

Configurazione di vRealize Automation

vRealize Automation 7.1



vmware®

È possibile consultare la documentazione tecnica più aggiornata sul sito Web all'indirizzo:

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

Inoltrare eventuali commenti sulla documentazione al seguente indirizzo:

docfeedback@vmware.com

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

VMware, Inc.
P.le Biancamano 8
20121 Milano
tel: 02-6203.2075
fax: 02-6203.4000
www.vmware.com/it

Copyright © 2015, 2016 VMware Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi.](#)

Contenuti

Configurazione di vRealize Automation 7

Informazioni aggiornate 8

1 Preparazioni esterne per il provisioning 9

Preparazione dell'ambiente per la gestione di vRealize Automation 9

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

Elenco di controllo per la preparazione del supporto di provider IPAM esterni 13

Preparazione dell'ambiente di vCloud Director per vRealize Automation 16

Preparazione dell'ambiente di vCloud Air per vRealize Automation 16

Preparazione dell'ambiente di Amazon AWS 17

Preparazione delle funzionalità di rete e sicurezza di Red Hat OpenStack 23

Preparazione dell'ambiente di SCVMM 23

Preparazione per il provisioning delle macchine 24

Scelta del metodo di provisioning delle macchine da preparare 24

Elenco di controllo per l'esecuzione di script Visual Basic durante il provisioning 28

Utilizzo dell'agente guest di vRealize Automation nel provisioning 29

Elenco di controllo per la preparazione al provisioning tramite clonazione 37

Preparazione per il provisioning di vCloud Air e vCloud Director 52

Preparazione per il provisioning Linux Kickstart 54

Preparazione per il provisioning SCCM 56

Preparazione per il provisioning di WIM 58

Preparazione per il provisioning dell'immagine delle macchine virtuali 68

Preparazione per il provisioning dell'immagine della macchina Amazon 69

Scenario: preparazione di risorse vSphere per il provisioning di macchine in Rainpole 72

Preparazione per il provisioning Software 74

Preparazione per il provisioning delle macchine con Software 75

Scenario: preparazione di un modello CentOS di vSphere per clonare blueprint di componenti software e macchine 81

Scenario: preparazione per l'importazione di Dukes Bank per il blueprint dell'applicazione campione di vSphere 85

2 Configurazione delle impostazioni del tenant 91

Scelta delle opzioni di configurazione di Gestione directory 92

Panoramica di Gestione directory 93

Utilizzo di Gestione directory per creare un collegamento ad Active Directory 97

Gestione degli attributi utente sincronizzati da Active Directory 110

Gestione dei connettori 112

Unione della macchina con un connettore a un dominio	112
Informazioni sulla selezione dei controller di dominio	113
Gestione dei criteri di accesso	117
Integrazione di prodotti di autenticazione dell'utente alternativi con Gestione directory	123
Scenario: configurazione di un collegamento Active Directory per un vRealize Automation ad alta disponibilità	145
Configurazione dell'autenticazione smart card per vRealize Automation	147
Generazione di un token di attivazione del connettore	148
Distribuzione del file OVA per il connettore	149
Configurazione delle impostazioni del connettore	150
Applicazione di autorità di certificati pubblici	151
Creazione di un provider di identità per l'area di lavoro	153
Configurazione dell'autenticazione dei certificati e delle regole predefinite dei criteri di accesso	154
Creazione di un link di Active Directory multidominio o a più foreste	154
Configurazione dei ruoli di utenti e gruppi	157
Assegnazione di ruoli a utenti e gruppi della directory	157
Creazione di un gruppo personalizzato	157
Creazione di un gruppo di business	158
Risoluzione dei problemi relativi alle prestazioni durante la visualizzazione dei membri di un gruppo	161
Scenario: configurazione del tenant predefinito per Rainpole	162
Scenario: creazione degli account utente locali per Rainpole	163
Scenario: connessione di Active Directory aziendale a vRealize Automation per Rainpole	164
Scenario: configurazione del branding per il tenant predefinito per Rainpole	166
Scenario: creazione di un gruppo personalizzato per gli architetti Rainpole	166
Scenario: assegnazione di privilegi di amministratore IaaS al gruppo personalizzato di architetti Rainpole	167
Creazione di tenant aggiuntivi	168
Definizione delle informazioni sui tenant	169
Configurazione di utenti locali	169
Nomina degli amministratori	170
Eliminazione di un tenant	171
Configurazione del branding personalizzato	171
Branding personalizzato per la pagina di accesso del tenant	171
Branding personalizzato per le applicazioni del tenant	172
Elenco di controllo per la configurazione delle notifiche	173
Configurazione di server email globali per le notifiche	176
Aggiunta di un server email in uscita specifico di un tenant	178
Aggiunta di un server email in entrata specifico di un tenant	179
Priorità inferiore del server di email in uscita predefinito di un sistema	180
Priorità inferiore del server di email in entrata predefinito di un sistema	181
Ripristino dei server email predefiniti del sistema	182

