtuale.</p> <p>I campi disponibili per la definizione delle condizioni dipendono dal tipo di criterio di approvazione o dall'elemento di catalogo selezionato.</p> <p>Nei valori immessi per le condizioni viene fatta distinzione tra maiuscole e minuscole.</p> <p>Per configurare più clausole di condizioni, selezionare l'operazione booleana desiderata.</p> <ul style="list-style-type: none"> ■ Tutti tra i seguenti. L'approvazione viene attivata quando tutte le clausole sono vere. Corrisponde all'operatore booleano AND tra ciascuna clausola. ■ Qualsiasi tra i seguenti. Il livello di approvazione viene attivato quando è vera almeno una delle clausole. Corrisponde all'operatore booleano OR tra ciascuna clausola. ■ Non i seguenti. Il livello di approvazione viene attivato quando nessuna delle clausole è vera. Corrisponde all'operatore booleano NOT tra ciascuna clausola.
Approvatori	Selezionare il metodo di approvazione.
Gruppi e utenti specifici	<p>La richiesta di approvazione viene inviata agli utenti selezionati.</p> <p>Selezionare gli utenti o i gruppi di utenti che devono approvare la richiesta del catalogo dei servizi prima che si possa procedere all'esecuzione del provisioning o di un'azione. Ad esempio, se si seleziona Chiunque può approvare la richiesta viene inoltrata al gruppo degli amministratori dell'infrastruttura virtuale.</p>

Tabella 3-77. Opzioni per le informazioni sul livello (continua)

Opzione	Descrizione
Determina approvatori della richiesta	<p>La richiesta di approvazione viene inviata agli utenti in base alla condizione specificata.</p> <p>Ad esempio, se si applica questo criterio di approvazione a diversi gruppi di business e si desidera che il manager del gruppo di business approvi la richiesta, selezionare Gruppo di business > Consumatore > Utenti > Manager.</p>
Usa sottoscrizione evento	<p>Consente di elaborare la richiesta di approvazione in base alle sottoscrizioni evento definite.</p> <p>La sottoscrizione del workflow deve essere definita in Amministrazione > Eventi > Sottoscrizioni. Le sottoscrizioni dei workflow applicabili sono Prima dell'approvazione e Dopo l'approvazione.</p>
Chiunque può approvare	<p>Per poter essere elaborata, è sufficiente che la richiesta venga approvata da uno solo degli approvatori.</p> <p>Quando l'elemento viene richiesto nel catalogo dei servizi, la richiesta di approvazione viene inviata a tutti gli approvatori. Una volta approvata da un approvatore, la richiesta è considerata approvata e viene rimossa dalla Posta in arrivo degli altri approvatori.</p> <p>Se il primo approvatore la rifiuta, l'utente richiedente riceve una notifica del rifiuto e la richiesta di approvazione viene rimossa dalla Posta in arrivo degli approvatori.</p> <p>Se il primo approvatore approva la richiesta mentre questa è aperta anche nella console del secondo approvatore, quest'ultimo non può procedere all'invio in quanto la richiesta di approvazione viene considerata già completata dal primo approvatore.</p> <p>Questa è una delle opzioni aggiuntive disponibili se si seleziona Gruppi e utenti specifici o Determina approvatori della richiesta e sono presenti più approvatori. Se esiste un solo approvatore, questa opzione non è applicabile.</p>
Tutti devono approvare	<p>Per poter essere elaborata, la richiesta deve essere approvata da tutti gli approvatori specificati.</p> <p>Questa è una delle opzioni aggiuntive disponibili se si seleziona Gruppi e utenti specifici o Determina approvatori della richiesta e sono presenti più approvatori. Se esiste un solo approvatore, questa opzione non è applicabile.</p>

Aggiunta di proprietà di sistema alle impostazioni dei criteri di approvazione

È possibile selezionare proprietà di sistema da aggiungere al modulo di approvazione e permettere così all'approvatore di modificarne i valori.

Ad esempio, per un'approvazione di una macchina virtuale, selezionare CPU per permettere all'approvatore di modificare una richiesta di 6 CPU a 4 CPU.

Per selezionare proprietà di sistema, scegliere **Amministrazione > Criteri di approvazione**. Fare clic su **Nuovo**. Selezionare il tipo di criterio e scegliere **OK**. Nella scheda Prima dell'approvazione o nella scheda Dopo l'approvazione, fare clic sull'icona **Nuovo (+)** e scegliere la scheda **Proprietà di sistema**.

Tabella 3-78. Opzioni delle proprietà di sistema

Opzione	Descrizione
Proprietà	<p>Le proprietà di sistema disponibili dipendono dal tipo di richiesta o elemento di catalogo selezionato, nonché dall'esistenza di proprietà di sistema per tale elemento.</p> <p>Alcune proprietà sono disponibili solo per specifiche configurazioni del blueprint. Ad esempio, nel caso di CPU, il blueprint a cui si applica il criterio di approvazione con la proprietà di sistema CPU deve essere configurato come un intervallo. Ad esempio, il numero minimo di CPU è 2 e il numero massimo è 8.</p>

Aggiunta di proprietà personalizzate alle impostazioni dei criteri di approvazione

È possibile configurare proprietà personalizzate da aggiungere al modulo di approvazione e permettere così all'approvatore di modificarne i valori.

Ad esempio, nel caso dell'approvazione di una macchina virtuale, aggiungere **VMware.VirtualCenter.Folder** per permettere all'approvatore di specificare la cartella in cui verrà aggiunta la macchina in vCenter Server.

È anche possibile aggiungere una proprietà personalizzata specifica del singolo modulo di criterio di approvazione.

Per selezionare proprietà di sistema, scegliere **Amministrazione > Criteri di approvazione**. Fare clic su **Nuovo**. Selezionare il tipo di criterio e scegliere **OK**. Nella scheda Prima dell'approvazione o nella scheda Dopo l'approvazione, fare clic sull'icona **Nuovo (+)** e scegliere la scheda **Proprietà personalizzate**.

Tabella 3-79. Proprietà personalizzate

Opzione	Descrizione
Nome	Specificare il nome della proprietà.
Etichetta	Immettere l'etichetta che viene presentata all'approvatore nel modulo di approvazione.
Descrizione	<p>Immettere informazioni estese per l'approvatore.</p> <p>Queste verranno visualizzate come una descrizione di comando del campo nel modulo.</p>

Modifica di un criterio di approvazione

Non è possibile modificare un criterio di approvazione attivo o inattivo. È necessario creare una copia del criterio originale e sostituire il criterio che non sta producendo i risultati richiesti. I criteri

di approvazione attivi e inattivi sono di sola lettura. È possibile modificare i criteri di approvazione che sono in uno stato di bozza.


Quando si crea la copia del criterio di approvazione, il nuovo criterio si basa sul tipo di criterio originale. È possibile modificare tutti gli attributi ad eccezione del tipo di criterio. Questa operazione viene eseguita quando si desidera modificare, aggiungere o rimuovere i livelli di approvazione o aggiungere proprietà di sistema o personalizzate ai moduli.

È possibile creare livelli di pre-approvazione e post-approvazione. Per istruzioni sulla creazione di un livello di approvazione, vedere [Creazione di un livello di approvazione](#).

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant** o **amministratore approvazioni**.

Procedura

- 1 Selezionare **Amministrazione > Criteri di approvazione**.
- 2 Selezionare la riga del criterio di approvazione da copiare.
- 3 Fare clic sull'icona **Copia** .
- Verrà creata una copia del criterio di approvazione.
- 4 Selezionare il nuovo criterio di approvazione da modificare.
- 5 Immettere un nome nella casella di testo **Nome**.
- 6 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 7 Selezionare lo stato del criterio dal menu a discesa **Stato**.

Opzione	Descrizione
Bozza	Salva il criterio di approvazione in uno stato modificabile.
Attivo	Salva il criterio di approvazione in uno stato di sola lettura che è possibile utilizzare in un permesso.
Inattivo	Salva il criterio di approvazione in uno stato di sola lettura che non è possibile utilizzare in un permesso finché non si attiva il criterio.

- 8 Modificare i livelli di pre-approvazione e post-approvazione.
- 9 Fare clic su **OK**.

Risultati

È stato creato un nuovo criterio di approvazione basato su un criterio di approvazione esistente.

Operazioni successive

Applicare il nuovo criterio di approvazione in un permesso. Vedere [Autorizzazione degli utenti per servizi, elementi di catalogo e azioni](#).

Disattivazione di un criterio di approvazione

Se si stabilisce che un criterio di approvazione è obsoleto, è possibile disattivarlo in modo che non risulti disponibile durante il provisioning.

Per disattivare un criterio di approvazione, è necessario assegnare un nuovo criterio per ogni permesso al quale tale criterio di approvazione è attualmente applicato.

Successivamente è possibile riattivare un criterio di approvazione disattivato oppure eliminare un criterio disattivato.

Prerequisiti

Accedere a vRealize Automation come **amministratore tenant** o **amministratore approvazioni**.

Procedura

- 1 Selezionare **Amministrazione > Criteri di approvazione**.
- 2 Fare clic sul nome del criterio di approvazione.
- 3 Fare clic su **Visualizza permessi collegati**.
 - a Nel menu a discesa **Sostituisci tutto con**, selezionare il nuovo criterio di approvazione.
Se sono elencati più permessi, il nuovo criterio di approvazione viene applicato a tutti i permessi elencati.
 - b Fare clic su **OK**.
- 4 Dopo aver verificato che nessun permesso è collegato al criterio di approvazione, selezionare **Inattivo** dal menu a discesa Stato.
- 5 Fare clic su **OK**.
- 6 Per eliminare un criterio di approvazione, selezionare la riga contenente il criterio inattivo.
 - a Fare clic su **Elimina**.
 - b Fare clic su **OK**.

Risultati

Il criterio di approvazione viene scollegato da tutti i permessi in cui è utilizzato e viene quindi disattivato. È possibile riattivarlo e riapplicarlo agli elementi di un permesso in un secondo momento.

Operazioni successive

Se il criterio di approvazione non è più necessario, è possibile eliminarlo. Vedere [Eliminazione di un criterio di approvazione](#).

Eliminazione di un criterio di approvazione

Se sono presenti criteri di approvazione disattivati e non più necessari, è possibile eliminarli da vRealize Automation.

Prerequisiti

- Scollegare e disattivare i criteri di approvazione. Vedere [Disattivazione di un criterio di approvazione](#).
- Accedere a vRealize Automation come **amministratore tenant** o **amministratore approvazioni**.

Procedura

- 1 Selezionare **Amministrazione > Criteri di approvazione**.
- 2 Selezionare la riga contenente il criterio inattivo.
- 3 Fare clic su **Elimina**.
- 4 Fare clic su **OK**.

Risultati

Il criterio di approvazione viene eliminato.

Scenario: creazione e applicazione di criteri di approvazione di CentOS con MySQL

Un amministratore tenant, responsabile del gruppo di business dei tecnici di sviluppo e qualità, è interessato a esercitare una stretta governance sulle richieste di elementi di catalogo. Prima che gli utenti possano eseguire il provisioning dell'elemento di catalogo CentOS con MySQL, è consigliabile che l'amministratore dell'infrastruttura virtuale di vSphere approvi la richiesta della macchina e che il responsabile del software approvi la richiesta del software.

Si crea e applica così un criterio di approvazione per la richiesta di catalogo del servizio CentOS con MySQL vSphere per richiedere l'approvazione della macchina da parte di un amministratore di infrastruttura virtuale di vSphere in base a specifiche condizioni, quindi un altro criterio di approvazione per il componente Software MySQL per richiedere l'approvazione da parte del responsabile del software per ogni richiesta.

Gli amministratori approvazioni possono solo creare le approvazioni, ma successivamente i manager dei gruppi di business possono applicarle ai permessi. In qualità di amministratore tenant, creare le approvazioni e applicarle ai permessi.

Prerequisiti

- Accedere alla console vRealize Automation come **amministratore tenant**. Solo un amministratore tenant può sia creare che applicare i criteri di approvazione.
- Verificare che l'elemento del catalogo CentOS con MySQL sia incluso in un servizio. Vedere [Scenario: rendere un blueprint dell'applicazione CentOS con MySQL disponibile nel catalogo dei servizi](#).

Scenario: creazione di un CentOS con criterio di approvazione per la macchina virtuale MySQL

In qualità di amministratore tenant si ha il compito di garantire che il gruppo di ingegneri addetti allo sviluppo e alla qualità riceva macchine virtuali che vengono correttamente sottoposte a provisioning nel proprio ambiente. A tale scopo, si crea un criterio di approvazione che richiede un'approvazione preliminare per alcuni tipi di richieste.


Poiché la macchina virtuale CentOS con MySQL utilizza le risorse di vCenter Server, si desidera che l'amministratore dell'infrastruttura virtuale vSphere approvi le richieste quando la memoria necessaria è superiore a 2048 MB o quando vengono richieste più di 2 CPU, allo scopo di garantire un utilizzo efficiente delle risorse. Inoltre, si offre all'approvatore la possibilità di modificare i valori relativi a CPU e memoria prima di approvare una richiesta.

Procedura

- 1 Selezionare **Amministrazione > Criteri di approvazione**.
- 2 Creare un criterio di approvazione per il provisioning della macchina virtuale.
 - a Fare clic sull'icona **Nuovo** (+).
 - b Scegliere **Seleziona un tipo di criterio di approvazione**.
 - c Nell'elenco selezionare **Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale**.
 - d Fare clic su **OK**.
 - e Configurare le opzioni seguenti:

Opzione	Configurazione
Nome	Immettere CPU o memoria macchina virtuale CentOS on vSphere.
Descrizione	Immettere Richiede approvazione amministratore VI per CPU>2 o Memoria>2048.
Stato	Selezionare Attivo .

- 3 Nella scheda **Prima dell'approvazione** fare clic sull'icona **Aggiungi** (+).
- 4 Configurare la scheda **Informazioni livello** con i criteri di attivazione e le azioni di approvazione.
 - a Nella casella di testo **Nome** immettere CPU>2 o Memoria>2048 – Amministratore VI.
 - b Nella casella di testo **Descrizione** immettere
Approvazione amministratore VI per CPU e memoria.
 - c Selezionare **Necessaria in base alle condizioni**.
 - d Nell'elenco a discesa Clausola selezionare **Qualsiasi tra i seguenti**.
 - e Nel nuovo elenco a discesa Clausola, selezionare **CPU** e configurare la clausola con i valori **CPU, > 2**.

- f Fare clic su **Aggiungi espressione** e configurare la clausola i valori **Memoria (MB) > 2048**.
- g Selezionare **Gruppi e utenti specifici**.
- h Immettere il nome dell'amministratore o del gruppo di amministratori dell'infrastruttura virtuale vSphere nella casella di testo di ricerca e fare clic sull'icona di ricerca ()
- i Selezionare l'utente o il gruppo.
- j Selezionare **Chiunque può approvare**.

Per la verifica delle risorse e l'approvazione della richiesta, è necessario un solo amministratore dell'infrastruttura virtuale.

- 5 Fare clic sulla scheda **Proprietà di sistema** e selezionare le proprietà che consentono all'approvatore di modificare i valori di CPU e Memoria richiesti prima di approvare una richiesta.

- a Selezionare le caselle di controllo **CPU** e **Memoria (MB)**.
- b Fare clic su **OK**.

- 6 Fare clic su **OK**.

Risultati


È stato creato un criterio di approvazione per le richieste relative alla macchina virtuale, ma si desidera ancora creare un'approvazione per il componente MySQL. Nessuna approvazione verrà attivata finché i criteri non verranno applicati a un permesso.

Scenario: creazione di un criterio di approvazione del componente Software MySQL

I responsabili del software possono richiedere agli amministratori tenant di creare e applicare criteri di approvazione per le installazioni di MySQL al fine di tracciare l'uso delle licenze. In virtù di tale richiesta, gli amministratori possono creare un criterio per informare il responsabile delle licenze software ogni volta che viene richiesto il componente Software MySQL per macchine virtuali Linux.

Negli ambienti in il responsabile del software fornisce le chiavi di licenza, questo tipo di approvazione può essere necessaria. In una situazione come questa, occorre solo che il responsabile del software tenga traccia della richiesta e la approvi. Dopo aver creato il criterio di approvazione, si applica il criterio all'elemento di catalogo MySQL per macchine virtuali Linux. Questo criterio di approvazione è molto specifico e può essere applicato solo al componente Software MySQL per macchine virtuali Linux nei permessi.

Procedura

- 1 Selezionare **Amministrazione > Criteri di approvazione**.
- 2 Creare un criterio di approvazione per il componente Software MySQL.
 - a Fare clic sull'icona **Nuovo** ()
 - b Scegliere **Seleziona un elemento**.

- c Selezionare **MySQL per macchine virtuali Linux**.
- d Fare clic su **OK**.
- e Configurare le opzioni seguenti:

Opzione	Configurazione
Nome	Immettere MySQL tracking approval .
Descrizione	Immettere Approval request sent to software manager .
Stato	Selezionare Attivo .

- 3 Nella scheda **Prima dell'approvazione** fare clic sull'icona **Aggiungi** (+).
- 4 Configurare la scheda **Informazioni livello** con i criteri di attivazione e le azioni di approvazione.
 - a Nella casella di testo **Nome**, immettere **MySQL software deployment notice**.
 - b Nella casella di testo **Descrizione**, immettere **Software mgr approval of software installation**.
 - c Selezionare **Sempre necessaria**.
 - d Selezionare **Gruppi e utenti specifici**.
 - e Immettere il nome del responsabile del software nella casella di testo di ricerca, fare clic sull'icona di ricerca (🔍) e selezionare l'utente.
 - f Selezionare **Chiunque può approvare**.

La richiesta necessita di approvazione da parte di un solo responsabile del software.

Fare clic su **OK**.

- 5 Fare clic su **OK**.

Risultati

In questo modo sono stati creati i criteri di approvazione per le macchine virtuali e per i componenti Software delle macchine virtuali MySQL per Linux. Nessuna approvazione verrà attivata finché i criteri di approvazione non verranno applicati a un permesso.

Scenario: applicazione di criteri di approvazione a componenti CentOS con MySQL

L'amministratore tenant può creare criteri di approvazione e permessi. Modificare il permesso Dev e QE per applicare i criteri di approvazione creati, in modo da attivare le approvazioni alla richiesta dell'elemento da parte di un utente del catalogo dei servizi.

Mentre potrebbe essere più semplice autorizzare il proprio gruppo di business all'intero servizio di catalogo, ciò non consentirebbe di avere lo stesso controllo e lo stesso livello di governance di permessi individuali creati per gli elementi di catalogo. Ad esempio, se si autorizzano utenti a un servizio, questi possono richiedere qualsiasi elemento di catalogo contenuto nel servizio e tutti gli elementi che verrebbero aggiunti al servizio in futuro. Questo significa anche che è possibile

utilizzare solo criteri di approvazione di livello molto alto che si applicano a ogni elemento di catalogo nel servizio, ad esempio richiedendo sempre l'approvazione di un manager. Se si sceglie di autorizzare elementi di catalogo singolarmente, è possibile creare e applicare criteri di approvazione molto specifici per ogni elemento e controllare strettamente chi può richiedere quali elementi nel servizio. Se si sceglie di autorizzare per singoli componenti di elementi di catalogo, è possibile avere un controllo anche maggiore.