Configurazione delle notifiche	183
Personalizzazione della data per la notifica via email della scadenza di una macchina	183
Configurazione dei modelli per le email automatiche di IaaS	184
Iscrizione alle notifiche	184
Creazione di un file RDP personalizzato per il supporto di connessioni RDP per le macchine di cui è stato eseguito il provisioning	184
Scenario: aggiunta di posizioni di data center per distribuzioni tra più regioni	185
Configurazione di vRealize Orchestrator e dei plug-in	186
Configurazione della cartella di workflow predefinita per un tenant	187
Configurazione di un server vRealize Orchestrator esterno	187
Accesso all'interfaccia di configurazione di vRealize Orchestrator	189
Accesso al client di vRealize Orchestrator	189
3 Configurazione delle risorse	191
Elenco di controllo per la configurazione di risorse di IaaS	191
Archiviazione delle credenziali utente	192
Scelta dello scenario per un endpoint	194
Creazione di un gruppo di strutture	214
Configurazione dei prefissi macchina	214
Gestione delle coppie di chiavi	215
Creazione di un profilo di rete	217
Configurazione di prenotazione e criteri di prenotazione	234
Scenario: configurazione di risorse IaaS per Rainpole	274
Scenario: applicazione di una posizione a una risorsa di elaborazione per distribuzioni tra più regioni	278
Elenco di controllo per il provisioning di una distribuzione di vRealize Automation mediante un provider IPAM esterno	279
Configurazione delle risorse XaaS	280
Configurazione del plug-in di Active Directory come endpoint	280
Configurazione del plug-in HTTP-REST come endpoint	282
Configurazione del plug-in PowerShell come endpoint	284
Configurazione del plug-in SOAP come endpoint	285
Configurazione del plug-in di vCenter Server come endpoint	287
Installazione di plug-in aggiuntivi sul server vRealize Orchestrator predefinito	288
Utilizzo dei criteri di Active Directory	289
Creazione e applicazione di criteri di Active Directory	290
4 Fornitura di servizi su richiesta agli utenti	294
Progettazione dei blueprint	294
Esportazione e importazione dei blueprint	296
Scenario: importazione di Dukes Bank per l'applicazione campione di vSphere e configurazione dell'ambiente	297

Scenario: test dell'applicazione campione Dukes Bank	301
Creazione di una libreria di progettazione	303
Progettazione dei blueprint delle macchine	305
Progettazione di blueprint di macchine con rete e sicurezza di NSX	348
Progettazioni di componenti Software	364
Creazione di blueprint e azioni risorsa di XaaS	385
Pubblicazione di un blueprint	436
Assemblaggio di blueprint compositi	437
Informazioni sul comportamento dei blueprint nidificati	439
Selezione di un componente della macchina che supporta i componenti di Software	441
Creazione di binding di proprietà tra componenti di blueprint	442
Creazione di dipendenze esplicite e controllo dell'ordine di provisioning	443
Scenario: assemblaggio e test di un blueprint per la fornitura di macchine di cloni collegati MySQL su Rainpole	444
Gestione del catalogo dei servizi	447
Elenco di controllo per la configurazione del catalogo dei servizi	448
Creazione di un servizio	449
Funzionamento di elementi del catalogo e azioni	452
Creazione di permessi	455
Utilizzo dei criteri di approvazione	463
Scenario: configurazione del catalogo per consentire agli architetti di Rainpole di testare i blueprint	485
Scenario: test della macchina CentOS di Rainpole	488
Scenario: rendere il blueprint dell'applicazione CentOS con MySQL disponibile nel catalogo dei servizi	489
Scenario: creazione e applicazione di criteri di approvazione di CentOS con MySQL	493

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.