Se non si conoscono i criteri di approvazione da applicare agli elementi in un permesso, è possibile tornare in un secondo momento e applicarli. In questo scenario, applicare criteri di approvazione differenti a due componenti dello stesso blueprint di applicazione pubblicato.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.
- 2 Fare clic su **Permesso Dev e QE**.
- 3 Fare clic sulla scheda **Elementi e approvazioni**.
- 4 Aggiungere la macchina CentOS con MySQL e applicare il criterio di approvazione.
 - a Fare clic sull'icona **Aggiungi elementi** (+) accanto all'intestazione Elementi autorizzati.
 - b Selezionare la casella di controllo **CentOS con MySQL**.
 - c Fare clic sulla freccia giù **Applicare questo criterio agli elementi selezionati**.
Il criterio CPU e memoria di CentOS su vSphere non è nell'elenco.
 - d Fare clic su **Visualizza tutto** e poi sulla freccia giù per visualizzare tutti i criteri di approvazione.
 - e Selezionare **CPU e memoria di CentOS su vSphere [Catalogo dei servizi - Richiesta di elemento del catalogo - Macchina virtuale]**.
La macchina CentOS di vSphere è un blueprint di macchina in un blueprint di applicazione. Riesaminare i nomi dei criteri così da favorire la selezione del criterio appropriato per il tipo di elemento di catalogo. Se si applica il criterio errato, il criterio di approvazione avrà esito negativo o attiverà richieste di approvazione basate su condizioni errate.
 - f Fare clic su **OK**.
- 5 Aggiungere il componente software MySQL per macchina virtuale Linux come elemento e applicare un criterio di approvazione all'elemento MySQL.
 - a Fare clic sull'icona per **aggiungere elementi e componenti di catalogo** (+) accanto all'intestazione relativa agli elementi e componenti di catalogo permessi.
 - b Nel menu a discesa degli **elementi e componenti di catalogo**, selezionare **No**.
I componenti software sono sempre associati a una macchina e non sono disponibili per essere richiesti individualmente nel catalogo dei servizi.
 - c Selezionare la casella di controllo **MySQL per macchine virtuali Linux**.

- d Fare clic sulla freccia giù **Applicare questo criterio agli elementi selezionati**.
- e Selezionare **MySQL tracking approval [Catalogo dei servizi - Richiesta di elemento del catalogo - Componente software]**.

L'opzione avanzata non è necessaria perché il criterio di approvazione è stato creato per questo specifico componente software, aggiunto a una macchina virtuale.

- f Fare clic su **OK**.

- 6** Aggiungere le azioni che gli utenti potranno eseguire sulla macchina con provisioning eseguito.

I criteri di approvazione non vengono applicati alle azioni in questo scenario.

- a Fare clic sull'icona **Aggiungi azioni (+)** accanto all'intestazione Azioni autorizzate.
- b Selezionare le seguenti azioni.

Nome / Tipo	Descrizione
Crea snapshot / Macchina virtuale	Crea uno snapshot della macchina virtuale, incluso il software installato. Consente agli sviluppatori di creare snapshot a cui è possibile ritornare durante lo sviluppo.
Elimina / Distribuzione	Elimina l'intero blueprint con provisioning eseguito, non solo la macchina. Utilizzare questa azione per evitare componenti orfani.
Spegni / Macchina	Spegne la macchina virtuale.
Accendi / Macchina	Accende la macchina virtuale.
Ripristina snapshot / Macchina virtuale	Ripristina il sistema a uno snapshot precedentemente creato.

- c Fare clic su **OK**.

- 7** Fare clic su **Fine**.

Risultati

Questo permesso consente di richiedere diverse approvazioni su componenti blueprint differenti.

Operazioni successive

Richiedere l'elemento CentOS con MySQL nel catalogo dei servizi in qualità di membro del gruppo di business per verificare che il permesso e le approvazioni si stiano comportando come previsto.

Richiesta di provisioning di una macchina mediante un blueprint con parametri

Quando si richiede il provisioning di una macchina per un blueprint di una macchina vSphere che è stato progettato per includere i profili dei componenti dimensione o immagine, è possibile specificare l'impostazione di provisioning selezionando un set di valori disponibile.

Quando si richiede il provisioning, è possibile scegliere tra le opzioni Size e Image disponibili. Quando si sceglie uno dei set di valori, i valori delle proprietà corrispondenti vengono associati alla richiesta.

Il set di valori del profilo componente viene applicato a tutte le macchine vSphere di un cluster.

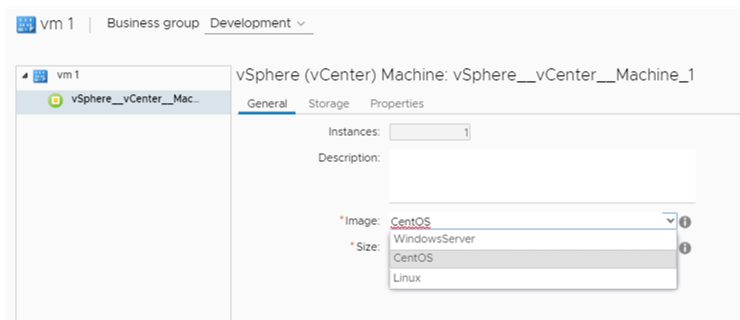
Per informazioni sulla configurazione dei profili di componente, vedere [Aspetti da conoscere e utilizzo della parametrizzazione dei blueprint](#).

Prerequisiti

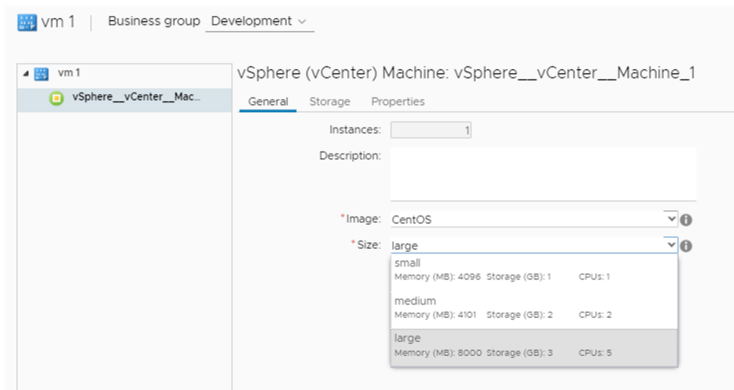
- Definire i set di valori per i profili di componente Size o Image. Vedere *e in Guida di riferimento alle proprietà personalizzate*.
- Creare un blueprint contenente un componente macchina vSphere che include un profilo di componente Image o Size . Vedere [Configurazione del blueprint di una macchina](#) e [vSphereImpostazioni dei componenti macchina in vRealize Automation](#).
- Pubblicare il blueprint nel catalogo. Vedere [Pubblicazione di un blueprint](#).
- Configurare il blueprint nel catalogo. Vedere [Elenco di controllo per la configurazione del catalogo dei servizi](#) e [Esempi di criteri di approvazione basati sul tipo di criterio macchina virtuale](#).

Procedura

- 1 Fare clic su **Catalogo**.
- 2 Selezionare il servizio di catalogo da richiedere e fare clic su **Richiedi**.
- 3 Selezionare il componente macchina vSphere di cui eseguire il provisioning e specificare il numero di istanze di cui eseguire il provisioning.
- 4 Selezionare un'opzione del set di valori immagine nel menu a discesa **Immagine**.



5 Selezionare un'opzione del set di valori dimensione nel menu a discesa **Dimensione**.



6 Fare clic su **Invia**.

Operazioni successive

I set di valori definiti per i profili di componente **Size** e **Image** sono ora disponibili nei menu a discesa **Immagine** e **Dimensione** nel modulo di richiesta di provisioning del catalogo della scheda **Catalogo**.

Scenario: rendere un blueprint dell'applicazione CentOS con MySQL disponibile nel catalogo dei servizi

In qualità di amministratore tenant, si chiede agli architetti dei blueprint di creare un elemento del catalogo per MySQL su CentOS in cui il gruppo di ingegneri addetti alla distribuzione e alla qualità possa eseguire i test case. L'architetto del software ha comunicato che l'elemento del catalogo è pronto per gli utenti. Per rendere l'elemento disponibile per gli utenti aziendali, è necessario associare i blueprint e il componente Software a un servizio di catalogo e quindi autorizzare i membri del gruppo aziendale a richiedere l'elemento del catalogo.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.
- Pubblicare un blueprint per MySQL in una macchina virtuale CentOS di vSphere. Vedere i processi per la creazione di blueprint di componenti macchina e software in [Creazione di una libreria di progettazione](#).
- Se si creano blueprint in un ambiente di sviluppo, importare il blueprint nell'ambiente di produzione. Vedere [Esportazione e importazione di blueprint e contenuti](#).

- Creare una prenotazione per allocare le risorse vSphere al proprio gruppo aziendale addetto allo sviluppo e alla progettazione di qualità. Vedere [Creazione di una prenotazione per Hyper-V, KVM, SCVMM, vSphere o XenServer](#).

Procedura

1 Scenario: creazione di un servizio di catalogo per i tecnici di sviluppo e qualità

Gli amministratori tenant possono creare un servizio di catalogo separato per il gruppo dei tecnici di sviluppo e qualità in modo che gli altri gruppi, come quelli di finanze e risorse umane, non possano accedere agli elementi di catalogo specializzati. È possibile creare un servizio di catalogo chiamato Dev and QE Service per pubblicare tutti gli elementi del catalogo su cui i tecnici di sviluppo e qualità dovranno eseguire i propri test.

2 Scenario: aggiunta di CentOS con MySQL al proprio servizio di sviluppo e progettazione di qualità

In qualità di amministratore tenant, si desidera aggiungere l'elemento di catalogo CentOS con MySQL al servizio di sviluppo e progettazione di qualità.

3 Scenario: autorizzazione degli utenti a richiedere elementi Dev and QE Service come elementi di catalogo

Gli amministratori tenant possono creare un permesso Dev and QE e aggiungere gli elementi di catalogo e alcune azioni rilevanti in modo che gli utenti del gruppo di tecnici di sviluppo e qualità possano richiedere l'elemento di catalogo CentOS con MySQL, nonché eseguire azioni rispetto alla macchina e alla distribuzione.

Scenario: creazione di un servizio di catalogo per i tecnici di sviluppo e qualità

Gli amministratori tenant possono creare un servizio di catalogo separato per il gruppo dei tecnici di sviluppo e qualità in modo che gli altri gruppi, come quelli di finanze e risorse umane, non possano accedere agli elementi di catalogo specializzati. È possibile creare un servizio di catalogo chiamato Dev and QE Service per pubblicare tutti gli elementi del catalogo su cui i tecnici di sviluppo e qualità dovranno eseguire i propri test.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere il nome **Dev and QE Service** nella casella di testo **Nome**.
- 4 Immettere la descrizione **Elementi di catalogo applicazioni Sviluppo e Qualità a scopo di test** nella casella di testo **Descrizione**.
- 5 Selezionare **Attivo** dal menu a discesa **Stato**.
- 6 L'amministratore del catalogo che crea il servizio può utilizzare l'opzione di ricerca per aggiungere il proprio nome come Proprietario.

- 7 Aggiungere il gruppo di utenti personalizzato Team di supporto.

Ad esempio, aggiungere un gruppo di utenti personalizzato che includa gli architetti di IaaS e gli architetti software, in modo che sia sempre possibile, anche per gli utenti del catalogo dei servizi, contattare qualcuno in caso di problemi nel provisioning degli elementi del catalogo.

- 8 Fare clic su **OK**.

Risultati

È stato creato e attivato un servizio di catalogo Dev and QE, che non contiene ancora elementi di catalogo.

Scenario: aggiunta di CentOS con MySQL al proprio servizio di sviluppo e progettazione di qualità

In qualità di amministratore tenant, si desidera aggiungere l'elemento di catalogo CentOS con MySQL al servizio di sviluppo e progettazione di qualità.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.
- 2 Selezionare la riga relativa al servizio di sviluppo e progettazione di qualità nell'elenco **Servizi** e fare clic su **Gestisci elementi del catalogo**.
- 3 Fare clic sull'icona **Nuovo** (+).
- 4 Selezionare **CentOS con MySQL**.

L'elenco include solo i componenti e i blueprint pubblicati non ancora associati a un servizio. Se il blueprint non è presente, verificare che sia stato pubblicato o che non sia incluso in un altro servizio.
- 5 Fare clic su **OK**.
- 6 Fare clic su **Chiudi**.

Risultati

È stato pubblicato l'elemento di catalogo CentOS con MySQL nel servizio di sviluppo e progettazione di qualità, ma finché non si autorizzano gli utenti per l'elemento o il servizio, nessuno potrà visualizzare o richiedere l'elemento.

Scenario: autorizzazione degli utenti a richiedere elementi Dev and QE Service come elementi di catalogo

Gli amministratori tenant possono creare un permesso Dev and QE e aggiungere gli elementi di catalogo e alcune azioni rilevanti in modo che gli utenti del gruppo di tecnici di sviluppo e qualità possano richiedere l'elemento di catalogo CentOS con MySQL, nonché eseguire azioni rispetto alla macchina e alla distribuzione.

In questo scenario, autorizzare il servizio in modo da autorizzare gli utenti a eventuali elementi di catalogo futuri aggiunti a questo servizio. Si desidera anche consentire agli utenti di gestire la loro distribuzione con provisioning eseguito, pertanto si aggiungono azioni quali accensione e spegnimento, snapshot ed eliminazione della distribuzione nel permesso.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Configurare i dettagli.
 - a Immettere il nome **Dev and QE Entitlement** nella casella di testo **Nome**.
 - b Nel menu a discesa **Stato**, selezionare **Attivo**.
 - c Nel menu a discesa **Gruppo di business**, selezionare il gruppo **Dev e QE**.
 - d Nell'area di utenti e gruppi, aggiungere uno o più utenti.

Aggiungere solo se stessi, a meno che non si sia certi che il blueprint sta funzionando come previsto. In questo caso, è possibile aggiungere singoli utenti e gruppi di utenti personalizzati.

- e Fare clic su **Avanti**.
- 4 Aggiungere il servizio.

Sebbene si stiano aggiungendo gli elementi del catalogo CentOS e MySQL separatamente, l'aggiunta del servizio garantisce che qualsiasi ulteriore elemento che verrà aggiunto al servizio in una data successiva, sarà disponibile per i membri del gruppo di business nel catalogo dei servizi.

- a Fare clic sull'icona **Aggiungi servizi** (+) accanto all'intestazione Servizi autorizzati.
- b Selezionare **Dev and QE Service**.
- c Fare clic su **OK**.

Il servizio Dev and QE viene aggiunto all'elenco Servizi autorizzati.

5 Aggiungere le azioni.

- a Fare clic sull'icona **Aggiungi azioni** (+) accanto all'intestazione Azioni autorizzate.
- b Fare clic sull'intestazione di colonna Tipo per ordinare l'elenco.

Selezionare le seguenti azioni in base al tipo. Queste azioni sono utili agli utenti del gruppo di tecnici di sviluppo e qualità che lavorano con le proprie macchine di test e sono le uniche azioni che si desidera rendere disponibili per l'uso a questi membri del gruppo di business.

Tipo	Nome azione
Macchina	Accendi
Macchina	Spegni
Macchina virtuale	Crea snapshot
Macchina virtuale	Ripristina snapshot
Distribuzione	Elimina L'azione di eliminazione della distribuzione elimina l'intera distribuzione e non solo la macchina virtuale.

- c Fare clic su **OK**.

Le cinque azioni vengono aggiunte all'elenco Azioni autorizzate.

6 Fare clic su **Fine**.

Risultati

È stato aggiunto l'elemento di catalogo CentOS con MySQL al nuovo servizio di catalogo Dev and QE e sono stati autorizzati i membri del gruppo di business per richiedere e gestire l'elemento.

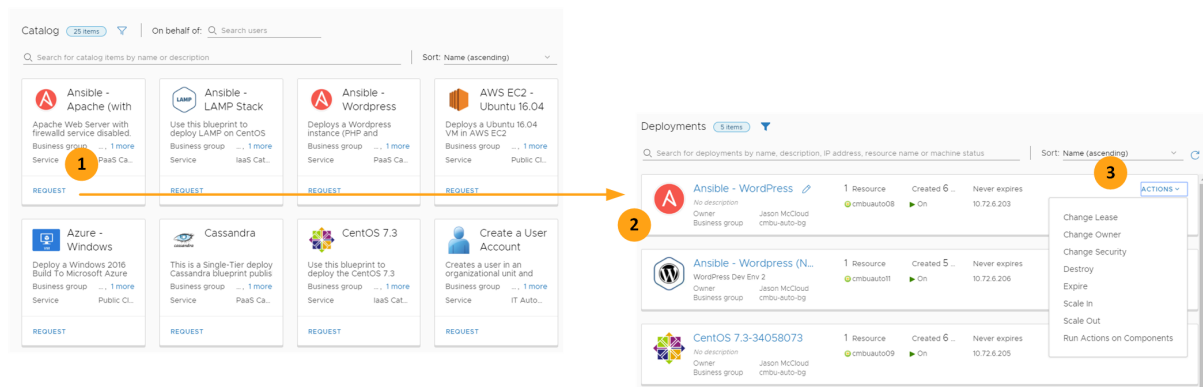
Operazioni successive

Dopo aver verificato il lavoro con il provisioning dell'elemento di catalogo CentOS con MySQL, è possibile aggiungere altri utenti al permesso per rendere l'elemento di catalogo pubblicamente disponibile agli utenti del gruppo di tecnici di sviluppo e qualità. Se si desidera ottenere un livello di governance maggiore sul provisioning di risorse nell'ambiente, è possibile creare criteri di approvazione per il componente Software MySQL e la macchina CentOS per test software. Vedere [Scenario: creazione e applicazione di criteri di approvazione di CentOS con MySQL](#).

Uso del catalogo e gestione delle distribuzioni

4

Il catalogo è formato dai blueprint disponibili e le distribuzioni sono i blueprint sottoposti a provisioning. L'amministratore fornisce gli elementi del catalogo. È quindi possibile richiedere e gestire le risorse come distribuzioni. Come parte della gestione delle distribuzioni, è possibile eseguire azioni per effettuare modifiche.



Il seguente workflow inizia con il catalogo.

- 1 L'utente richiede gli elementi del catalogo. Il catalogo contiene i blueprint pubblicati associati ai gruppi di business di cui l'utente è membro.
- 2 Le risorse sottoposte a provisioning sono gestite come distribuzioni. È possibile monitorare il processo di provisioning, gestire le proprie distribuzioni ed eseguire azioni sulle distribuzioni.
- 3 Le azioni servono per apportare modifiche alla distribuzione dopo la distribuzione. Le azioni possono includere un aumento della memoria, una riduzione della CPU o l'eliminazione della distribuzione quando non è più necessaria.

Questo capitolo include i seguenti argomenti:

- [Utilizzo del catalogo](#)
- [Utilizzo delle distribuzioni](#)
- [Utilizzo della posta in arrivo](#)

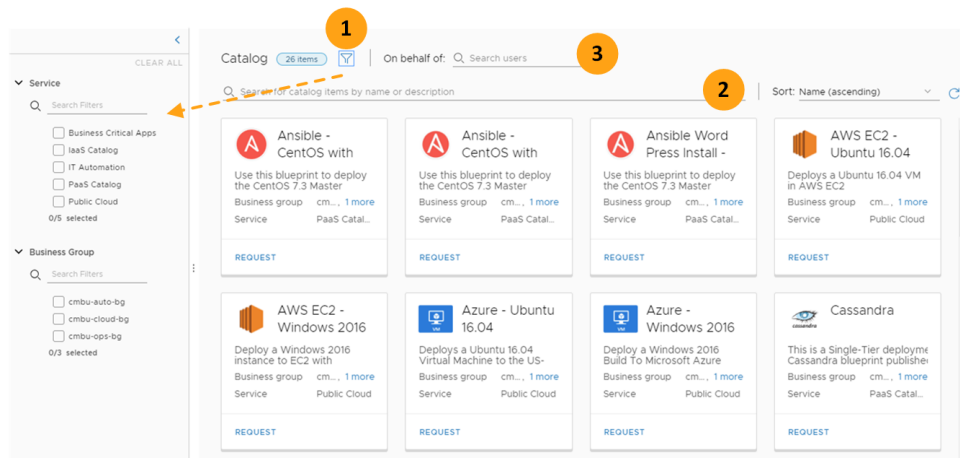
Utilizzo del catalogo

Il catalogo rappresenta l'elenco di blueprint che è possibile distribuire. L'architetto di blueprint si occupa della progettazione dei componenti, stabilisce le opzioni personalizzate che è possibile selezionare quando si richiede l'elemento e dove viene distribuito in base agli endpoint vRealize Automation delle organizzazioni.

Gli elementi del catalogo disponibili si basano sull'iscrizione a uno o più gruppi di business e sul tipo di autorizzazione per eseguire il provisioning dei blueprint di cui tali gruppi dispongono.

Ricerca di elementi del catalogo

Questo esempio riporta un catalogo di piccole dimensioni. Negli ambienti aziendali più grandi gli elementi potrebbero non rientrare in un'unica pagina.

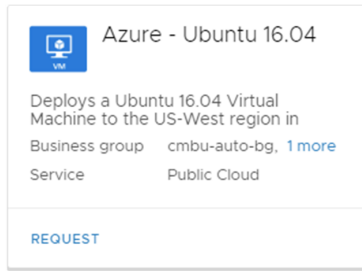


Utilizzare le seguenti opzioni per trovare il blueprint che si desidera distribuire.

- 1 Applicare un **Filtro** all'elenco in base ai servizi e ai gruppi di business.
- 2 Fare clic su **Cerca** e **Ordina** per individuare e organizzare gli elementi del catalogo.
- 3 Selezionare un utente **Per conto di** per limitare il numero di elementi del catalogo prima di richiedere l'elemento per quell'utente. È possibile distribuire i blueprint dotati dell'autorizzazione per i gruppi di business di cui l'utente è membro. Quando si seleziona il nome utente, nell'elenco degli elementi del catalogo disponibili è indicata l'iscrizione al gruppo. L'autorizzazione Per conto di è disponibile per gli amministratori, i manager dei gruppi di business e può venire assegnata a uno o più membri del gruppo di business quando si configura il gruppo di business. Vedere [Creazione di un gruppo di business](#).

Schede del catalogo

Le schede del catalogo rappresentano il blueprint che può distribuire macchine singole o un'intera applicazione. Rappresentano anche i flussi di lavoro di XaaS che eseguono il provisioning in altri modi. Ad esempio, l'aggiunta di utenti ad Active Directory.



Le informazioni sulla scheda includono i gruppi di business che sono autorizzati a richiedere l'elemento del catalogo e il servizio a cui l'elemento è associato.

Come inviare una richiesta di catalogo

I moduli di richiesta del catalogo dei singoli Blueprint potrebbero presentare delle differenze. Le differenze nei moduli vengono configurate dal designer del Blueprint.

Le differenze dei moduli dipendono da quanto è consentito personalizzare la propria richiesta. Potrebbero essere presenti più opzioni da selezionare per personalizzare la richiesta, ma anche nessuna.

Ad esempio, l'architetto potrebbe progettare il blueprint in modo che sia possibile selezionare un numero preciso di CPU o specificare una dimensione piccola, media o grande, ognuna delle quali prevede un numero predefinito di CPU. Oppure un blueprint potrebbe essere restrittivo e non consentire alcuna modifica prima dell'invio.

Dopo il provisioning della richiesta, il servizio o il carico di lavoro distribuito deve essere gestito dall'utente.

Prerequisiti

- È necessario essere membro del gruppo di business dotato del permesso per uno o più elementi del catalogo. Vedere [Creazione di permessi](#).
- Se si esegue la distribuzione per conto di un altro utente, è necessario ricevere in assegnazione il ruolo di supporto del gruppo di business. Vedere [Creazione di un gruppo di business](#).

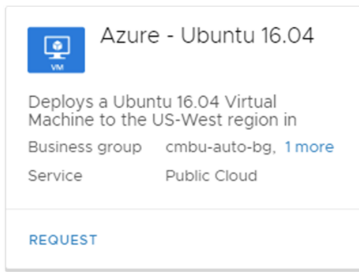
Procedura

- 1 Fare clic su **Catalogo**.
- 2 Se è stata ricevuta l'assegnazione del ruolo di supporto in uno o più gruppi di business e si distribuisce per conto di altri membri del gruppo, immettere il nome dell'utente o del gruppo personalizzato nell'area di ricerca **Per conto di**.

L'elenco degli elementi del catalogo è limitato agli elementi dotati del permesso per i gruppi di business di cui l'utente o il gruppo selezionato è membro.

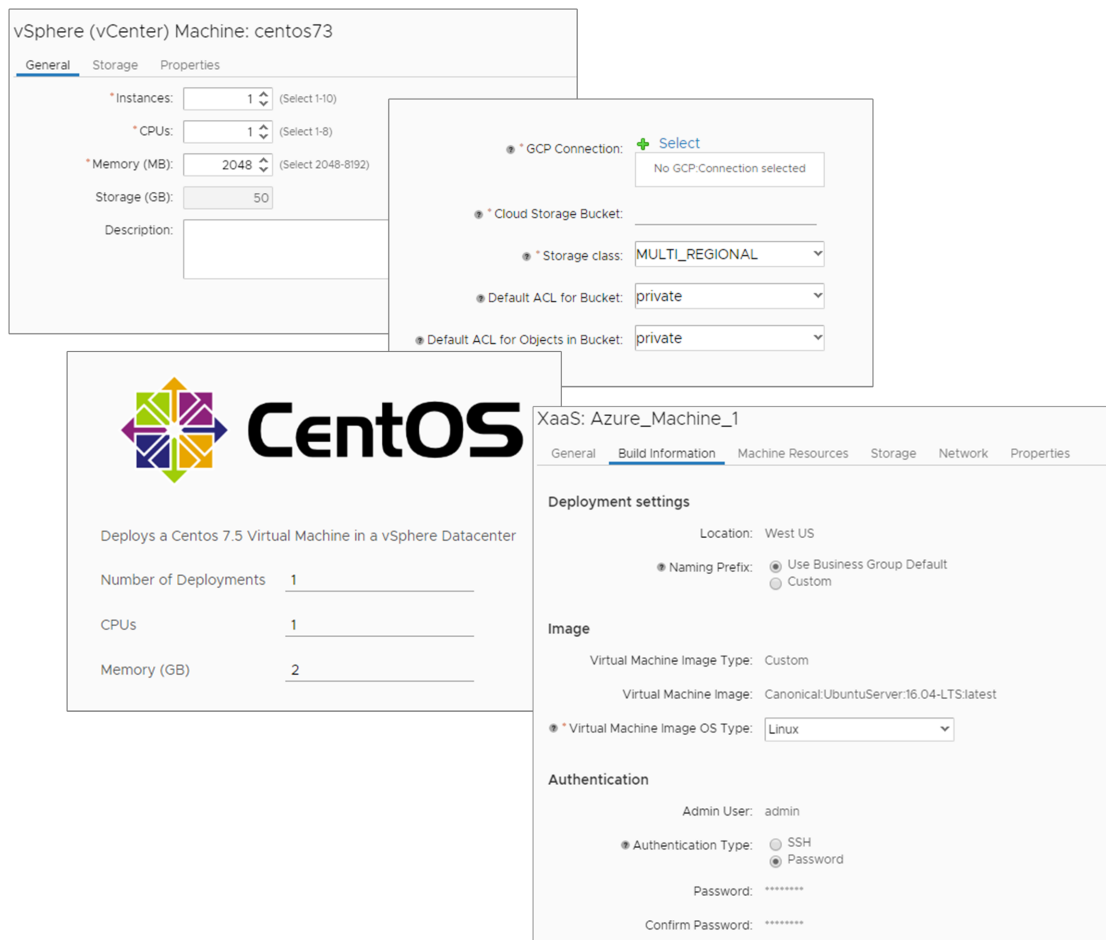
Se non si seleziona un utente, la richiesta viene inviata automaticamente.

- 3 Utilizzare le opzioni di ricerca e ordinamento per individuare l'elemento che si desidera distribuire e fare clic su **Richiesta**.



- 4 Se si è un membro di più di un gruppo di business autorizzato per il Blueprint, selezionare il gruppo di business da associare alla distribuzione.
- 5 Nel modulo di richiesta configurare le opzioni obbligatorie e disponibili.

I moduli possono presentare delle differenze che dipendono dalla configurazione del Blueprint. Di seguito sono riportati esempi che vanno dai più semplici ai più complessi, con più schede.



- 6 Fare clic su **Invia**.

Risultati

La richiesta è stata inviata per il provisioning e verrà visualizzata la scheda Distribuzioni, in modo che si possa tenere traccia dell'avanzamento della richiesta.

Operazioni successive

Verificare che la richiesta venga distribuita. Vedere [Monitoraggio delle richieste di provisioning](#).

Utilizzo delle distribuzioni


Le distribuzioni sono blueprint con provisioning che vengono richiesti dal catalogo. È possibile monitorare lo stato delle richieste inviate attraverso il processo di provisioning, monitorare le risorse distribuite e gestire tali risorse distribuite mediante le azioni.

Monitoraggio dello stato delle richieste

Le richieste in corso vengono visualizzate nella scheda Distribuzioni. La scheda consente di monitorare il processo di provisioning fino al completamento.

Se il processo di provisioning non riesce, è possibile esaminare gli eventi e il messaggio di errore per determinare dove la richiesta non è riuscita e risolvere il problema. Vedere [Richieste di provisioning non riuscite per test e risoluzione dei problemi](#).

The screenshot shows the 'Deployments' section of the vRealize Automation interface. At the top, it says 'Deployments' with a '1 item' badge and a filter icon. Below is a search bar with the placeholder text 'Search for deployments by name, description, IP address, resource name or machine status'. To the right of the search bar is a 'Sort' dropdown menu set to 'Created Date (descending)' with a refresh icon. The main content area displays a single deployment item:

 Ansible Word Press Install - PHP, MyS... <small>No description</small> <small>Owner: Jason McCloud</small> <small>Business group: cmbu-auto-bg</small>	#287 - Provision Ansible Word Press Install - PHP, MySQL all in one - In Progress	14%	CANCEL 3 minutes since submitted
--	--	-----	---

Gestione delle risorse distribuite

È possibile gestire le richieste nella scheda Distribuzioni.

La gestione comprende la verifica che la distribuzione sia attivata. Potrebbe inoltre essere necessario modificare la distribuzione in base alle proprie esigenze di scalabilità verticale o orizzontale. Oppure potrebbe essere necessario esaminare i dettagli della distribuzione. Per ulteriori informazioni, vedere [Gestione degli elementi di catalogo distribuiti](#).

Monitoraggio delle richieste di provisioning

Le distribuzioni vengono utilizzate per monitorare l'avanzamento di una richiesta effettuata nel catalogo. Se il provisioning di una risorsa viene eseguito correttamente, è anche possibile gestire la risorsa distribuita.

Se non viene visualizzata una richiesta in corso, significa che non è stata inviata o che è stata completata.

Monitorare le richieste

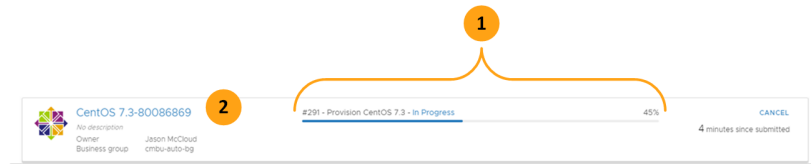
Per monitorare le richieste del catalogo, selezionare **Distribuzioni**.

Tenere traccia dello stato della richiesta nell'elenco delle distribuzioni.

- 1 Tenere traccia dello stato della richiesta nella scheda della distribuzione (1). Se è la prima volta che viene richiesto l'elemento del catalogo, la barra di stato mostra l'avanzamento senza la percentuale. Dopo la prima distribuzione, nelle richieste successive viene visualizzata la percentuale di completamento calcolata.

Se si esegue un'azione su una risorsa distribuita, la barra di stato indica lo stato della modifica selezionata.

- 2 Per visualizzare i dettagli in corso, fare clic sulla barra di stato della distribuzione (1) o sul nome della distribuzione (2).



Esaminare i dettagli del provisioning durante il processo di distribuzione.

- 1 La scheda Cronologia (3) include gli eventi di distribuzione e i valori di input.
- 2 La scheda Eventi (4) include i dettagli della richiesta di provisioning.
- 3 È possibile esaminare il workflow del provisioning (5) per identificare quali componenti vengono attualmente distribuiti.

Se una richiesta non completa il processo di provisioning, vedere [Richieste di provisioning non riuscite per test e risoluzione dei problemi](#).

Tasks	Component	Status	Depends On	Start Time	Completion Time
Submitted	Deployment	Successful		09/06/2018 1:50:06 PM	09/06/2018 1:50
Pre-approval	Deployment	Approved		09/06/2018 1:50:06 PM	09/06/2018 1:50
Provisioning	Deployment	In Progress		09/06/2018 1:50:08 PM	
Provision	centos73: vSphere (vCenter) Machine	Submitted	centos73		
Allocate	centos73: vSphere (vCenter) Machine	Submitted			
Post-approval	Deployment				
Completed	Deployment				

Annullare richieste in corso

Se si invia una richiesta poi si decide di annullarla, il processo di provisioning viene arrestato e per le eventuali risorse distribuite viene effettuato il rollback e la pulizia.

Se il processo di annullamento impiega troppo tempo, è possibile chiedere all'amministratore di forzare l'annullamento. In qualità di amministratore, è possibile annullare una richiesta che si trova nello stato di annullamento. Se si forza l'annullamento, è possibile che il rollback non venga completato e che sia necessario cancellare manualmente le risorse nel sistema di destinazione.

Risoluzione dei problemi per le richieste di catalogo non riuscite

È possibile che la richiesta di un elemento del catalogo non riesca per diversi motivi. Ciò può avvenire a causa del traffico di rete, risorse insufficienti dell'endpoint o una specifica di blueprint difettosa. Oppure, è possibile che la richiesta di provisioning sia stata completata, ma la distribuzione non sembra funzionare. È possibile utilizzare vRealize Automation per esaminare la distribuzione e i messaggi di errore, oltre che determinare se è possibile risolvere il problema presente nell'ambiente.

Se si dispone del ruolo in vRealize Automation come cliente di catalogo e non si dispone di privilegi di amministratore, è possibile utilizzare questo workflow per la risoluzione dei problemi iniziale. Potrebbe essere necessario disporre di qualcuno nell'organizzazione per eseguire ricerche più specifiche.

Possibili stati di errore

Se una richiesta di provisioning non riesce, viene visualizzato uno degli stati seguenti.

- **Non riuscito** Una richiesta può non riuscire per diversi motivi. Un motivo può essere che il processo di provisioning non ha funzionato a causa della mancanza di risorse nell'endpoint di destinazione, risorse insufficienti per supportare il blueprint o un blueprint progettato in modo errato che deve essere corretto. Un altro motivo è che la richiesta necessita l'approvazione di un utente dell'organizzazione, ma l'approvatore rifiuta la richiesta. È inoltre possibile che un'azione eseguita in una distribuzione non sia riuscita. L'errore può essere causato dai motivi relativi all'ambiente o all'approvazione già indicati.

Utilizzare il workflow per la risoluzione dei problemi seguente per individuare la causa del problema. Se si è in grado di risolvere il problema, esaminare le opzioni delle azioni **Ignora** e **Invia di nuovo**. Vedere [Comandi del menu Azione per le risorse di cui è stato eseguito il provisioning](#).

- **Parzialmente completata.** Una richiesta può essere parzialmente riuscita, il che significa che alcuni componenti sono stati distribuiti, ma non tutti i passaggi del provisioning sono stati completati correttamente.

Utilizzare il workflow di risoluzione dei problemi seguente per determinare quali componenti sono riusciti solo parzialmente e individuare la causa del problema. Se si è in grado di risolvere il problema, esaminare le opzioni dell'azione **Ignora** e verificare se è possibile utilizzare **Riprendi**. Vedere [Comandi del menu Azione per le risorse di cui è stato eseguito il provisioning](#) e [Funzionamento dell'azione Riprendi](#).

Risoluzione dei problemi del workflow per i clienti del catalogo

È possibile utilizzare questo workflow per iniziare l'analisi di una distribuzione non riuscita. Se l'analisi rivela che l'errore si è verificato a causa di un problema ambientale temporaneo, è possibile correggere l'errore e inviare di nuovo la richiesta. Se il problema riguarda la specifica della richiesta, potrebbe essere necessario contattare l'architetto del blueprint.

Tabella 4-1. Come iniziare a risolvere i problemi

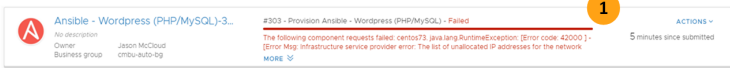
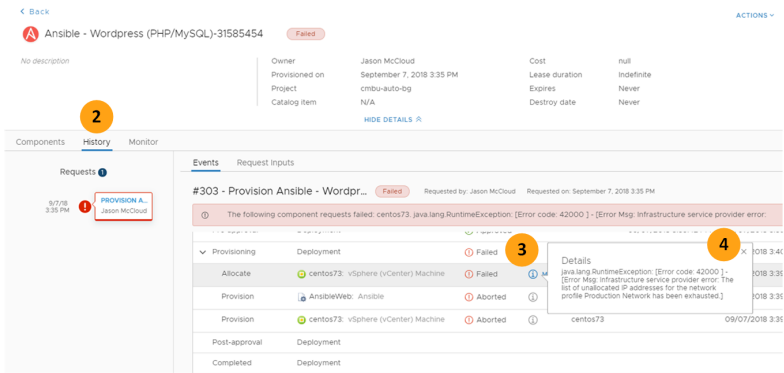
Workflow	Passaggio di risoluzione dei problemi	Esempio
1	Nella scheda Distribuzioni , le distribuzioni non riuscite sono indicate nella barra di stato. La scheda include l'ultimo messaggio di errore. Per ulteriori informazioni, fare clic sul nome della distribuzione o sulla barra di avanzamento.	
2	Nella scheda Cronologia dei dettagli della distribuzione, è possibile utilizzare il workflow degli eventi per verificare dove il processo di provisioning non è riuscito. Questo workflow è inoltre utile quando si esegue un'azione in una distribuzione, ma la modifica non riesce.	

Tabella 4-1. Come iniziare a risolvere i problemi (continua)

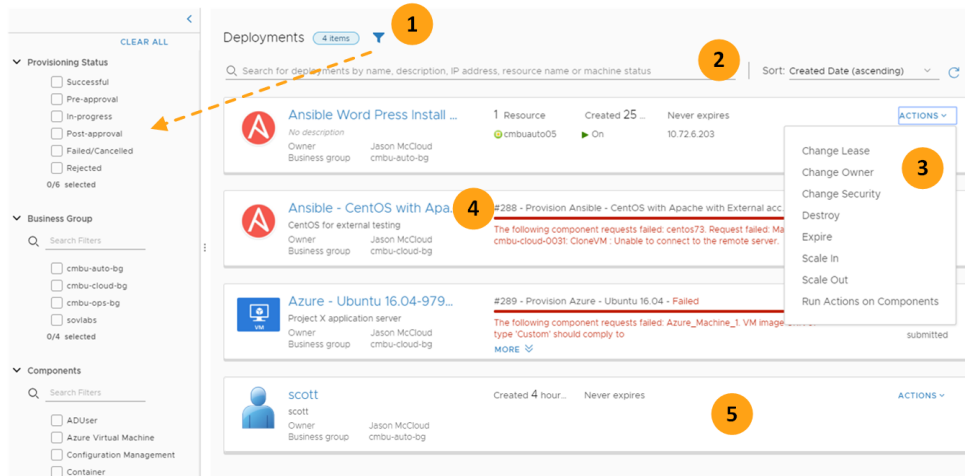
Workflow	Passaggio di risoluzione dei problemi	Esempio
3	Lo stato di errore indica dove il workflow non è riuscito.	
4	<p>Le informazioni forniscono una versione più dettagliata del messaggio di errore.</p> <p>Se queste informazioni non sono sufficienti per identificare e risolvere il problema, è possibile eseguire ricerche aggiuntive nei registri eventi.</p> <p>Per visualizzare i registri degli eventi, è necessario disporre del ruolo utente necessario.</p> <p>L'architetto del blueprint o l'amministratore può eseguire una risoluzione dei problemi aggiuntiva.</p> <p>Vedere Richieste di provisioning non riuscite per test e risoluzione dei problemi.</p>	

Gestione degli elementi di catalogo distribuiti

Il proprietario di una distribuzione o un amministratore che fornisce assistenza ad altri utenti può utilizzare i dettagli della distribuzione per gestire il ciclo di vita degli elementi distribuiti. I dettagli della distribuzione forniscono le informazioni aggiornate su ogni componente e utilizzano la cronologia per tenere traccia delle modifiche nel tempo. Quando si utilizzano le distribuzioni, è possibile usare le azioni per modificare gli elementi distribuiti. Alcune modifiche possono essere apportate anche senza utilizzare le azioni.