Per informazioni sulle integrazioni supportate, vedere <https://www.vmware.com/pdf/vrealize-automation-71-support-matrix.pdf>.

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.

Glossario delle pubblicazioni tecniche di VMware

Il sito delle pubblicazioni tecniche di VMware Technical fornisce un glossario dei termini che potrebbero risultare non familiari. Per le definizioni dei termini utilizzati nella documentazione tecnica di VMware, consultare la pagina <http://www.vmware.com/support/pubs>.

Informazioni aggiornate

Configurazione di vRealize Automation viene aggiornato a ogni release del prodotto oppure quando necessario.

Nella tabella viene riportata la cronologia degli aggiornamenti di *Configurazione di vRealize Automation*.

Revisione	Descrizione
IT-002076-04	<ul style="list-style-type: none">■ Aggiornamento di Installazione dell'agente guest su una macchina di riferimento Windows.■ Aggiornamento di Preparazione di una macchina di riferimento Windows per il supporto di Software.■ Aggiornamento di Preparazione di una macchina di riferimento Linux per il supporto di Software.■ Aggiornamento di Creazione di un criterio di Active Directory.
IT-002076-03	Aggiunta una nota a Definizione delle informazioni sui tenant per indicare che è necessario utilizzare solo caratteri minuscoli per gli URL dei tenant.
IT-002076-02	<ul style="list-style-type: none">■ Aggiornamento di Preparazione per il provisioning di vCloud Air e vCloud Director.■ Aggiornamento di Creazione di un endpoint vCloud Director.■ Aggiornamento di Esportazione e importazione dei blueprint.■ Aggiornamento di Impostazioni dei componenti macchina di vSphere.
IT-002076-01	<ul style="list-style-type: none">■ Aggiunta di Eliminazione di un tenant.■ Aggiornamento di Impostazioni dei componenti macchina Amazon.■ Aggiornamento di Risoluzione dei problemi dei blueprint per cloni e cloni collegati.
IT-002076-00	Release 7.1 iniziale.

Preparazioni esterne per il provisioning

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](#)
- [Preparazione per il provisioning delle macchine](#)
- [Preparazione per il provisioning Software](#)

Preparazione dell'ambiente per la gestione di vRealize Automation

A seconda della piattaforma di integrazione in uso, 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.

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






Ambiente	Preparazioni
 NSX	Se si desidera sfruttare NSX per gestire le funzionalità di networking e sicurezza delle macchine fornite in provisioning con vRealize Automation, preparare la propria istanza di NSX per l'integrazione. Vedere Elenco di controllo per la preparazione della configurazione di rete e sicurezza di NSX .
 vCloud Director	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 .

Tavola 1-1. Preparazione dell'ambiente per l'integrazione di vRealize Automation (Continua)

Ambiente	Preparazioni
 vCloud Air	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 .
 Amazon AWS	Preparare gli elementi e i ruoli utente nell'ambiente Amazon AWS per l'uso in vRealize Automation e analizzare le corrispondenze delle funzionalità di Amazon AWS con le funzionalità di vRealize Automation. Vedere Preparazione dell'ambiente di Amazon AWS .
 Red Hat OpenStack	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 .
 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 la preparazione del supporto di provider IPAM esterni .
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 esterno che si intende utilizzare.

Una parte significativa del supporto di vRealize Automation per la configurazione di rete e sicurezza specificata nei blueprint e nelle prenotazioni è configurata esternamente e resa disponibile a vRealize Automation dopo l'esecuzione della raccolta dati sulle risorse di elaborazione.

Per ulteriori informazioni sulle opzioni di configurazione di rete e sicurezza che è possibile configurare per vRealize Automation, vedere [Configurazione delle impostazioni dei componenti rete e sicurezza](#).