Gestione delle distribuzioni dalle schede

L'elenco delle schede delle distribuzioni fornisce una panoramica delle distribuzioni. Sono state eseguite correttamente? Sono in esecuzione?



Utilizzare le seguenti opzioni per trovare e gestire le risorse distribuite da vRealize Automation.

- 1 L'opzione **Filtro** consente di filtrare l'elenco in base allo stato corrente della richiesta, al gruppo di business per cui è stata distribuita, ai componenti secondari inclusi, all'utente proprietario e agli intervalli di date del provisioning o della scadenza. I filtri Stato provisioning e Numero richiesta valgono solo per il processo di provisioning iniziale, non per le azioni successive eventualmente eseguite. Gli altri filtri si applicano alla distribuzione in generale.
- 2 **Cerca e Ordina** consentono di individuare e organizzare le distribuzioni.
- 3 Per gestire la distribuzione, fare clic su **Azioni** per eseguire le azioni autorizzate a livello di distribuzione. Per eseguire azioni sui singoli componenti, è necessario aprire i dettagli della distribuzione. Le azioni possono essere azioni standard autorizzate per i blueprint di progettazione o azioni di risorse di XaaS personalizzate create e autorizzate per il blueprint di XaaS. Per ulteriori informazioni sulle azioni standard, vedere [Esecuzione di azioni su risorse distribuite](#).
- 4 Per visualizzare e gestire i dettagli di una distribuzione, inclusi gli eventi di provisioning, la cronologia e le azioni a livello di componente, fare clic sul nome della distribuzione. I primi tre rappresentano le richieste di provisioning iniziale per i blueprint standard.
- 5 È inoltre possibile gestire le richieste di distribuzione di XaaS che eseguono workflow. I workflow possono trasformarsi in risorse oppure vengono eseguiti in sistemi esterni. In questo esempio XaaS ha aggiunto un utente a un dominio di Active Directory.

Gestione di una distribuzione mediante i dettagli della distribuzione

I dettagli della distribuzione vengono utilizzati per eseguire le seguenti informazioni di gestione.

- **Dettagli.** Le informazioni di base che si trovano nella scheda. È anche possibile modificare il nome e la descrizione della distribuzione ed eseguire azioni a livello di distribuzione.
- **Scheda Componenti.** La configurazione completa di ciascun componente. È inoltre possibile eseguire azioni a livello di componente.

- **Scheda Cronologia.** Cronologia completa delle modifiche apportate alla distribuzione. È anche possibile trovare ulteriori informazioni sulla posizione e sui valori di input forniti per ogni modifica.
- **Scheda Monitora** Se si esegue l'integrazione con vRealize Operations Manager, vengono visualizzati i dati delle metriche di monitoraggio e gli avvisi per la distribuzione e i componenti.
- **Azioni.** Utilizzando i dettagli è possibile eseguire anche azioni a livello di distribuzione o di componente.

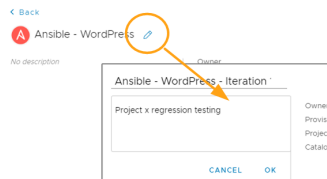
Utilizzo dei dettagli della distribuzione

I dettagli della distribuzione forniscono più informazioni rispetto a quelle di base presenti nella scheda. È anche possibile modificare il nome e la descrizione della distribuzione, nonché eseguire la distribuzione e le azioni a livello di componente.

Esaminare le informazioni di base della distribuzione, incluso il blueprint da cui è stata distribuita e il costo.

Modificare il nome della distribuzione

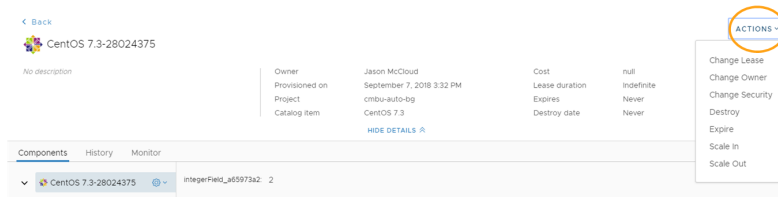
La distribuzione prende il nome del blueprint. Se mentre si utilizza la distribuzione ci si accorge che questo nome non è particolarmente significativo, è possibile aggiornare il nome e la descrizione in base alle proprie esigenze.



- 1 Posizionare il puntatore sul nome e fare clic sull'icona a forma di matita.
- 2 Aggiornare il nome e la descrizione in modo che risultino significativi.

Eseguire azioni a livello di distribuzione

Le azioni a livello di distribuzione sono limitate alle modifiche che influiscono sull'intera distribuzione. Le azioni disponibili dipendono dalle autorizzazioni di utilizzo concesse al gruppo di business.



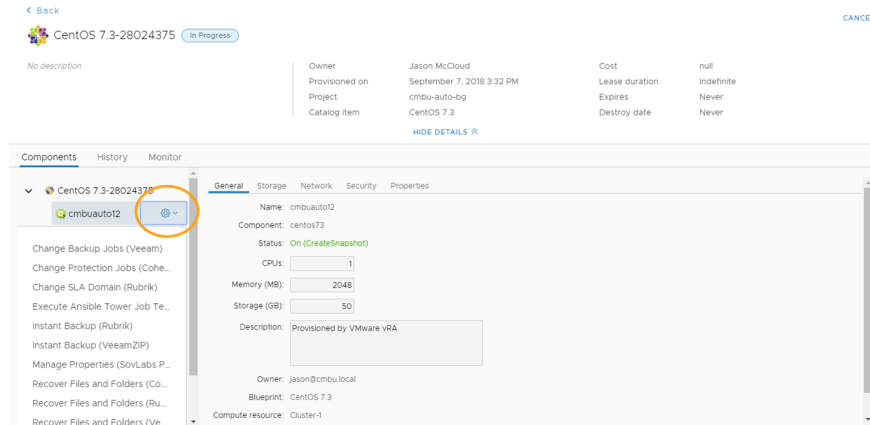
Componenti della distribuzione

Nella scheda Componenti dei dettagli della distribuzione è presente la configurazione completa di tutti i componenti della distribuzione. È possibile visualizzare in che modo le macchine e le reti

sono configurate. È inoltre possibile eseguire azioni a livello di componente per modificare la configurazione.

Esaminare i dettagli del componente quando è necessario comprendere la distribuzione fornita o quando si sta risolvendo un problema relativo all'istanza.

Le modifiche apportate mediante le azioni si riflettono nei dettagli.



Esecuzione di azioni a livello di componente

Le azioni a livello di componente sono specifiche del componente. Le azioni disponibili dipendono dalle autorizzazioni di utilizzo concesse al gruppo di business. Se l'amministratore non ha concesso alcuna autorizzazione per l'esecuzione delle azioni, l'icona a forma di ingranaggio e l'elenco delle azioni non sono visibili.

Cronologia di distribuzione

La scheda Cronologia nei dettagli della distribuzione presenta la cronologia completa della distribuzione, dal provisioning iniziale fino a eventuali modifiche apportate mediante una o più azioni. È possibile utilizzare la cronologia di provisioning completa per scoprire eventuali modifiche apportate e quali valori siano stati forniti.

Esaminare i dettagli della cronologia per determinare eventuali modifiche o durante l'analisi di problemi con l'istanza. È inoltre possibile utilizzare la cronologia per la risoluzione dei problemi di distribuzioni non riuscite. Vedere [Richieste di provisioning non riuscite per test e risoluzione dei problemi](#).

CentOS 7.3-28024375 In Progress

No description

Owner: Jason McCloud
Provisioned on: September 7, 2018 3:32 PM
Project: cmbu-auto-big
Catalog item: CentOS 7.3

Cost: null
Lease duration: Indefinite
Expires: Never
Destroy date: Never

[HIDE DETAILS](#)

Components **History** Monitor

Requests

9/10/18 4:01 PM CREATE SNA... Jason McCloud

9/10/18 3:42 PM REBOOT CMB... Jason McCloud

9/7/18 3:32 PM PROVISION C... Jason McCloud

Events **Request Inputs**

#316 - Create Snapshot cmbuauto... In Progress Requested by: Jason McCloud Requested on: September 10, 2018 4:01 PM

Task	Component	Status	Depends On	Start Time	Completion Time
Submitted	Deployment	Successful		09/10/2018 4:01:09 PM	09/10/2018 4:01:09 PM
Pre-approval	Deployment	Approved		09/10/2018 4:01:09 PM	09/10/2018 4:01:09 PM
Create Snapshot	Deployment	In Progress		09/10/2018 4:01:11 PM	
Post-approval	Deployment				
Completed	Deployment				

Components **History** Monitor

Requests

9/10/18 4:01 PM CREATE SNA... Jason McCloud

9/10/18 3:42 PM REBOOT CMB... Jason McCloud

9/7/18 3:32 PM PROVISION C... Jason McCloud

Events **Request Inputs**

Machine Name: cmbuauto12

Snapshot name: cmbuauto12 (Monday, September 10, 2018 10:01:02 PM +00:00)

Snapshot description:

Include memory?: No

Monitoraggio della distribuzione basato su vRealize Operations Manager

vRealize Automation può mostrare i dati di vRealize Operations Manager sulle distribuzioni.

- Avvisi a livello di distribuzione
- Metriche a livello di macchina

Controllare il set filtrato di avvisi e metriche direttamente in vRealize Automation consente di evitare la necessità di accedere o cercare vRealize Operations Manager. Sebbene non sia possibile avviare il contesto in vRealize Operations Manager, è ovviamente possibile accedere e utilizzare vRealize Operations Manager per gli eventuali dati aggiuntivi.

Abilitazione dei dati di vRealize Operations Manager

Per consentire a vRealize Automation di mostrare i dati di vRealize Operations Manager, è innanzitutto necessario configurare le impostazioni e gli adattatori.

La configurazione richiede passaggi in vRealize Operations Manager e vRealize Automation.

Prerequisiti

Verificare di disporre di vRealize Operations Manager versione 6 o successiva.

Procedura

- 1 In vRealize Operations Manager, accedere ad **Amministrazione > Soluzioni**.
- 2 In **Soluzioni**, verificare di disporre della [soluzione vRealize Automation](#) e che riceva dati.
 - a Selezionare la soluzione vRealize Automation.
 - b Nella barra degli strumenti sopra le soluzioni, fare clic sull'icona Configura (ingranaggio).

- c In **Impostazioni dell'istanza**, andare in **Credenziali** e fare clic sul segno più verde per aggiungere le credenziali.

Nome della credenziale	Descrizione di questo set di credenziali
SysAdmin	Nome utente e password dell'amministratore tenant predefinito di vRealize Automation, in genere administrator@vsphere.local
SuperUser	Nome utente e password di un accesso ad accesso elevato per il tenant di lavoro di vRealize Automation

- d Salvare e verificare le credenziali per una corretta connessione.

- 3 In **Istanze dell'adattatore configurate**, verificare di disporre di una [scheda vCenter](#) per l'endpoint vSphere a cui vRealize Automation esegue il provisioning e che riceva dati.

Figura 4-1. Soluzioni e adattatori di vRealize Operations Manager

Name	Description	Version	Provided by	Licensing	Adapter Status
VMware vRealize Business to Management Pack for VMwar...		6.0.7963016	VMware Inc.	Not applicable	None Configured
VMware vRealize Automator		4.0.9272301	VMware Inc.	Not applicable	Data receiving (1)

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vCenter Adapter	vCenter_BLR_Lab	cred_BLR_Lab	vRealize Operations Manager ...	Collecting	Data receiving

- 4 In vRealize Operations Manager, accedere ad **Avvisi > Impostazioni degli avvisi**.
- 5 Verificare che le definizioni di avvisi e sintomi generino gli avvisi di vRealize Automation desiderati.

La maggior parte degli utenti di vRealize Automation dee solo verificare che una distribuzione rimanga integra. Ulteriori avvisi dal livello della macchina virtuale possono essere molto impegnativi e contenere dettagli che non possono essere gestiti tramite vRealize Automation.

Per gli [avvisi di vRealize Automation](#), la distribuzione globale è l'oggetto principale. Le macchine virtuali all'interno della distribuzione sono gli oggetti figlio. Per impostazione predefinita, gli avvisi si trovano al livello principale della distribuzione.

L'utente è libero di utilizzare vRealize Operations Manager per creare avvisi a livello della distribuzione che espongono sintomi aggiuntivi specifici. Potrebbe ad esempio, voler visualizzare tutti i problemi di SQL Server in una distribuzione.

- 6 In vRealize Automation, accedere ad **Amministrazione > Recupero > Fornitore di metriche**.
- 7 Selezionare **Endpoint di vRealize Operations Manager**.
- 8 Entrare nell'URL vRealize Operations Manager `https://master-nodo-FQDN-o-IP/suite-api/` e il nome utente e la password di un account con diritti di amministratore di vRealize Operations Manager.

Nota Quando sono presenti più origini di autenticazione, immettere il nome utente in formato `user@domain@source`, dove `@source` è l'origine di importazione LDAP in vRealize Operations Manager. L'account utente richiede un ruolo minimo di `ReadOnly` e i diritti degli oggetti per l'adattatore di vCenter e Cloud vCenter Server.

- 9 Provare la connessione e salvarla.
- 10 Fare clic su **Distribuzioni**, selezionare una distribuzione e verificare che venga visualizzata la scheda **Monitora**.

La scheda **Monitora** viene visualizzata solo quando vRealize Operations Manager è selezionato come fornitore di metriche.

Avvisi forniti da vRealize Operations Manager

Quando è abilitato il monitoraggio, vRealize Automation recupera avvisi di vRealize Operations Manager sulle distribuzioni.

Per accedere al monitoraggio, fare clic su una distribuzione e selezionare la scheda **Monitora**. Se la scheda non è presente, vedere [Abilitazione dei dati di vRealize Operations Manager](#).

Per visualizzare gli avvisi, selezionare il nome della distribuzione nella parte superiore della struttura del componente a sinistra.

- È possibile rivedere il livello di gravità e il testo degli avvisi.

- Per concentrarsi sulle aree di interesse, filtrare e ordinare i dati nelle colonne.
- Vengono visualizzati solo gli avvisi di integrità. Altri tipi di avviso come quelli relativi all'efficienza o al rischio non sono supportati.

Components	History	Monitor																		
<div> <div>VC-65-DND Deployme...</div> <div>VC-65-DND</div> </div>																				
<div> <div>Alerts</div> <div>5</div> </div>																				
<div> <div>Total VMs</div> <div>1</div> </div>																				
<div> <div>Total CPUs</div> <div>4</div> </div>																				
<div> <div>Total Memory</div> <div>16384 MB</div> </div>																				
<div> <div>Total Storage</div> <div>270 GB</div> </div>																				
<table> <thead> <tr> <th>Criticality</th><th>Alert</th><th>Created On</th></tr> </thead> <tbody> <tr> <td>Warning</td><td>One or more VM's of Deployment is not having memory ballooning</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Critical</td><td>One or more VM's Disk usage is above 70%</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Immediate</td><td>One or more VM is having CPU in idle state</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Critical</td><td>Most deployment resources have health issues</td><td>7/26/18, 7:47 PM</td></tr> <tr> <td>Critical</td><td>One or more VM of Deployment is running out of Guest file system disk space</td><td>7/26/18, 7:47 PM</td></tr> </tbody> </table>			Criticality	Alert	Created On	Warning	One or more VM's of Deployment is not having memory ballooning	7/26/18, 7:47 PM	Critical	One or more VM's Disk usage is above 70%	7/26/18, 7:47 PM	Immediate	One or more VM is having CPU in idle state	7/26/18, 7:47 PM	Critical	Most deployment resources have health issues	7/26/18, 7:47 PM	Critical	One or more VM of Deployment is running out of Guest file system disk space	7/26/18, 7:47 PM
Criticality	Alert	Created On																		
Warning	One or more VM's of Deployment is not having memory ballooning	7/26/18, 7:47 PM																		
Critical	One or more VM's Disk usage is above 70%	7/26/18, 7:47 PM																		
Immediate	One or more VM is having CPU in idle state	7/26/18, 7:47 PM																		
Critical	Most deployment resources have health issues	7/26/18, 7:47 PM																		
Critical	One or more VM of Deployment is running out of Guest file system disk space	7/26/18, 7:47 PM																		

Metriche fornite da vRealize Operations Manager

Quando è abilitato il monitoraggio, vRealize Automation recupera le metriche di vRealize Operations Manager relative alle distribuzioni.

Per accedere al monitoraggio, fare clic su una distribuzione e selezionare la scheda **Monitora**. Se la scheda non è presente, vedere [Abilitazione dei dati di vRealize Operations Manager](#).

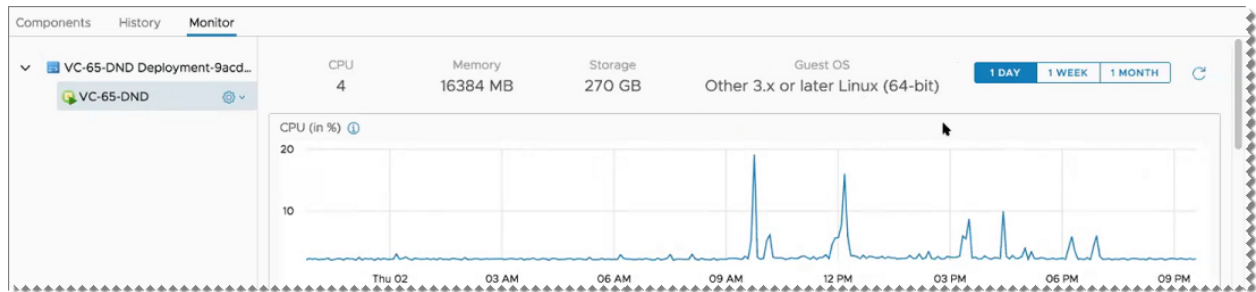
Per visualizzare le metriche, espandere la struttura del componente a sinistra ed evidenziare una macchina virtuale.

- Le metriche non vengono memorizzate nella cache. Provengono direttamente da vRealize Operations Manager e possono richiedere del tempo per caricarsi.
- Vengono visualizzate solo le metriche della macchina virtuale. Le metriche di altri componenti, come vCloud Director, Software o XaaS, non sono supportate.
- Vengono visualizzate solo le metriche della macchina virtuale vSphere. Altri fornitori di cloud, come AWS o Azure, non sono supportati.

Le metriche vengono visualizzate come grafici temporali che mostrano valori massimi e minimi per le seguenti misure.

- CPU
- Memoria
- IOPS storage
- MBPS rete

Per visualizzare il nome della metrica specifica, fare clic sull'icona blu delle informazioni in alto a sinistra nella linea temporale.