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

Attività	Posizione	Dettagli
<input type="checkbox"/> Installare e configurare il plug-in NSX .	Installare il plug-in NSX in vRealize Orchestrator.	Vedere Installazione del plug-in NSX su vRealize Orchestrator e la <i>guida di amministrazione di NSX</i> .
<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 in NSX.	Vedere la <i>guida di amministrazione di NSX</i> .
<input type="checkbox"/> Creare i tag, i gruppi e i criteri di sicurezza di NSX.	Configurare le impostazioni di sicurezza in NSX.	Vedere la <i>guida di amministrazione di NSX</i> .
<input type="checkbox"/> Configurare le impostazioni di bilanciamento del carico di NSX.	Configurare un bilanciamento del carico di NSX che funzioni con vRealize Automation.	Vedere la <i>guida di amministrazione di NSX</i> . Vedere anche Proprietà personalizzate per il networking in <i>Guida di riferimento alle proprietà personalizzate</i> .

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.

Nota: Se si utilizza un vRealize Orchestrator incorporato in cui è installato un plug-in di NSX, non è necessario eseguire questi passaggi di installazione del plug-in perché il plug-in di NSX è già installato.

Per informazioni generali su aggiornamento dei plug-in e risoluzione dei problemi, consultare la documentazione di vRealize Orchestrator all'indirizzo

https://www.vmware.com/support/pubs/orchestrator_pubs.html.

Prerequisiti

- Assicurarsi di eseguire un'istanza di vRealize Orchestrator supportata.

Per informazioni sulla configurazione di vRealize Orchestrator, vedere *Installazione e configurazione di VMware 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.
- Verificare di aver installato la versione corretta del plug-in di NSX. Vedere *Matrice di supporto di vRealize Automation*.
- Assicurarsi di avere installato il client vRealize Orchestrator e che sia possibile accedere con credenziali dell'amministratore.

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 d'installazione dei plug-in per il prodotto di rete e sicurezza NSX sono disponibili dal sito di download del prodotto VMware all'indirizzo <http://vmware.com/web/vmware/downloads>.
- 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.

Vedere *Matrice di supporto di vRealize Automation* per informazioni sulla versione.

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.

Passi successivi

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

Esecuzione di un workflow di sicurezza di vRealize Orchestrator e NSX

Prima di utilizzare le funzionalità dei criteri di protezione di NSX da vRealize Automation, è necessario che un amministratore esegua il workflow `Enable security policy support for overlapping subnets` in vRealize Orchestrator.

Il supporto del criterio di protezione per i workflow di subnet sovrapposte è applicabile a endpoint NSX 6.1 e versioni successive. Eseguire questo workflow una sola volta per abilitare questo supporto.

Prerequisiti

- Verificare che un endpoint vSphere sia registrato con un endpoint NSX. Vedere [Creazione di un endpoint vSphere](#).
- Accedere al client vRealize Orchestrator come amministratore.
- Verificare di avere eseguito il workflow `vRO Create NSX endpoint`.

Procedura

- 1 Fare clic sulla scheda **Workflow** e selezionare **NSX > NSX workflow per VCAC**.
- 2 Eseguire il workflow **Crea endpoint NSX** e rispondere alle richieste.
- 3 Eseguire il workflow **Abilita supporto criterio di protezione per subnet sovrapposte**.
- 4 Selezionare l'endpoint NSX come parametro di input per il workflow.

Utilizzare l'indirizzo IP specificato quando è stato creato l'endpoint di vSphere per registrare un'istanza di NSX.

Dopo aver eseguito questo workflow, le regole firewall distribuite definite nel criterio di protezione vengono applicate solo sulle vNIC dei membri del gruppo di sicurezza a cui è applicato il criterio di protezione.

Passi successivi

Applicare le funzionalità di sicurezza pertinenti per il blueprint.

Elenco di controllo per la preparazione del supporto di provider IPAM esterni

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

Prima di poter utilizzare un endpoint di provider IPAM esterni in un profilo di rete di vRealize Automation, è necessario scaricare oppure ottenere in altro modo un pacchetto di provider IPAM di vRealize Orchestrator, importarlo ed eseguire i workflow richiesti in vRealize Orchestrator, quindi registrare la soluzione IPAM come endpoint di vRealize Automation in vRealize Orchestrator.

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 [Elenco di controllo per il provisioning di una distribuzione di vRealize Automation mediante un provider IPAM esterno](#).