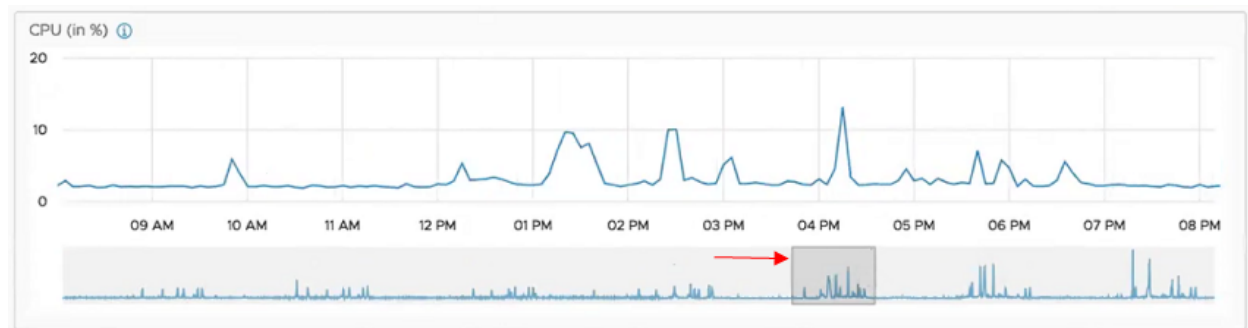
Azioni sui dati forniti da vRealize Operations Manager

Quando le metriche fornite da vRealize Operations Manager espongono un problema, è possibile effettuare alcune azioni correttive direttamente in vRealize Automation.

Per visualizzare le metriche fornite da vRealize Operations Manager, fare clic su una distribuzione e selezionare la scheda **Monitora**. Se la scheda non è presente, vedere [Abilitazione dei dati di vRealize Operations Manager](#).

Localizzazione dei problemi

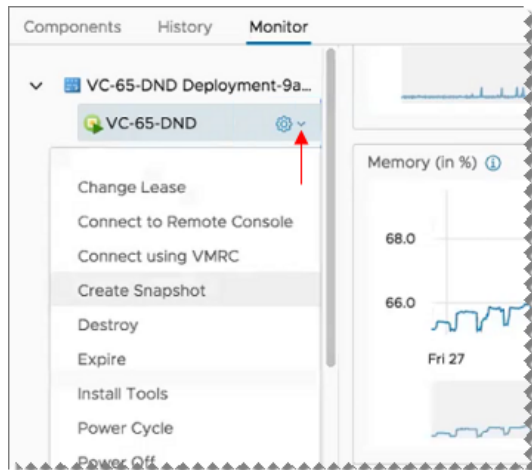
Sono disponibili le metriche nell'ultimo giorno, settimana o mese. Per ingrandire un'area di interesse, selezionare un'area di piccole dimensioni nella parte inferiore ombreggiata nella linea temporale di una metrica qualsiasi:



Applicazione delle modifiche

Quando si verifica un problema, è possibile effettuare alcune azioni correttive direttamente nella stessa interfaccia.

Ad esempio, se la memoria mostra picchi di utilizzo costanti, è possibile decidere di aggiungere memoria. Nella struttura del componente sulla sinistra, fare clic sul menu a discesa della macchina virtuale e utilizzare le opzioni del menu di scelta rapida per eseguire operazioni di manutenzione o riconfigurazione.



Esecuzione di azioni su risorse distribuite

Le azioni disponibili per una risorsa distribuita dipendono dal tipo di risorsa in oggetto, dal modo in cui l'azione è stata configurata e resa disponibile per gli elementi con provisioning e dallo stato operativo dell'elemento.

Le azioni configurate disponibili per una distribuzione o un componente di distribuzione vengono visualizzate nel menu **Azioni** per la distribuzione o il componente selezionati.

L'elenco delle azioni disponibili è determinato da ciò che il proprio gruppo di business è autorizzato a eseguire per la distribuzione e per il componente del tipo di risorsa o di macchina. La disponibilità di un'azione dipende dal tipo o dallo stato della macchina.

Se il provisioning dell'elemento è stato eseguito utilizzando un blueprint XaaS, le azioni per le risorse devono essere create, pubblicate e autorizzate nello stesso servizio utilizzato per il provisioning dell'elemento. L'elenco delle azioni disponibili dipende dal tipo e dallo stato corrente dell'elemento.

Le azioni disponibili per un elemento di cui è stato eseguito il provisioning come macchina IaaS possono inoltre includere azioni per risorse XaaS, qualora le azioni siano state mappate sull'elemento.

Comandi del menu Azione per le risorse di cui è stato eseguito il provisioning

Le azioni sono cambiamenti che si apportano alle risorse di cui viene eseguito il provisioning. Le azioni di vRealize Automation vengono utilizzate per gestire il ciclo di vita delle risorse.

I comandi disponibili nei menu **Azione** dipendono dalla configurazione (da parte del manager del gruppo di business o dell'amministratore tenant) dei permessi contenenti la risorsa su cui vengono eseguite le azioni stesse. La disponibilità di un'opzione del menu dipende anche dal tipo di risorsa e dal suo stato operativo.

È possibile eseguire una sola azione per volta. Per eseguire una seconda azione su una risorsa, attendere che la prima completi la modifica richiesta.

Tabella 4-2. Comandi del menu Azione

Azione	Tipo di risorsa	Descrizione
Associa IP mobile	Macchina (OpenStack)	Associazione di un indirizzo IP mobile a una macchina OpenStack.
Annulla	Macchina	<p>Annullamento di un'azione di riconfigurazione in corso.</p> <p>Gli utenti possono annullare solo le azioni per cui è possibile eseguire il rollback a uno stato precedente.</p> <p>Se un'azione non supporta il rollback a uno stato precedente, ad esempio Spegni, solo un utente con privilegi di amministratore tenant può annullare la richiesta.</p>
Modifica lease	Distribuzione e Macchina	Modifica del numero di giorni restanti nel lease per una macchina specifica o per tutte le risorse incluse in una distribuzione. Se non si fornisce un valore, il lease non ha alcuna scadenza.
Cambia regole NAT	Rete NAT	Aggiungere nuove regole di inoltro della porta NAT, riordinare regole, modificare regole esistenti o eliminare regole.
Cambia proprietario	Distribuzione	<p>Modifica del proprietario di tutta la distribuzione e delle relative risorse. Solo i manager dei gruppi di business e gli utenti di supporto possono cambiare la proprietà di una distribuzione.</p> <p>Quando si avvia l'azione di modifica del proprietario, lo stato della macchina deve essere Attivato, Disattivato o Attivo. In caso contrario, l'azione ha esito negativo e l'errore seguente:</p> <p>L'azione per la macchina non è valida.</p>
Modifica sicurezza	Profilo di	<p>È possibile aggiungere o rimuovere tag e gruppi di sicurezza NSX esistenti. È anche possibile rimuovere i gruppi di sicurezza su richiesta.</p> <p>Per ulteriori informazioni, vedere Aggiunta o rimozione di elementi di sicurezza in una distribuzione.</p>

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Connetti utilizzando VMRC	Macchina	<p>Connessione alla macchina virtuale utilizzando un'applicazione VMRC 8.x.</p> <p>Per utilizzare questa azione, l'applicazione VMRC deve essere installata sul sistema locale dell'utente del catalogo dei servizi che sta eseguendo l'azione.</p> <p>Per istruzioni sull'installazione e per l'utente, vedere Documentazione di VMware Remote Console. Per eseguire il download, vedere Download di VMware Remote Console.</p> <p>VMRC 8.x sostituisce la precedente VMware Remote Console.</p>
Connetti a console remota	Macchina	<p>Connessione alla macchina selezionata mediante VMware Remote Console.</p> <p>La console della macchina virtuale viene visualizzata nel browser. Il VMRC 8.x sostituisce la VMware Remote Console.</p>
Connessione tramite ticket della console	Macchina (OpenStack e KVM)	Connessione alla macchina virtuale OpenStack o KVM tramite ticket della console per una connessione VMware Remote Console.
Connessione con ICA	Macchina (Citrix)	Connessione alla macchina Citrix mediante il protocollo ICA (Independent Computing Architecture).
Connessione con RDP	Macchina	Connessione alla macchina mediante Microsoft Remote Desktop Protocol.
Connessione con SSH	Macchina	<p>Connessione alla macchina selezionata utilizzando SSH.</p> <p>L'opzione Connessione con SSH richiede un browser con un plug-in che supporti SSH, ad esempio il client terminale FireSSH SSH per Mozilla Firefox e Google Chrome. Quando il plug-in è presente, se si seleziona Connessione con SSH viene visualizzata una console SSH e vengono richieste le credenziali di amministratore.</p> <p>Per utilizzare questa azione è necessario includere la proprietà personalizzata Machine.SSH, impostata su True, nel componente macchina del blueprint, all'interno di un gruppo di proprietà o in una proprietà personalizzata singola.</p>
Connessione tramite desktop virtuale	Macchina	Connessione alla macchina selezionata tramite desktop virtuale di Microsoft.

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Crea snapshot	Macchina virtuale	Creazione di uno snapshot della macchina virtuale. Se sono consentiti solo due snapshot e sono già stati utilizzati entrambi, il comando diventa disponibile solo dopo l'eliminazione di uno snapshot.
Elimina snapshot	Macchina virtuale	Eliminazione di uno snapshot della macchina virtuale.

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Elimina	Distribuzione, macchina e gruppo di sicurezza su richiesta	<p>Eliminazione immediata di una risorsa di cui è stato eseguito il provisioning.</p> <p>Eccetto che per XaaS, l'eliminazione di componenti di una distribuzione non rappresenta la pratica migliore. Utilizzare l'azione di scalabilità verticale per ridurre il numero di macchine nella propria distribuzione oppure eliminare la distribuzione completa.</p> <p>È necessario eseguire questa azione per eliminare risorse di XaaS, anche se fanno parte di una distribuzione che si sta eliminando. Altre risorse vengono eliminate alla scadenza del relativo lease o periodo di archiviazione.</p> <p>L'azione Elimina non è disponibile per le seguenti situazioni di distribuzione:</p> <ul style="list-style-type: none"> ■ distribuzioni di macchine fisiche ■ distribuzioni con una rete NSX o una risorsa di sicurezza NSX esistente ■ distribuzioni con una risorsa bilanciamento del carico su richiesta NSX <p>Poiché un bilanciamento del carico NSX appartiene a un edge NSX, quando si elimina un edge NSX viene eliminata anche la risorsa bilanciamento del carico e le risorse vengono rilasciate. Quando si elimina un livello macchina con bilanciamento del carico, tale livello macchina viene rimosso dal pool di bilanciamento del carico sul relativo edge NSX.</p> <hr/> <p>Nota L'azione di eliminazione potrebbe restituire un messaggio di operazione completata anche se non è possibile rimuovere la distribuzione di una macchina dal relativo endpoint. Ad esempio, se una macchina vSphere si trova in un datastore non vSAN e il file VMX contiene dati danneggiati o non validi. Anche se il messaggio di eliminazione indica che l'operazione è riuscita, è possibile esaminare il registro della richiesta per ulteriori informazioni. Forzare l'eliminazione di una macchina in questo stato potrebbe lasciarla in esecuzione sull'endpoint e causare conflitti IP. Se i dati danneggiati vengono corretti nell'endpoint (al di fuori di vRealize Automation), è possibile riprovare l'azione Elimina.</p>

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
		<p>Gli amministratori dei gruppi di business possono forzare l'eliminazione di una distribuzione dopo che una richiesta di eliminazione non riesce. La forzatura dell'eliminazione indica a vRealize Automation di ignorare le richieste di eliminazione di risorse individuali non riuscite durante la distruzione della distribuzione. Per ulteriori informazioni sull'uso della forzatura dell'eliminazione, vedere Eliminazione forzata di una distribuzione dopo una richiesta di eliminazione non riuscita.</p> <hr/> <p>Nota Lo storage e la memoria assegnati a una macchina sottoposta a provisioning da una prenotazione vengono rilasciati quando la macchina a cui sono assegnati viene eliminata in vRealize Automation dall'azione di eliminazione. La memoria e lo storage non vengono rilasciati se la macchina viene eliminata in vCenter Server.</p> <hr/> <p>Quando si elimina una distribuzione che contiene un componente macchina Amazon, è possibile eliminare più volumi EBS contemporaneamente, in base al modo in cui è stata configurata l'impostazione Elimina volumi nel blueprint. Per ulteriori informazioni, vedere Impostazioni dei componenti macchina Amazon.</p> <p>Quando si elimina una distribuzione contenente un componente macchina Amazon, tutti i volumi EBS aggiunti alla macchina durante il suo ciclo di vita vengono scollegati anziché eliminati. vRealize Automation non fornisce alcuna opzione per l'eliminazione dei volumi EBS.</p> <hr/>
Annulla associazione IP mobile	Macchina (OpenStack)	Rimozione dell'IP mobile dalla macchina OpenStack.

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Ignora	Nessun tipo di risorsa. Richiesta di provisioning iniziale o azione non riuscita.	<p>Si ignora una richiesta non riuscita. Si annulla una richiesta in corso.</p> <ul style="list-style-type: none"> ■ Se la richiesta ignorata è una richiesta di distribuzione, la distribuzione non riuscita viene rimossa dall'elenco delle distribuzioni. ■ Se la richiesta ignorata è un'azione, la richiesta di azione non riuscita viene rimossa dalla scheda, lasciando la distribuzione nello stato precedente. <p>È necessario ignorare una richiesta di azione non riuscita in modo che sia possibile visualizzare l'esecuzione delle altre azioni nella distribuzione associata. È inoltre necessario ignorare le azioni non riuscite in modo che gli utenti della distribuzione possano visualizzare la cronologia della macchina.</p> <p>Non è possibile ignorare le richieste inviate dall'API e non blocca le azioni inviate dall'API. Questa azione è disponibile per tutte le richieste di provisioning iniziale non riuscite. Non richiede alcun permesso.</p>
Esegui riconfigurazione	Macchina	Riconfigurare immediatamente la macchina o pianificare l'azione di riconfigurazione in un secondo momento.
Scadenza	Distribuzione e Macchina	Termine del lease della macchina o della distribuzione per tutte le risorse incluse nella distribuzione.
Esporta certificato	Macchina	Esportazione del certificato da una macchina cloud.
Genera promemoria scadenza	Macchina	Download di un file di eventi calendario per la data di scadenza del lease corrente.
Installa VMware Tools	Macchina	Installazione di VMware Tools in una macchina virtuale vSphere.
Reset	Macchina	Spegnimento e riaccensione della macchina.
Spegni	Macchina	Spegnimento della macchina senza shutdown del sistema operativo guest.
Accendi	Macchina	Accensione della macchina. Se la macchina è stata sospesa, il funzionamento normale riprende dal punto in cui la macchina è stata sospesa.

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Reboot	Macchina	Riavvio del sistema operativo guest su una macchina virtuale vSphere. Per utilizzare questa azione, è necessario che sulla macchina sia installato VMware Tools.
Riconfigura	Macchina	<p>Un manager del gruppo di business, un utente di supporto o un proprietario di macchina può eseguire le seguenti azioni di riconfigurazione per la macchina virtuale vSphere selezionata:</p> <ul style="list-style-type: none"> ■ Cambiare la descrizione ■ Cambiare le impostazioni relative a CPU, memoria, rete e disco ■ Aggiungere, modificare ed eliminare proprietà personalizzate e gruppi di proprietà ■ Aggiungere, modificare, riordinare o eliminare una scheda di rete per le regole di inoltro della porta NAT ■ Riconfigurare lo shutdown ■ Modifica del proprietario di macchina (disponibile solo per manager dei gruppi di business e utenti di supporto) <p>Non è possibile modificare un criterio di prenotazione storage se è l'operazione potrebbe comportare la modifica del profilo di storage in un disco.</p> <p>Per ulteriori informazioni, vedere Come specificare le impostazioni di riconfigurazione della macchina e considerazioni sulla riconfigurazione.</p> <p>Se si seleziona l'opzione Propaga aggiornamenti alle distribuzioni esistenti nella pagina Impostazioni blueprint del blueprint di origine, qualsiasi aumento delle impostazioni minima e massima di CPU, memoria o storage nel blueprint viene propagato alle distribuzioni attive il cui provisioning è stato effettuato da tale blueprint. Per ulteriori informazioni, vedere Impostazioni delle proprietà dei blueprint.</p> <p>Non gestire oggetti NSX amministrati da vRealize Automation all'esterno di vRealize Automation. Ad esempio, se si modifica la porta membro di un bilanciamento del carico distribuito in NSX, anziché in vRealize Automation, la raccolta dei dati di NSX si interrompe. Anche le operazioni di scalabilità verticale e orizzontale generano risultati imprevisti.</p>

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Riconfigura	Bilanciamento del carico	<p>Un proprietario della macchina, utente di supporto, amministratore tenant o manager gruppo di business autorizzato può cambiare qualsiasi impostazione di un server virtuale e può aggiungere o rimuovere server virtuali nel bilanciamento del carico NSX:</p> <p>Per ulteriori informazioni, vedere Riconfigurazione di un bilanciamento del carico in una distribuzione.</p> <p>Per informazioni relative alle impostazioni del server virtuale nel bilanciamento del carico, vedere Aggiunta di un componente bilanciamento del carico su richiesta.</p> <p>Non gestire oggetti NSX amministrati da vRealize Automation all'esterno di vRealize Automation. Ad esempio, se si modifica la porta membro di un bilanciamento del carico distribuito in NSX, anziché in vRealize Automation, la raccolta dei dati di NSX si interrompe. Anche le operazioni di scalabilità verticale e orizzontale generano risultati imprevisti.</p>
Registra VDI	Macchina virtuale (XenServer)	Registrazione dell'immagine di disco virtuale su elementi XenServer.
Rimuovi dal catalogo	Distribuzioni	Rimuovere le risorse di cui è stato eseguito il provisioning XaaS dal catalogo. È possibile eseguire questa operazione su oggetti esistenti e oggetti che non sono più nell'inventario di Orchestrator.

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Riesegui provisioning	Macchina	<p>Elimina la macchina, quindi avvia il workflow di provisioning per creare una macchina con lo stesso nome.</p> <p>Quando si richiede la riesecuzione del provisioning di una macchina, a causa di un problema noto è possibile che nel catalogo di vRealize Automation lo stato di riesecuzione del provisioning venga indicato come completato mentre invece è ancora in corso. Dopo l'invio di una richiesta di riesecuzione del provisioning di una macchina, è possibile verificare lo stato della macchina utilizzando una delle seguenti sequenze:</p> <ul style="list-style-type: none"> ■ Infrastruttura > Macchine gestite ■ Scheda Distribuzioni ■ Amministrazione > Eventi > Registri eventi <hr/> <p>Nota Non è possibile rieseguire il provisioning di una macchina Amazon.</p> <hr/> <p>Per informazioni correlate, vedere l'articolo 2065873 della Knowledge Base di VMware "Reprovisioned machine tasks" all'indirizzo http://kb.vmware.com/kb/2065873.</p>
Invia di nuovo	Nessun tipo di risorsa. Richiesta di provisioning iniziale non riuscita.	<p>Inviare nuovamente una richiesta di provisioning non riuscita. La richiesta nuovamente inviata parte all'inizio del processo di provisioning con i valori già immessi.</p> <p>Se una richiesta non riesce e il problema può essere risolto, è possibile inviare nuovamente la richiesta, anziché crearne una nuova. Se l'errore è dovuto a valori non corretti, ad esempio un datastore che non supporta la richiesta, è necessario creare una nuova richiesta con i nuovi valori.</p> <p>Questa azione è disponibile per tutte le richieste di provisioning iniziale non riuscite. Non richiede alcun permesso.</p>

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Riprendi	Profilo di	<p>Riprendere la richiesta di provisioning parzialmente completata. La richiesta continua dal punto di errore.</p> <p>Se una distribuzione non riesce durante il processo di provisioning a causa di problemi temporanei dell'ambiente o dell'infrastruttura, timeout o altri problemi che possono essere risolti all'esterno della richiesta, è possibile riprendere il processo di provisioning, anziché creare una nuova richiesta di provisioning. Se la non corretta esecuzione dell'operazione è stata causata da errori nel blueprint, la ripresa non funziona. È necessario richiedere una nuova distribuzione anziché tentare la ripresa.</p> <p>Se una richiesta di distribuzione riesce solo parzialmente ed è possibile risolvere il problema, è possibile utilizzare l'azione di ripresa. La richiesta ripresa continua dal punto di errore.</p> <p>Per ulteriori informazioni, vedere Funzionamento dell'azione Riprendi.</p>
Ripristina snapshot	Macchina virtuale	<p>Ripristino di uno snapshot precedente della macchina. Per utilizzare questa azione è necessario disporre di uno snapshot esistente.</p>

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Scalabilità verticale	Distribuzione	<p>Consente di eliminare le istanze non necessarie delle macchine nella distribuzione per l'adeguamento ai ridotti requisiti di capacità. Vengono eliminati i componenti macchina e tutti i componenti software installati su di essi. I componenti software dipendenti e i componenti di rete e sicurezza vengono aggiornati per la configurazione di distribuzione nuova. I componenti di XaaS non sono scalabili e non vengono aggiornati durante le operazioni di scalabilità.</p> <p>È possibile tentare di riparare le operazioni di scalabilità riuscite parzialmente provando a scalare nuovamente la distribuzione.</p> <p>Tuttavia, non è possibile scalare una distribuzione alla sua dimensione corrente e la correzione di un'operazione di scalabilità parzialmente riuscita in questo modo non comporta l'annullamento dell'allocazione delle risorse tralasciate. È possibile visualizzare la schermata dei dettagli di esecuzione delle richieste e identificare le attività che non sono riuscite e su quali nodi per decidere se correggere l'operazione di scalabilità parzialmente riuscita con un'altra operazione di scalabilità. Le operazioni di scalabilità non riuscite o parzialmente non riuscite non influiscono sulla funzionalità della distribuzione originale ed è possibile continuare a utilizzare gli elementi del catalogo durante la risoluzione di eventuali problemi.</p>

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Scalabilità orizzontale	Distribuzione	<p>Consente di eseguire il provisioning di istanze aggiuntive delle macchine nella propria distribuzione per l'adeguamento all'aumento dei requisiti di capacità. Viene eseguito il provisioning dei componenti macchina e di tutti i componenti software installati su di essi. I componenti software dipendenti e i componenti di rete e sicurezza vengono aggiornati per la configurazione di distribuzione nuova. I componenti di XaaS non sono scalabili e non vengono aggiornati durante le operazioni di scalabilità.</p> <p>È possibile tentare di riparare le operazioni di scalabilità riuscite parzialmente provando a scalare nuovamente la distribuzione. Tuttavia, non è possibile scalare una distribuzione alla sua dimensione corrente e la correzione di un'operazione di scalabilità parzialmente riuscita in questo modo non comporta l'annullamento dell'allocazione delle risorse tralasciate. È possibile visualizzare la schermata dei dettagli di esecuzione delle richieste e identificare le attività che non sono riuscite e su quali nodi per decidere se correggere l'operazione di scalabilità parzialmente riuscita con un'altra operazione di scalabilità. Le operazioni di scalabilità non riuscite o parzialmente non riuscite non influiscono sulla funzionalità della distribuzione originale ed è possibile continuare a utilizzare gli elementi del catalogo durante la risoluzione di eventuali problemi.</p> <p>Se si seleziona l'opzione Propaga aggiornamenti alle distribuzioni esistenti nella pagina Impostazioni blueprint del blueprint di origine, qualsiasi aumento delle impostazioni minima e massima di CPU, memoria o storage nel blueprint viene propagato alle distribuzioni attive il cui provisioning è stato effettuato da tale blueprint. Per ulteriori informazioni, vedere Impostazioni delle proprietà dei blueprint.</p>
Shutdown	Macchina	<p>Shutdown del sistema operativo guest e spegnimento della macchina. Per utilizzare questa azione, è necessario che sulla macchina sia installato VMware Tools.</p>

Tabella 4-2. Comandi del menu Azione (continua)

Azione	Tipo di risorsa	Descrizione
Sospendi	Macchina	Messa in pausa della macchina, che nel frattempo non potrà essere utilizzata e non consumerà risorse del sistema diverse dallo storage utilizzato.
Annula registrazione	Macchina	Rimozione della macchina dall'inventario senza eliminarla. Le macchine di cui sia stata annullata la registrazione non sono utilizzabili.
Annula registrazione	Rete	Rimozione della rete dall'inventario senza eliminarla. Le reti non registrate non sono utilizzabili.
Annula registrazione VDI	Macchina virtuale (XenServer)	Annullamento della registrazione dell'immagine di disco virtuale su elementi XenServer.

Risoluzione dei problemi relativi alle azioni mancanti nel menu Azioni risorsa

Il proprietario di una macchina o di una risorsa non vede tutte le azioni autorizzate per un elemento di cui è stato eseguito il provisioning.

Problema

In un ambiente in cui si sa che un'azione è stata autorizzata per un utente o un gruppo di business, ci si aspetta di vedere tutte le azioni disponibili quando si seleziona un elemento nell'elenco **Distribuzione**.

Causa

Tuttavia, la disponibilità delle azioni dipende dallo stato operativo e dal tipo della risorsa di cui è stato eseguito il provisioning, nonché da come è stata configurata e resa disponibile. L'elenco seguente include alcuni dei motivi per i quali potrebbero non essere visibili tutte le azioni configurate.

- L'azione non è applicabile, sulla base dello stato corrente della risorsa di cui è stato eseguito il provisioning. Ad esempio, Spegni è disponibile solo se la macchina è accesa.
- L'azione non è applicabile al tipo di elemento selezionato. Se l'elemento non supporta l'azione, questa non viene inclusa nell'elenco. Ad esempio, l'azione Crea snapshot non è disponibile per una macchina fisica e l'azione Connessione con RDP non è disponibile se l'elemento selezionato è una macchina Linux.
- L'azione è applicabile per il tipo di risorsa di cui è stato eseguito il provisioning, ma è disattivata nel blueprint dell'infrastruttura. Le azioni disattivate non sono mai elencate tra le azioni disponibili per nessuno degli elementi il cui provisioning è stato eseguito mediante il blueprint.
- L'azione non è inclusa nel permesso utilizzato per il provisioning dell'elemento in cui è necessario eseguire l'azione. Nel menu Azioni vengono elencate solo le azioni autorizzate come parte di un blueprint IaaS o come azioni risorsa XaaS.

- L'azione è stata creata come azione risorsa XaaS ma non è stata inclusa nel permesso utilizzato per il provisioning dell'elemento in cui è necessario eseguire l'azione. Nel menu Azioni vengono elencate solo le azioni autorizzate.
- L'azione potrebbe essere limitata in base ai criteri target configurati per le azioni risorsa XaaS o alle mappature delle risorse alle macchine IaaS di cui è stato eseguito il provisioning.

Soluzione

- ◆ Accertarsi che l'azione sia applicabile all'elemento di cui è stato eseguito il provisioning o al suo stato.
- ◆ Verificare che l'azione sia configurata e inclusa nel permesso utilizzato per eseguire il provisioning dell'elemento.

Creazione di uno snapshot della macchina

In base alla configurazione dell'ambiente operativo definita dagli amministratori, può essere possibile creare uno snapshot della macchina virtuale. Uno snapshot è l'immagine di una macchina virtuale in uno specifico momento. Si tratta in sostanza di una copia dell'immagine VM originale, ma dalle dimensioni ottimizzate. Gli snapshot rappresentano un modo semplice di ripristinare un sistema dopo un danno, una perdita di dati o una minaccia alla sicurezza. Dopo aver creato uno snapshot della macchina virtuale, è possibile applicarlo e riportare il sistema esattamente al punto in cui era quando è stato creato lo snapshot.

Quando si crea uno snapshot memoria, lo snapshot cattura lo stato delle impostazioni di alimentazione della macchina virtuale e, facoltativamente, la memoria della macchina virtuale. L'operazione di cattura dello snapshot richiede più tempo quando si acquisisce anche la memoria della macchina virtuale. Potrebbe inoltre verificarsi un rallentamento momentaneo nella risposta in rete.

Prerequisiti

- Una macchina virtuale esistente accesa, spenta o sospesa.
- Se la macchina virtuale è configurata per uno o più dischi indipendenti, spegnere la macchina prima di creare uno snapshot. Non è possibile creare uno snapshot quando la macchina è accesa. Per informazioni sulla configurazione dei dischi, vedere *Tabella delle proprietà personalizzate che iniziano con V*.
- L'azione snapshot è stata autorizzata dall'amministratore tenant o dal manager del gruppo di business.

Procedura

- 1 Fare clic su **Distribuzioni**.
- 2 Individuare la distribuzione che include la macchina di cui eseguire lo snapshot e fare clic sul nome della distribuzione.

- 3 Nella scheda **Componenti**, fare clic sulla macchina virtuale e fare clic sull'icona delle azioni a forma di ingranaggio.

Viene visualizzato il menu delle azioni del componente.

- 4 Fare clic su **Crea snapshot** nel menu Azioni.
- 5 Immettere un nome e, facoltativamente, una descrizione.
- 6 Per catturare le impostazioni di memoria e alimentazione della macchina, selezionare **Includere la memoria?**.
- 7 Fare clic su **Invia**.

Connessione remota a una macchina

È possibile connettersi in remoto a una macchina dalla console di vRealize Automation.

Se si utilizza VMware Remote Console per la connessione, consultare l'articolo della Knowledge Base [Troubleshooting VMRC connectivity in vRealize Automation \(2114235\)](#).

Prerequisiti

- Accedere a vRealize Automation come **proprietario macchina, amministratore tenant o manager del gruppo di business**.

- Assicurarsi che VMware Tools sia installato.

VMware Tools deve essere installato sul client vRealize Automation per supportare l'accesso con funzionamento completo mediante la connessione con VMware Remote Console. Se VMware Tools non è installato, dopo la connessione alla macchina di destinazione si verificano problemi quali il non funzionamento del puntatore e dei tasti del mouse. Per informazioni sulle versioni supportate di VMware Tools, vedere *Matrice di supporto di vRealize Automation* nella [documentazione del prodotto di vRealize Automation](#).

- Assicurarsi che la macchina fornita in provisioning sia accesa.
- Consente il traffico di rete tra le appliance vRealize Automation e il server ESXi sulla porta 902.
- Consente il traffico di rete tra le appliance vRealize Automation e il browser client sulla porta 8444.
- Consente il traffico di rete tra i server Windows con il componente Web IaaS e gli endpoint di vSphere associati sulla porta 443.

Procedura

- 1 Fare clic su **Distribuzioni**.
- 2 Individuare la distribuzione che include la macchina che è necessario connettere e fare clic sul nome della distribuzione.

- 3 Nella scheda **Componenti**, individuare la macchina e fare clic sull'icona delle azioni a forma di ingranaggio.

Viene visualizzato il menu delle azioni del componente.

- 4 Selezionare il metodo di connessione remota.

- Selezionare **Connessione con RDP** per effettuare la connessione usando l'RDP.
- Selezionare **Connetti a console remota** per effettuare la connessione usando VMware Remote Console.

Fornire eventuali informazioni richieste.

- 5 Fare clic su **Connetti** e accedere alla macchina come da istruzioni.

- 6 Al termine, disconnettersi e chiudere la finestra del browser.

Configurazione di console remote per vSphere con certificati SSL non attendibili

Se la distribuzione di vRealize Automation utilizza certificati non attendibili, prima di poter utilizzare console remote con VMware Remote Console è necessario configurare il browser client affinché consideri attendibili i certificati. I passaggi per eseguire tale operazione variano in base al browser in uso.

se vRealize Automation è configurato con un certificato SSL attendibile per l'ambiente, VMware Remote Console non richiede alcuna configurazione aggiuntiva sui browser dei client. Quando un certificato dell'appliance vRealize Automation viene sostituito ed è attendibile, non è necessario aggiornare le informazioni sul certificato per il client del browser Web.

Per sostituire il certificato, consultare l'argomento sulla sostituzione di un certificato di Appliance vRealize Automation nella guida *Amministrazione di sistema* per vRealize Automation.

Le connessioni remote che utilizzano VMware Remote Console per le macchine con provisioning eseguito in vSphere sono protette da certificati dell'appliance vRealize Automation mediante una console proxy. VMware Remote Console richiede il supporto di WebSockets nel browser e i browser devono considerare attendibile il certificato dell'appliance vRealize Automation. Il certificato può essere ottenuto accedendo all'appliance virtuale a livello radice con un indirizzo nella forma <https://vra-vr.eng.mycompany.com/>.

Per informazioni sui requisiti relativi al supporto per i browser e vSphere, vedere *Matrice di supporto di vRealize Automation*.

Configurazione di Firefox in modo che consideri attendibile un certificato per vRealize Automation

I certificati dell'appliance vRealize Automation non attendibili devono essere importati manualmente nei browser dei client per supportare VMware Remote Console nei client con provisioning eseguito in vSphere.

Per informazioni sulle versioni supportate di Firefox, vedere *VMware vRealize Support Matrix* nel [centro informazioni](#) di vRealize Automation.

Nota se vRealize Automation è configurato con un certificato SSL attendibile per l'ambiente, VMware Remote Console non richiede alcuna configurazione aggiuntiva sui browser dei client.

Procedura

- 1 In un browser Firefox, accedere all'appliance vRealize Automation.
Viene visualizzato un messaggio che informa l'utente che il certificato non è attendibile.
- 2 Selezionare **Apri menu > Opzioni**.
- 3 Fare clic su **Privacy e sicurezza**, quindi fare clic su **Visualizza certificati**.
- 4 Nella finestra di dialogo Gestione certificati, fare clic su **Server**, quindi fare clic su **Aggiungi eccezione**.
- 5 Aggiungere l'URL dell'appliance vRealize Automation con la porta 8444.
Ad esempio `https://your-vra-fqdn-domain:8444`.
- 6 Fare clic su **Recupera certificato** e quindi su **Conferma eccezione di sicurezza**.
- 7 Fare clic su **OK**.

Risultati

La connessione alla console remota avverrà senza errori di certificato.

Configurazione di Internet Explorer in modo che consideri attendibile un certificato per vRealize Automation Appliance

I certificati di Appliance vRealize Automation non attendibili devono essere importati manualmente nei browser dei client per supportare VMware Remote Console sui client con provisioning eseguito su vSphere.

Nota se vRealize Automation è configurato con un certificato SSL attendibile per l'ambiente, VMware Remote Console non richiede alcuna configurazione aggiuntiva sui browser dei client.

I passaggi riportati in questa procedura si applicano in presenza di certificati autofirmati e di certificati emessi da un'autorità di certificazione.

Per informazioni sulle versioni di Internet Explorer supportate, fare riferimento alla *Matrice di supporto di VMware vRealize* sul sito Web di VMware.

Procedura

- 1 Da un browser Internet Explorer, accedere a Appliance vRealize Automation.
- 2 Fare clic su **Visualizza certificato** nel messaggio di errore del certificato visualizzato nella barra degli indirizzi del browser.
- 3 Fare clic sulla scheda **Generale** della finestra Informazioni sul certificato.
- 4 Verificare che le informazioni sul certificato siano corrette e fare clic su **Installa certificato**.
- 5 Selezionare **Colloca tutti i certificati nel seguente archivio** nella finestra di dialogo Archivio certificati.
- 6 Fare clic su **Sfoggia** per selezionare l'archivio dei certificati.
- 7 Selezionare **Autorità di certificazione radice attendibile** e fare clic su **OK**.

- 8 Fare clic su **Avanti** nella finestra di dialogo Archivio certificati.
- 9 Fare clic su **Sì** nella finestra di dialogo Avviso di protezione per installare il certificato.
- 10 Riavviare il browser.

Risultati

La connessione alla console remota avverrà senza errori di certificato.

Configurazione di Chrome in modo che consideri attendibile un certificato per vRealize Automation Appliance

I certificati di Appliance vRealize Automation non attendibili devono essere importati manualmente nei browser dei client per supportare VMware Remote Console sui client con provisioning eseguito su vSphere.

Per informazioni sulle versioni supportate di Chrome, vedere *Matrice di supporto di vRealize Automation* nella [documentazione del prodotto vRealize Automation](#).

Nota se vRealize Automation è configurato con un certificato SSL attendibile per l'ambiente, VMware Remote Console non richiede alcuna configurazione aggiuntiva sui browser dei client.

In Windows, Chrome e Internet Explorer utilizzano lo stesso archivio di certificati. Questo significa che i certificati attendibili in Internet Explorer sono attendibili anche in Chrome. Per far sì che Chrome consideri attendibili i certificati, importarli tramite Internet Explorer. Per informazioni su questa procedura, vedere [Configurazione di Internet Explorer in modo che consideri attendibile un certificato per vRealize Automation Appliance](#).

Terminata la procedura, riavviare Chrome.

Per rendere attendibile un certificato in modo permanente sul sistema operativo Macintosh, scaricare il file del certificato e installare il certificato come attendibile nello strumento di gestione dei certificati utilizzato.

Procedura

- 1 Da un browser Chrome, accedere a Appliance vRealize Automation.
- 2 Fare clic sull'icona *Visualizza informazioni sul sito* accanto alla barra degli indirizzi del browser e fare clic sull'icona **Certificato** per visualizzare le informazioni sul certificato.
- 3 Salvare il certificato.
- 4 Avviare l'applicazione Keychain Access, che si trova in genere nella cartella Utilities della cartella Applications.
- 5 Selezionare **File > Import Items**.
- 6 Nella schermata di Keychain Access, selezionare il file del certificato precedentemente salvato.

Impostare il valore di **Destination Key** su **System**.
- 7 Fare clic su **Open** per importare il certificato.

8 Riavviare il browser.

Come specificare le impostazioni di riconfigurazione della macchina e considerazioni sulla riconfigurazione

Le piattaforme vSphere, vCloud Air e vCloud Director supportano la riconfigurazione delle macchine esistenti in una distribuzione per la modifica di specifiche quali CPU, memoria e storage.

Le richieste di riconfigurazione sono soggette all'approvazione in base ai permessi, ai criteri e alle azioni abilitate per il componente macchina nel blueprint.

La riconfigurazione di una macchina virtuale assegnata a una rete su richiesta non è supportata. Non è possibile riconfigurare una NIC collegata a una rete su richiesta. Se si prova a riconfigurare una rete su richiesta NAT o instradata, viene visualizzato il messaggio di errore `Original network [<network>] is not selected in the machine's reservation.`, le reti nella macchina restano intatte e gli indirizzi IP nella macchina non vengono modificati.

Se si dispone dei permessi per le azioni Annulla riconfigurazione (macchina) ed Esegui riconfigurazione (macchina), è possibile annullare una riconfigurazione o ripetere una riconfigurazione non riuscita.

L'espansione di un disco in una macchina virtuale il cui provisioning è stato eseguito da un blueprint clone collegato non è supportata.

Non è possibile riconfigurare le macchine utilizzando i profili componente **Size** o **Image**. L'intervallo di CPU, memoria e storage viene calcolato dal profilo e rimane disponibile per le azioni di riconfigurazione. Ad esempio, utilizzare un set di valori **Size** piccolo (1 CPU, 1024 MB di memoria e 10 GB di storage), medio (3 CPU, 2048 MB di memoria, 12 GB di storage) e grande (5 CPU, 3072 MB di memoria, 15 GB di storage). Gli intervalli disponibili durante la riconfigurazione della macchina sono 1-5 CPU, 1024-3072 MB di memoria e 1-15 GB di storage.

vRealize Automation esegue uno snapshot del blueprint in fase di distribuzione. Se si verificano i problemi di riconfigurazione durante l'aggiornamento delle proprietà della macchina quali CPU e memoria RAM in una distribuzione, vedere l'articolo della Knowledge Base [2150829 relativo alla creazione dello snapshot blueprint vRA 7.x](#).

Prerequisiti

- Accedere a vRealize Automation come **proprietario macchina, utente di supporto, utente del gruppo di business con ruolo accesso condiviso o manager del gruppo di business**.
- La macchina da riconfigurare deve essere nello stato accesa o spenta, senza alcuno stato di riconfigurazione attivo.
- Il tipo di macchina deve essere vSphere, vCloud Air o vCloud Director, anche se le impostazioni di NSX si applicano solo a vSphere.
- Verificare di disporre del permesso per riconfigurare una macchina.

Procedura

- 1 Fare clic su **Distribuzioni**.