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

Attività	Posizione	Dettagli
<input type="checkbox"/> Ottenere e importare il plug-in di vRealize Orchestrator del provider IPAM esterno.	Scaricare il pacchetto del provider IPAM, ad esempio l'IPAM di Infoblox, da VMware Solution Exchange e importarlo in vRealize Orchestrator. Se VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_group/s/cloud-management) non contiene il pacchetto del provider IPAM necessario, è possibile creare il proprio utilizzando l'SDK del provider di soluzioni IPAM e la documentazione di supporto.	Vedere Ottenere e importare il pacchetto di provider IPAM esterni in vRealize Orchestrator .
<input type="checkbox"/> Eseguire i workflow di configurazione richiesti e registrare la soluzione IPAM esterna come endpoint di vRealize Automation.	Eseguire il workflow di configurazione di vRealize Orchestrator e registrare il tipo di endpoint del provider IPAM in vRealize Orchestrator.	Vedere Eseguire il workflow per registrare il tipo di endpoint IPAM di Infoblox in vRealize Orchestrator .

Ottenere e importare il pacchetto di provider IPAM esterni in vRealize Orchestrator

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

È possibile scaricare e utilizzare un pacchetto di provider di gestione degli indirizzi IP di terze parti esistente, quale l'IPAM di Infoblox. È anche possibile creare pacchetti propri utilizzando un SDK fornito da VMware e la relativa documentazione, ad esempio per creare un pacchetto da utilizzare con l'IPAM di Bluecat. In questo esempio viene utilizzato il pacchetto IPAM di Infoblox.

Dopo aver ottenuto e importato il pacchetto di provider IPAM esterni in vRealize Orchestrator, eseguire i workflow richiesti e registrare il tipo di endpoint IPAM.

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

Prerequisiti

- Accedere a vRealize Orchestrator con i privilegi di amministratore per importare, configurare e registrare un pacchetto di vRealize Orchestrator.

Procedura

- 1 Accedere al sito VMware Solution Exchange all'indirizzo https://solutionexchange.vmware.com/store/category_groups/cloud-management.

- 2 Selezionare **Cloud Management Marketplace**.
- 3 Individuare e scaricare il plug-in o il pacchetto, ad esempio Infoblox VIPAM Plug-in.
- 4 In vRealize Orchestrator, fare clic sulla scheda **Amministratore** e fare clic su **Importa pacchetto**.
- 5 Selezionare il pacchetto o il plug-in, ad esempio il plug-in Infoblox IPAM.
- 6 Selezionare tutti i workflow e gli artefatti e fare clic sul pulsante per **importare gli elementi selezionati**.

Passi successivi

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

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

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

Per registrare i tipi di endpoint IPAM in vRealize Orchestrator, viene chiesto di fornire le credenziali dell'amministratore vRA di vRealize Automation. T

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

Prerequisiti

- [Ottenere e importare il pacchetto di provider IPAM esterni in vRealize Orchestrator](#)
- Verificare di aver effettuato l'accesso a vRealize Orchestrator con vRealize Automation con l'autorità per eseguire workflow.
- Quando richiesto, fornire le credenziali dell'amministratore IaaS 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. I nomi dei workflow potrebbero essere simili tra provider di pacchetti. La posizione dei workflow in vRealize Orchestrator può variare ed è specifica in base ai singoli provider.
- 2 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 dell'amministratore IaaS di vRealize Automation.

Il pacchetto registra InfoBlox come nuovo tipo di endpoint IPAM nel servizio endpoint di vRealize Automation e lo rende disponibile durante la definizione degli endpoint in vRealize Automation.

Passi successivi

Ora è possibile creare un endpoint di tipo InfoBlox IPAM in vRealize Automation. Vedere [Creazione di un endpoint del provider IPAM esterno](#).

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 AWS

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

Ruoli utente di Amazon AWS 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.

È necessario disporre di specifici diritti di accesso di Amazon per poter eseguire correttamente il provisioning di macchine utilizzando vRealize Automation.

■ Ruoli e autorizzazioni in Amazon Web Service

Il ruolo di Power User in AWS concede a un utente o gruppo di AWS Directory Service l'accesso completo ai servizi e alle risorse di AWS.

Non è necessaria alcuna credenziale di AWS per creare un endpoint AWS in vRealize Automation.

Tuttavia, vRealize Automation presume che l'utente di AWS che crea un'immagine di una macchina di Amazon abbia il ruolo di Power User.