- 2 Individuare la distribuzione che include la macchina da riconfigurare e fare clic sul nome della distribuzione.
- 3 Nella scheda **Componenti**, fare clic sulla macchina virtuale e fare clic sull'icona delle azioni a forma di ingranaggio.

Viene visualizzato il menu delle azioni del componente.

- 4 Selezionare **Riconfigura**.
- 5 Selezionare la scheda appropriata per le impostazioni che si intende riconfigurare.

Tabella 4-3. Modifiche della richiesta di riconfigurazione

Scheda	Argomento
Generale	Riconfigurazione di CPU e memoria
Storage	Modifica delle impostazioni di storage
Rete	Modifica delle impostazioni di rete Per modificare le regole NAT, vedere Modifica di regole NAT in una distribuzione .
Sicurezza	Per riconfigurare le impostazioni di sicurezza, vedere Aggiunta o rimozione di elementi di sicurezza in una distribuzione .
Proprietà	Modifica delle impostazioni delle proprietà personalizzate e dei gruppi di proprietà

Operazioni successive

[Esecuzione della riconfigurazione della macchina richiesta](#) .

Riconfigurazione di CPU e memoria

È possibile cambiare il numero di CPU o la quantità di memoria e storage utilizzati dalla macchina fornita in provisioning, entro i limiti impostati dal blueprint del provisioning.

Per le distribuzioni Amazon con provisioning, è possibile riconfigurare tutti i volumi di storage nella distribuzione ad eccezione del volume principale.

L'espansione di un disco in una macchina virtuale il cui provisioning è stato eseguito da un blueprint clone collegato non è supportata.

Prerequisiti

[Come specificare le impostazioni di riconfigurazione della macchina e considerazioni sulla riconfigurazione](#).

Procedura

- 1 Fare clic sulla scheda **Generale**.
- 2 Immettere il numero di CPU nella casella di testo **CPU**.
- 3 Immettere la quantità di memoria nella casella di testo **Memoria (MB)**.

4 Immettere la quantità di storage nella casella di testo **Storage (GB)**.

Operazioni successive

Specificare altre impostazioni di riconfigurazione della macchina. Dopo avere completato la modifica delle impostazioni della macchina, avviare la richiesta di riconfigurazione. Vedere [Esecuzione della riconfigurazione della macchina richiesta](#).

Modifica delle impostazioni di storage

È possibile aggiungere, eliminare o cambiare la dimensione di un volume di storage su una macchina virtuale di cui è stato eseguito il provisioning.

Non è possibile riconfigurare lo storage per il tipo di dischi IDE.

Lo storage e la memoria assegnati a una macchina sottoposta a provisioning da una prenotazione vengono rilasciati quando la macchina a cui sono assegnati viene eliminata in vRealize Automation dall'azione di eliminazione. La memoria e lo storage non vengono rilasciati se la macchina viene eliminata in vCenter Server.

Ad esempio, non è possibile eliminare una prenotazione associata alle macchine in una distribuzione esistente. Se si spostano o si eliminano manualmente macchine distribuite in vCenter Server, vRealize Automation continua a riconoscere le macchine distribuite come funzionanti e impedisce l'eliminazione delle prenotazioni associate.

È possibile modificare alcune impostazioni, ad esempio la capacità e il criterio di prenotazione storage, dopo il provisioning e la distribuzione della macchina.

I valori di **Lettera di unità/Percorso di montaggio** ed **Etichetta** vengono applicati all'agente guest al momento del provisioning. Questi valori non vengono aggiornati dopo il provisioning e pertanto potrebbero non essere attuali. Per raccogliere i dati e visualizzarne i rispettivi valori correnti, è possibile creare ed eseguire un workflow di vRealize Orchestrator personalizzato.

Prerequisiti

[Come specificare le impostazioni di riconfigurazione della macchina e considerazioni sulla riconfigurazione.](#)

Per le distribuzioni Amazon con provisioning effettuato, è possibile riconfigurare tutti i volumi di storage nella distribuzione ad eccezione del volume principale.

Procedura

- 1 Fare clic sulla scheda **Storage**.
- 2 Visualizzare o modificare le opzioni di storage in base alle necessità.

- Se disponibile, aggiungere un nuovo volume.
- Se disponibile, eliminare un volume.

Un'icona non selezionabile indica un volume che non può essere eliminato, come ad esempio un volume proveniente da un clone collegato.

- Se disponibile, modificare la dimensione di un volume.

Non è possibile ridurre la dimensione di volumi esistenti. La dimensione del volume è limitata dalla quantità totale di storage specificata nel blueprint, meno la quantità allocata in altri volumi.

Operazioni successive

Specificare altre impostazioni di riconfigurazione della macchina. Dopo avere completato la modifica delle impostazioni della macchina, avviare la richiesta di riconfigurazione. Vedere [Esecuzione della riconfigurazione della macchina richiesta](#).

Modifica delle impostazioni di rete

È possibile aggiungere, rimuovere o modificare una scheda di rete.

Durante il processo di riconfigurazione della macchina, è possibile modificare le impostazioni di rete riportate di seguito:

- Aggiungere o rimuovere le NIC.
- Allocare o rilasciare indirizzi IP per le NIC esistenti.
- Assegnare nuovi indirizzi IP alle NIC, a condizione che la rete non sia una NAT su richiesta o una rete instradata su richiesta.

Non è possibile riconfigurare una rete instradata o NAT su richiesta.

Per eseguire la riconfigurazione di rete, è necessario che le reti di origine e target siano selezionate nella prenotazione.

Quando si aggiungono le NIC, gli indirizzi IP vengono allocati. Quando si rimuovono le NIC, gli indirizzi IP vengono rilasciati.

Dopo aver modificato le impostazioni dirette in base alle informazioni della prenotazione e del profilo di rete, il nuovo indirizzo IP di rete viene assegnato in vRealize Automation, tuttavia la macchina distribuita non viene aggiornata nell'endpoint con i nuovi dati dell'indirizzo IP. È necessario assegnare manualmente l'indirizzo IP alla macchina al termine del processo di riconfigurazione.



La riconfigurazione di una macchina virtuale assegnata a una rete su richiesta non è supportata. Non è possibile riconfigurare una NIC collegata a una rete su richiesta. Se si prova a riconfigurare una rete su richiesta NAT o instradata, viene visualizzato il messaggio di errore `Original network [<network>] is not selected in the machine's reservation.`, le reti nella macchina restano intatte e gli indirizzi IP nella macchina non vengono modificati.



La modifica delle impostazioni di rete di NSX non è supportata per le distribuzioni aggiornate o migrate da vRealize Automation 6.2.x a questa release di vRealize Automation.

Prerequisiti

[Come specificare le impostazioni di riconfigurazione della macchina e considerazioni sulla riconfigurazione.](#)

Procedura

- 1 Fare clic sulla scheda **Rete**.
- 2 (Facoltativo) Aggiungere una scheda di rete.
 - a Fare clic su **Nuova scheda di rete**.
 - b Selezionare una rete dal menu a discesa **Percorso di rete**.
Sono disponibili tutte le reti selezionate nella prenotazione della macchina.
 - c Immettere un indirizzo IP statico per la rete nella casella di testo **Indirizzo**.
L'indirizzo IP non deve essere allocato nel profilo di rete assegnato alla prenotazione.
 - d Fare clic sull'icona **Salva** ()
- 3 (Facoltativo) Rimuovere una scheda di rete.
 - a Individuare la scheda di rete.
 - b Fare clic sull'icona **Elimina** ()

Non è possibile rimuovere la scheda di rete 0.
- 4 (Facoltativo) Modificare una scheda di rete.
 - a Individuare la scheda di rete.
 - b Fare clic sull'icona **Modifica** ()
 - c Selezionare una rete dal menu a discesa **Percorso di rete**.
 - d Fare clic sull'icona **Salva** ()

Operazioni successive

Specificare altre impostazioni di riconfigurazione della macchina. Dopo avere completato la modifica delle impostazioni della macchina, avviare la richiesta di riconfigurazione. Vedere [Esecuzione della riconfigurazione della macchina richiesta](#).

Modifica delle impostazioni delle proprietà personalizzate e dei gruppi di proprietà

È possibile modificare, aggiungere o eliminare proprietà personalizzate nella macchina distribuita.

Non è possibile utilizzare le proprietà personalizzate per inserire valori relativi a numero di dischi di volumi, capacità, etichette o criteri di prenotazione di storage. Tali valori devono essere immessi aggiungendo o modificando un volume nella tabella dei volumi di storage. Vedere [Modifica delle impostazioni di storage](#).

Prerequisiti

[Come specificare le impostazioni di riconfigurazione della macchina e considerazioni sulla riconfigurazione.](#)

Procedura

- 1 Fare clic sulla scheda **Proprietà**.
- 2 Per aggiungere una proprietà, fare clic su **Nuova proprietà**.
- 3 Immettere il nome della proprietà nella casella di testo **Nome**.
- 4 Immettere il valore della proprietà nella casella di testo **Valore**.
- 5 Selezionare la casella di controllo **Codificato** per crittografare il valore.
- 6 Selezionare la casella di controllo **Richiedi conferma** per chiedere agli utenti il valore quando richiedono la macchina.
- 7 Aggiungere un'altra proprietà, modificare una proprietà esistente o eliminare una proprietà.

Operazioni successive

Specificare impostazioni di riconfigurazione macchina aggiuntive. Una volta completata la modifica delle impostazioni della macchina, avviare la richiesta di riconfigurazione macchina. Vedere [Esecuzione della riconfigurazione della macchina richiesta](#).

Esecuzione della riconfigurazione della macchina richiesta

È possibile avviare la riconfigurazione immediatamente o pianificarla a una data e a un'ora specifiche. È anche possibile specificare l'opzione di alimentazione per la macchina prima di riconfigurarla.

Prerequisiti

[Come specificare le impostazioni di riconfigurazione della macchina e considerazioni sulla riconfigurazione.](#)

Procedura

- 1 Se la scheda **Esecuzione** è visibile, è possibile selezionarla per specificare impostazioni di riconfigurazione aggiuntive. Se non è visibile, fare clic su **Invia** per avviare la riconfigurazione della macchina.
- 2 Se la scheda **Esecuzione** è visibile, fare clic su **Esecuzione** per pianificare l'azione di riconfigurazione.
- 3 (Facoltativo) Selezionare un'opzione dal menu a discesa **Esegui richiesta**.

Opzione	Descrizione
Immediato	Avvia la riconfigurazione appena possibile dopo l'approvazione.
Pianificato	Avvia la riconfigurazione alla data e all'ora specificate. Immettere la data e l'ora nelle caselle di testo visualizzate.

La data e l'ora pianificate sono nell'ora locale del luogo in cui si trova il server Web di vRealize Automation. Se **Esegui richiesta** non è disponibile, la riconfigurazione viene avviata immediatamente.

4 (Facoltativo) Selezionare un'azione di alimentazione dal menu a discesa **Azione alimentazione**.

Opzione	Descrizione
Riavvia se necessario	(Predefinita) Se richiesto, riavvia la macchina prima di riconfigurarla.
Riavvio	Riavvia la macchina prima di riconfigurarla, indipendentemente dal fatto che sia o meno necessario riavviarla.
Non riavviare	Non riavvia la macchina prima di riconfigurarla, anche se il riavvio è necessario.

Il riavvio della macchina prima della riconfigurazione è necessario nelle seguenti condizioni:

- Cambia la CPU in una macchina in cui l'aggiunta a caldo non è supportata o è disattivata
- Cambia la memoria in una macchina in cui la memoria a caldo non è supportata o è disattivata
- Cambia lo storage in una macchina in cui lo storage a caldo è disattivato

Se la macchina è nello stato di arresto, non viene riavviata.

Nota È possibile disattivare l'opzione di aggiunta a caldo di vSphere utilizzando la proprietà personalizzata `VirtualMachine.Reconfigure.DisableHotCpu`.

5 Fare clic su **OK**.

Operazioni successive

È possibile monitorare l'avanzamento della riconfigurazione osservando gli stati del workflow visualizzati nell'interfaccia utente. Vedere [Stati del workflow nelle operazioni di riconfigurazione](#).

Stati del workflow nelle operazioni di riconfigurazione

All'avvio di una riconfigurazione e man mano che questa procede nel workflow, è possibile monitorare l'avanzamento dalla pagina Modifica.

Tabella 4-4. Stati del workflow nelle operazioni di riconfigurazione

Stato	Descrizione
Riconfigurazione in sospeso	L'operazione di stato è stata creata.
Pianificato	È stato creato un workflow pianificato per il Distributed Execution Manager (DEM).
Riconfigurazione	Il workflow specifico dell'interfaccia è in esecuzione.
Riconfigurazione non riuscita, in attesa per riprovare	La riconfigurazione non è riuscita, in attesa di una richiesta di riprovare da parte del proprietario. Se il proprietario della macchina è autorizzato riconfigurare o annullare le azioni di riconfigurazione, può riprovare o annullare l'operazione di riconfigurazione.
Riconfigurazione non riuscita	La riconfigurazione non è riuscita, in attesa dell'esecuzione dell'azione successiva del workflow.
Riconfigurazione eseguita	La riconfigurazione è stata eseguita, in attesa dell'esecuzione dell'azione successiva del workflow.

Tabella 4-4. Stati del workflow nelle operazioni di riconfigurazione (continua)

Stato	Descrizione
Annullato	L'utente ha annullato la riconfigurazione. I proprietari delle macchine autorizzate possono annullare una riconfigurazione.
Completato	Il workflow di completamento imposta questo stato dopo aver completato la pulizia, in modo che il workflow possa procedere nella pulizia delle operazioni di stato e delle approvazioni. Lo stato di completamento indica che la richiesta da vRealize Automation è terminata, ma non indica che la riconfigurazione della macchina è stata eseguita con successo.

Riconfigurazione di un bilanciamento del carico in una distribuzione

È possibile aggiungere, modificare o eliminare un server virtuale in un bilanciamento del carico NSX distribuito.

Le considerazioni seguenti si applicano alle distribuzioni con origine in vRealize Automation 7.2 o versioni precedenti:

- La riconfigurazione del bilanciamento del carico è limitata alle distribuzioni contenenti un solo bilanciamento del carico.
- Nella pagina dei dettagli Elementi per ciascun bilanciamento del carico di una distribuzione sono visualizzati i server virtuali utilizzati da tutti i bilanciamenti del carico nella distribuzione. Per ulteriori informazioni, consultare l'[articolo 2150276 della Knowledge Base](#).
- L'operazione di riconfigurazione del bilanciamento del carico non è supportata per le distribuzioni che sono state aggiornate o migrate da vRealize Automation 6.2.x a questa release di vRealize Automation.

Per i bilanciamenti del carico aggiornati e quelli distribuiti nella versione di vRealize Automation corrente, non modificare un server virtuale e aggiungere un server virtuale nella stessa richiesta. Per ulteriori informazioni, consultare l'[articolo 2150240 della Knowledge Base](#).

Nota L'azione **Riconfigura** non è supportata per i bilanciamenti del carico di NSX-T.

Se si invia una richiesta per riconfigurare un bilanciamento del carico mentre nella distribuzione è in esecuzione un'altra azione, ad esempio se è in corso un'operazione di scalabilità orizzontale, la riconfigurazione non riesce e viene visualizzato un messaggio dell'assistenza. In questa situazione è possibile attendere fino al completamento dell'azione e quindi inviare la richiesta di riconfigurazione.

Nota Quando il blueprint associato alla distribuzione viene importato da un file YAML contenente un bilanciamento del carico su richiesta con un valore nel campo del nome diverso dal valore presente nel campo dell'ID, l'azione **Riconfigura** non riesce. Per abilitare l'opzione di riconfigurazione del bilanciamento del carico per una distribuzione basata su un blueprint importato, eseguire i passaggi seguenti nel blueprint per consentire azioni di post-provisioning per i componenti del bilanciamento del carico nelle distribuzioni future.

- 1 Nella console di vRealize Automation, selezionare il blueprint.
- 2 Fare clic su **Modifica** e modificare il nome del blueprint. Questa operazione consente di impostare il nome e l'ID incorporati sullo stesso valore.
- 3 Selezionare il componente del bilanciamento del carico nel blueprint.
- 4 Fare clic su **Modifica** e immettere nuovamente il nome del componente. Questa operazione consente di impostare il nome e l'ID incorporati sullo stesso valore.
- 5 Ripetere i passaggi per tutti i componenti del bilanciamento del carico nel blueprint.
- 6 Salvare il blueprint.

Quando si esegue il provisioning di una nuova distribuzione utilizzando il blueprint modificato, l'azione di riconfigurazione del bilanciamento del carico viene eseguita correttamente. Per evitare questo problema, prima di importare i file YAML verificare che abbiano tutti nome e ID identici per tutti i componenti di bilanciamento del carico, rete e sicurezza.

Non gestire oggetti NSX amministrati da vRealize Automation all'esterno di vRealize Automation. Ad esempio, se si modifica la porta membro di un bilanciamento del carico distribuito in NSX, anziché in vRealize Automation, la raccolta dei dati di NSX si interrompe. Anche le operazioni di scalabilità verticale e orizzontale generano risultati imprevisti.

Per informazioni sulle impostazioni disponibili quando si aggiunge o si modifica un server virtuale, vedere [Aggiunta di un componente bilanciamento del carico su richiesta](#).

Quando si riconfigura un bilanciamento del carico in vRealize Automation, viene ripristinato il valore predefinito di alcune impostazioni configurate in NSX che non sono disponibili come impostazioni in vRealize Automation. Dopo avere eseguito l'azione di riconfigurazione del bilanciamento del carico in vRealize Automation, verificare e aggiornare in modo appropriato le impostazioni seguenti in NSX:

- Intestazione HTTP Insert-X-Forwarded-For
- URL di reindirizzamento HTTP
- Estensione del monitoraggio servizi

Prerequisiti

- Accedere a vRealize Automation come **proprietario macchina, utente di supporto, utente del gruppo di business con ruolo accesso condiviso o manager del gruppo di business**.
- Verificare di disporre del permesso per riconfigurare i bilanciamenti del carico in una distribuzione. Il permesso di catalogo richiesto è Riconfigura (bilanciamento del carico).

Procedura

- 1 Fare clic su **Distribuzioni**.
- 2 Individuare la distribuzione che include il bilanciamento del carico da riconfigurare e fare clic sul nome della distribuzione.
- 3 Nella scheda **Componenti**, fare clic sul bilanciamento del carico e sull'icona a forma di ingranaggio delle azioni.

Viene visualizzato il menu delle azioni del componente.

- 4 Selezionare **Riconfigura**.
- 5 Aggiungere, modificare o rimuovere i server virtuali.

Virtual servers: + N... E... X Dele...

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 Fare clic su **Invia**.

Modifica di regole NAT in una distribuzione

È possibile aggiungere, modificare ed eliminare regole NAT NSX esistenti in una rete NAT distribuita di tipo uno a molti.

È anche possibile modificare l'ordine di elaborazione delle regole NAT.

Nota Se il blueprint di origine della distribuzione viene importato da un file YAML contenente un componente di rete NAT, e i valori di nome e ID del componente di rete NAT non sono identici, l'azione **Cambia regole NAT** non riesce. Per consentire l'azione **Cambia regole NAT** per una distribuzione basata su un blueprint importato, eseguire i passaggi seguenti nel blueprint prima del provisioning di una distribuzione.

- 1 Avviare vRealize Automation, fare clic sulla scheda Progettazione e aprire il blueprint.
- 2 Fare clic su **Modifica** e modificare il nome del blueprint. Questa operazione consente di impostare il nome e l'ID incorporati sullo stesso valore.
- 3 Selezionare il componente di rete NAT nel blueprint.
- 4 Fare clic su **Modifica** e immettere nuovamente il nome del componente. Questa operazione consente di impostare il nome e l'ID incorporati sullo stesso valore.
- 5 Ripetere questi passaggi per tutti i componenti di rete NAT nel blueprint.
- 6 Salvare il blueprint.

Per evitare questo problema, prima di importare i file YAML verificare che abbiano tutti nome e ID identici per tutti i blueprint e i componenti di bilanciamento del carico, rete e sicurezza.

Per informazioni correlate, vedere [Creazione e utilizzo di regole NAT per NSX for vSphere](#) e [Aggiunta di un componente di rete instradata o NAT su richiesta in vRealize Automation](#).

Prerequisiti

- Accedere a vRealize Automation come **proprietario macchina, utente di supporto, utente del gruppo di business con ruolo accesso condiviso** o **manager del gruppo di business**.
- Verificare di disporre del permesso di modificare le regole NAT in una rete.
- Verificare che la rete NAT sia configurata come una rete NAT di tipo uno a molti. L'azione non è disponibile per le reti NAT di tipo uno a uno.

NSX for vSphere supporta reti NAT One-to-One e NAT One-to-Many, ma NSX-T supporta solo reti NAT one-to-many.

Procedura

- 1 Fare clic su **Distribuzioni**.
- 2 Individuare la distribuzione che include il componente di rete che è necessario modificare e fare clic sul nome della distribuzione.

3 Nella scheda **Componenti**, fare clic su componente di rete NAT.

Per una rete NAT su richiesta associata a un provider IPAM di terze parti, non è possibile modificare il componente. È tuttavia possibile aggiungere manualmente un nuovo indirizzo IP di destinazione. Quando si aggiunge un nuovo indirizzo IP di destinazione, il valore del componente diventa null. Il nuovo indirizzo IP di destinazione e l'ID null della macchina vengono elaborati quando si invia la richiesta di riconfigurazione.

4 Fare clic sull'icona delle azioni a forma di ingranaggio.

Viene visualizzato il menu delle azioni del componente.

5 Fare clic su **Cambia regole NAT**.**6** Aggiungere nuove regole di inoltro della porta NAT, riordinare regole, modificare regole esistenti o eliminare regole.**7** Fare clic su **Invia**.**Visualizzazione di tutte le regole NAT per un NSX Edge esistente**

È possibile visualizzare informazioni sulle regole NAT relative agli NSX Edge utilizzati nelle distribuzioni attive.

Le regole NAT vengono mostrate nella vista Edge come aggregato di tutte le regole NAT utilizzate nella distribuzione. Nella vista Edge le regole non vengono necessariamente visualizzate nell'ordine di elaborazione.

Per visualizzare ed eventualmente modificare l'ordine di elaborazione delle regole NAT in una rete NAT One-to-Many, vedere [Modifica di regole NAT in una distribuzione](#).

Prerequisiti

- Accedere a vRealize Automation come **proprietario macchina, utente di supporto, utente del gruppo di business con ruolo accesso condiviso o manager del gruppo di business**.

Procedura**1** Fare clic su **Distribuzioni**.**2** Individuare la distribuzione che include l'edge NSX visualizzato e fare clic sul nome della distribuzione.**3** Nella scheda **Componenti**, individuare il componente edge NSX.**4** Selezionare il componente NSX Edge che si desidera visualizzare.**5** Al termine, fare clic su **Chiudi**.**Aggiunta o rimozione di elementi di sicurezza in una distribuzione**

È possibile aggiungere o rimuovere gruppi e tag di sicurezza NSX esistenti in una distribuzione macchina. Non è possibile aggiungere gruppi di sicurezza su richiesta ma è possibile rimuoverli.

L'azione di modifica della sicurezza si basa su un cluster o componente di macchina. Ad esempio, se la sicurezza è associata a un cluster denominato AppTier2 che consiste di 2 macchine, l'operazione di modifica della sicurezza viene eseguita sul cluster AppTier2 e non sulle macchine individuali all'interno del cluster.

L'operazione di modifica della sicurezza non viene supportata per le distribuzioni che hanno effettuato aggiornamenti o migrazioni da vRealize Automation 6.2.x a questa versione di vRealize Automation.

Prerequisiti

- Accedere a vRealize Automation come **proprietario macchina, utente di supporto, utente del gruppo di business con ruolo accesso condiviso o manager del gruppo di business**.
- Verificare di disporre del permesso di modificare la sicurezza in una distribuzione. Il permesso del catalogo richiesto è Modifica sicurezza (Distribuzione).

Procedura

- 1 Fare clic su **Distribuzioni**.
- 2 Individuare la distribuzione che include i tag e i gruppi di sicurezza e fare clic sul nome della distribuzione.
- 3 Nella scheda **Componenti**, fare clic sul componente di sicurezza e sull'icona a forma di ingranaggio delle azioni.
Viene visualizzato il menu delle azioni del componente.
- 4 Fare clic su **Modifica sicurezza**.
- 5 Selezionare il cluster o il componente della macchina distribuita in cui aggiungere o rimuovere elementi di sicurezza.
- 6 Aggiungere o rimuovere tag e gruppi di sicurezza esistenti per ciascun cluster o componente della macchina nella distribuzione come richiesto.
- 7 Rimuovere i gruppi di sicurezza su richiesta per ciascun cluster o componente della macchina nella distribuzione come richiesto.
- 8 (Facoltativo) Fare clic sulla scheda **Motivo** e immettere un motivo per la richiesta.
- 9 Fare clic su **Invia**.

Metodi di gestione aggiuntivi della distribuzione

Le risorse distribuite possono essere gestite utilizzando le azioni consentite, tuttavia esistono metodi aggiuntivi non inclusi come azioni.

Questi metodi non sono disponibili nella scheda Distribuzioni, ma vengono utilizzati per apportare modifiche a risorse sottoposte a provisioning.

Recupero delle risorse secondo le metriche di vRealize Operations Manager

Il recupero consente di utilizzare le risorse in modo efficiente. Se si utilizza anche vRealize Operations Manager per gestire le risorse nell'ambiente, è possibile configurare vRealize Automation per utilizzare le metriche per calcolare dove possibile recuperare risorse per la distribuzione.

Procedura

1 Configurazione di un provider di metriche

È possibile configurare vRealize Automation per utilizzare metriche di integrità e risorse di vRealize Operations Manager per macchine virtuali vSphere.

2 Invio delle richieste di recupero

È possibile visualizzare e gestire distribuzioni e inviare richieste di recupero ai proprietari delle distribuzioni. Una richiesta di recupero specifica una nuova lunghezza di lease espressa in giorni, la quantità di tempo dato per la risposta del proprietario di una distribuzione e quali sono le macchine destinazione del recupero.

3 Tenere traccia delle richieste di recupero

È possibile tenere traccia dello stato corrente delle richieste di recupero e altri dettagli.

Configurazione di un provider di metriche

È possibile configurare vRealize Automation per utilizzare metriche di integrità e risorse di vRealize Operations Manager per macchine virtuali vSphere.

Per ulteriori informazioni su metriche e badge di integrità di vRealize Operations Manager, vedere la documentazione di vRealize Operations Manager.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore tenant, manager del gruppo di business o proprietario della macchina**.

Recupero: gli utenti che creano richieste di recupero necessitano del ruolo di amministratore tenant e lo stesso account di amministratore tenant deve essere membro di almeno un gruppo di business nel tenant.

La mancata aggiunta dell'account di amministratore tenant a un gruppo di business causa un'eccezione di sistema all'apertura della scheda **Recupero > Distribuzioni**.

- Creare un account utente di vRealize Operations Manager con privilegi di visualizzazione ed esecuzione query per le metriche delle risorse per tutti i server vSphere integrati con vRealize Automation.
- Creare istanze di schede vRealize Operations Manager per tutti i server vSphere aggiunti come endpoint in vRealize Automation. Per informazioni sulla creazione di istanze di schede, vedere la documentazione di vRealize Operations Manager.

Procedura

- 1 Selezionare **Amministrazione > Recupero > Provider di metriche**.

2 Selezionare un provider di metriche.

Opzione	Descrizione
(Predefinito) Provider di metriche di vRealize Automation	Se non ha un'istanza di vRealize Operations Manager, vRealize Automation fornisce metriche di base sulla macchina.
Endpoint vRealize Operations Manager	Fornisce informazioni sulla connessione per l'istanza di vRealize Operations Manager che si desidera utilizzare come provider di metriche per le macchine virtuali vSphere.

3 Fare clic su **Prova connessione**.

4 Fare clic su **Salva**.

Risultati

Gli amministratori di tenant, i proprietari di macchine e i manager del gruppo di business nel quale risiede la macchina possono visualizzare i badge e gli avvisi di integrità nelle pagine dei dettagli degli elementi per le macchine virtuali di vSphere. Inoltre, possono visualizzare le metriche e i badge di integrità di vRealize Operations Manager filtrando per tipo di piattaforma vSphere nella pagina dei recuperi.

Operazioni successive

[Invio delle richieste di recupero.](#)

Invio delle richieste di recupero

È possibile visualizzare e gestire distribuzioni e inviare richieste di recupero ai proprietari delle distribuzioni. Una richiesta di recupero specifica una nuova lunghezza di lease espressa in giorni, la quantità di tempo dato per la risposta del proprietario di una distribuzione e quali sono le macchine destinazione del recupero.

Prerequisiti

- Accedere a vRealize Automation come **amministratore tenant**.
- (Facoltativo) Per consultare badge di integrità o visualizzare le metriche fornite da vRealize Operations Manager, vedere [Configurazione di un provider di metriche](#).

Procedura

1 Selezionare **Amministrazione > Recupero > Distribuzioni**.

2 Trovare le distribuzioni di macchine virtuali che corrispondono ai criteri di ricerca desiderati.

È necessario selezionare il tipo di piattaforma vSphere per visualizzare le metriche fornite da vRealize Operations Manager.

- a Fare clic sulla freccia giù della **Ricerca avanzata** per aprire la casella di ricerca.
- b Immettere o selezionare uno o più valori da cercare.

Opzione	Azione
Il nome della macchina virtuale contiene	Immettere uno o più caratteri nella casella di testo per trovare i nomi delle macchine virtuali corrispondenti.
Il nome del proprietario contiene	Immettere un nome nella casella di testo per trovare i nomi corrispondenti.
Il nome del gruppo di business contiene	Immettere un nome nella casella di testo per trovare i gruppi di business corrispondenti.
Tipo di piattaforma	Selezionare un tipo di piattaforma dal menu a discesa. Selezionare vSphere per visualizzare le metriche fornite da vRealize Operations Manager. Obbligatorio per vRealize Operations Manager.
Stato alimentazione	Selezionare un valore di stato di alimentazione dal menu a discesa per trovare le macchine virtuali aventi lo stato di alimentazione corrispondente.
Data di scadenza tra	Fare clic sulle icone del calendario e selezionare le date di inizio e fine per trovare le date di scadenza comprese nell'intervallo.
Utilizzo CPU	Selezionare un valore dal menu a discesa per trovare le macchine virtuali con Utilizzo della CPU alto (superiore all'80%), Utilizzo della CPU basso (inferiore al 5%) o Nessuno (nessun valore). Se si stanno interrogando le metriche di vRealize Operations Manager, non è possibile utilizzare questo filtro e non è possibile ordinare i risultati per utilizzo della CPU.
Utilizzo memoria	Selezionare un valore dal menu a discesa per trovare le macchine virtuali con Utilizzo della memoria alto (superiore all'80%), Utilizzo della memoria basso (inferiore al 10%) o Nessuno (nessun valore). Se si stanno effettuando query delle metriche di vRealize Operations Manager, non è possibile utilizzare questo filtro e non è possibile ordinare i risultati per utilizzo della memoria.
Utilizzo del disco	Selezionare un valore dal menu a discesa per trovare le macchine virtuali con Utilizzo del disco rigido basso (meno di 2 KB al secondo) o Nessuno (nessun valore). Se si stanno interrogando le metriche di vRealize Operations Manager, non è possibile utilizzare questo filtro e non è possibile ordinare i risultati per utilizzo del disco.
Utilizzo rete	Selezionare un valore dal menu a discesa per trovare le macchine virtuali con Utilizzo della rete basso (meno di 1 KB al secondo) o Nessuno (nessun valore).

Opzione	Azione
	Se si stanno interrogando le metriche di vRealize Operations Manager, non è possibile utilizzare questo filtro e non è possibile ordinare i risultati per utilizzo della rete.
Metrica complessa	<p>Selezionare un valore dal menu a discesa per trovare le macchine virtuali in base a metriche complesse. Ad esempio, selezionare Inattivo per trovare le macchine che hanno valori di utilizzo di CPU, rete, memoria e disco tutti inferiori al 20%.</p> <p>Non è possibile utilizzare questo filtro se si stanno interrogando metriche di vRealize Operations Manager.</p>

c Fare clic sull'icona di ricerca (.

- 3 Dalla pagina Distribuzioni, selezionare una o più macchine di cui è necessario recuperare la distribuzione principale.

Vengono recuperate esclusivamente le macchine selezionate visibili nella pagina dei risultati corrente.

- 4 Fare clic su **Recupera**

Le distribuzioni che contengono macchine virtuali selezionate nella pagina corrente sono incluse nella richiesta.

Nota La pagina Distribuzione di recupero può elencare le macchine non disponibili per il recupero, come ad esempio quelle per le quali è scaduto il lease. Se si specifica una macchina che non è disponibile per il recupero, viene visualizzato il seguente errore:

```
Selection Error: Virtual machine name is not in valid state for reclamation.
```

- 5 Immettere la durata del nuovo lease nella casella di testo **Durata nuovo lease (giorni)**.

Il minimo è 1 giorno, il massimo è 365 giorni, il valore predefinito è 7 giorni.

- 6 Nella casella di testo **Attesa prima di forzare il lease (giorni)**, specificare quanti giorni ha il proprietario della distribuzione per rispondere alla richiesta di recupero.

Alla termine di questo periodo di tempo, la distribuzione otterrà un nuovo lease con la nuova lunghezza di lease. Il periodo di attesa minimo è 1 giorno, il massimo è 365 giorni, il valore predefinito è 3 giorni.

- 7 Immettere un motivo per la richiesta nella casella di testo **Motivo della richiesta**.

- 8 Fare clic su **Invia**.

- 9 Fare clic su **OK**.

Risultati

Quando si invia una richiesta di recupero, questa verrà visualizzata nella Posta in arrivo del proprietario della distribuzione. Se il proprietario non risponde alla richiesta entro il numero di giorni richiesto, la distribuzione ottiene un nuovo lease della lunghezza specificata, a meno che il suo lease corrente non sia più breve. Se il proprietario fa clic su **Elemento in uso** alla richiesta di recupero, il lease della distribuzione resta immutato. Se il proprietario fa clic su **Rilascio per recupero**, il lease della distribuzione scade immediatamente.

Operazioni successive

[Tenere traccia delle richieste di recupero.](#)

Tenere traccia delle richieste di recupero

È possibile tenere traccia dello stato corrente delle richieste di recupero e altri dettagli.

I seguenti metodi alternativi sono disponibili per la verifica di una richiesta di recupero recente:

- Fare clic sulla scheda **Posta in arrivo** e selezionare **Richieste di recupero** per visualizzare le informazioni sulle richieste di recupero.
- Fare clic sulla scheda **Richieste di recupero** e visualizzare l'elenco di richieste recenti
- Fare clic su **Distribuzioni** per visualizzare le modifiche recenti alla distribuzione.


Prerequisiti

Accedere a vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Recupero > Richieste di recupero**.
- 2 Trovare le macchine virtuali che corrispondono ai criteri di ricerca desiderati.
 - a Fare clic sulla freccia giù della **Ricerca avanzata** per aprire la casella di ricerca.
 - b Digitare o selezionare uno o più valori da cercare.

Opzione	Azione
Il nome della macchina virtuale contiene	Immettere uno o più caratteri nella casella di testo per trovare i nomi delle macchine virtuali corrispondenti.
Il nome del proprietario contiene	Immettere uno o più caratteri nella casella di testo per trovare i nomi dei proprietari corrispondenti.
Il motivo della richiesta contiene	Immettere uno o più caratteri nella casella di testo per trovare il motivo della richiesta corrispondente.
Stato della richiesta	Selezionare un valore di stato della richiesta dal menu a discesa per trovare le macchine virtuali aventi uno stato di richiesta corrispondente.

- c Fare clic sull'icona **Cerca**  o premere Invio per avviare la ricerca.
- d Fare clic sulla freccia su della **Ricerca avanzata** per chiudere la casella di ricerca.

- 3 (Facoltativo) Fare clic su **Aggiorna dati** per aggiornare la visualizzazione delle richieste di recupero.

Cambiamento della prenotazione di una macchina gestita

È possibile modificare le impostazioni di prenotazione o storage per una macchina gestita. Questo è utile ad esempio se si deve spostare una macchina in un nuovo percorso di storage non disponibile nella prenotazione corrente. Per la distribuzione di una singola macchina, è anche possibile modificare il gruppo di business della macchina.

È possibile spostare una macchina di una distribuzione di una singola macchina in un gruppo di business diverso se il proprietario della macchina è un membro del gruppo di business di destinazione. Per poter modificare le impostazioni del gruppo di business, è necessario essere manager del gruppo di business originale e di quello di destinazione.

Nota Se alla macchina è stato assegnato un criterio di prenotazione, non è possibile modificarne il gruppo di business.

È possibile creare prenotazioni aggiuntive per la risorsa di elaborazione associata utilizzando le opzioni del menu **Amministrazione > Risorsa di elaborazione**.

Lo storage e la memoria assegnati a una macchina sottoposta a provisioning da una prenotazione vengono rilasciati quando la macchina a cui sono assegnati viene eliminata in vRealize Automation dall'azione di eliminazione. La memoria e lo storage non vengono rilasciati se la macchina viene eliminata in vCenter Server.

Ad esempio, non è possibile eliminare una prenotazione associata alle macchine in una distribuzione esistente. Se si spostano o si eliminano manualmente macchine distribuite in vCenter Server, vRealize Automation continua a riconoscere le macchine distribuite come funzionanti e impedisce l'eliminazione delle prenotazioni associate.

Se la modifica della prenotazione comporta lo spostamento di una macchina in vCenter Server in un nuovo percorso di storage che non fa parte della prenotazione di tale macchina in vRealize Automation, verificare che la destinazione o il nuovo percorso di storage siano selezionati nella prenotazione target della macchina prima di modificare la prenotazione della macchina.

Prerequisiti

Accedere a vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Macchine gestite**.
- 2 Individuare la macchina di cui si intende cambiare la prenotazione.
- 3 Fare clic su **Cambia prenotazione** nel menu a discesa.

È possibile visualizzare informazioni sulla macchina gestita, ad esempio la risorsa di elaborazione e il blueprint associati, facendo clic su **Visualizza** nel menu a discesa.

- 4 (Facoltativo) Selezionare un gruppo di business dal menu a discesa **Gruppo di business**.

- 5 (Facoltativo) Selezionare una prenotazione dal menu a discesa **Prenotazione**.
- 6 (Facoltativo) Selezionare un criterio di storage dal menu a discesa **Storage**.
- 7 Fare clic su **OK**.

Utilizzo della posta in arrivo

La posta in arrivo fornisce notifiche nel prodotto riguardanti le approvazioni delle richieste di catalogo, le interazioni richieste durante il processo di provisioning e lo stato delle richieste di recupero basate su qualsiasi metrica di vRealize Operations Manager.

È possibile esaminare ciascuna scheda per vedere se sono presenti notifiche in sospeso che richiedono un'azione.

- **Approvazioni.** È possibile tenere traccia delle richieste del catalogo che richiedono l'approvazione. Se l'utente è stato designato come approvatore di una richiesta di catalogo, è possibile rispondere a una richiesta di approvazione. Vedere [Aggiunta di informazioni sui livelli alle impostazioni dei criteri di approvazione](#).
- **Azione utente manuale.** Alcune richieste di catalogo richiedono l'interazione durante il processo di provisioning. È possibile rispondere alla richiesta di interazione. Vedere [Integrazione di vRealize Orchestrator in vRealize Automation](#).
- **Richieste di recupero.** Se si utilizza vRealize Operations Manager per determinare dove è possibile recuperare risorse, è possibile tenere traccia delle richieste di recupero. Vedere [Tenere traccia delle richieste di recupero](#).