■ Credenziali di autenticazione in Amazon Web Services

Il ruolo Power User di AWS non consente di gestire utenti e gruppi di AWS Identity and Access Management (IAM). Per poter gestire utenti e gruppi di IAM occorre essere configurati con le credenziali di accesso completo amministratore di AWS.

vRealize Automation richiede le chiavi di accesso per le credenziali degli endpoint e non supporta nomi utente e password. Per ottenere la chiave di accesso necessaria per creare l'endpoint Amazon, il Power User deve richiedere una chiave da un utente che dispone di credenziali di accesso completo amministratore di AWS oppure essere configurato ulteriormente con il criterio Accesso completo amministratore di AWS.

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 AWS 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 AWS (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 AWS 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 Amazon AWS VPC, consultare la documentazione di Amazon AWS.

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, disabilitare 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](#).
- 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.

Scenario: configurazione di connettività VPC da rete ad Amazon per un ambiente di prototipazione

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

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

- Installare e configurare completamente vRealize Automation. Vedere *Installazione e configurazione di vRealize Automation per lo scenario Rainpole*.
- Creare un gruppo di sicurezza Amazon AWS chiamato TunnelGroup e configurarlo per consentire l'accesso alla porta 22.
- Creare o identificare una macchina CentOS nel gruppo di sicurezza TunnelGroup di Amazon AWS 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 AWS come utente root o simile.
- 2 Disabilitare 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 AWS.

```
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 \
Utente della macchina tunnel Amazon@Indirizzo IP pubblico della macchina tunnel Amazon
```

Si è configurato l'inoltro della porta per consentire alla macchina tunnel Amazon AWS 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.

Passi successivi

- 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.

È possibile specificare i gruppi di sicurezza quando si crea una prenotazione e nella tela del blueprint. È possibile specificare i gruppi di sicurezza anche quando si richiede una macchina.

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.

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, le parole seguenti vengono ignorate 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.

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.

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.

Tavola 1-4. 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 AWS.	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 AWS.	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 AWS 	<ul style="list-style-type: none"> ■ (Obbligatorio) Agente guest ■ (Obbligatorio) Agente di avvio automatico software e agente guest 	<ul style="list-style-type: none"> ■ Clone ■ 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 .
Dopo il provisioning, è possibile utilizzare l'agente guest per personalizzare ulteriormente le macchine.	Tutti gli endpoint virtuali e Amazon AWS.	<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. Per ulteriori informazioni sull'agente guest, vedere Utilizzo dell'agente guest di vRealize Automation nel provisioning .
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.

Tavola 1-4. Scelta del metodo di provisioning delle macchine da preparare (Continua)

Scenario	Endpoint supportato	Supporto di agenti	Metodo di provisioning	Preparazioni pre-provisioning
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>
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	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 	Clone	<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>
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

Tavola 1-4. Scelta del metodo di provisioning delle macchine da preparare (Continua)

Scenario	Endpoint supportato	Supporto di agenti	Metodo di provisioning	Preparazioni pre-provisioning
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. È possibile utilizzare PEBuilder per creare un'immagine WinPE che includa l'agente guest. L'immagine WinPE può essere creata anche con un altro metodo, ma in quel caso sarà necessario inserire manualmente l'agente guest.	WIM	Preparazione per il provisioning di WIM
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 AWS	<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 AWS.</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 AWS 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.

Tavola 1-5. 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 7.1</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>%System Drive%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.

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.

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.

Tavola 1-6. Proprietà personalizzate per cambiare l'indirizzo IP di una macchina fornita in provisioning con un agente guest

Proprietà personalizzata	Descrizione
<code>VirtualMachine.Admin.UseGuestAgent</code>	Impostare su true per inizializzare l'agente guest quando la macchina fornita in provisioning viene avviata.
<code>VirtualMachine.Customize.WaitComplete</code>	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.

Tavola 1-6. 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 <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.</p> <p>Immettere <i>{Owner}</i> 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 <i>{YourCustomProperty}</i> nella stringa del percorso. Ad esempio, l'immissione del valore <i>\\vra-scripts.mycompany.com\scripts\changeIP.bat</i> esegue lo script <i>changeIP.bat</i> da una posizione condivisa, tuttavia l'immissione del valore <i>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</i> esegue lo script <i>changeIP</i>, ma passa anche il valore della proprietà <i>VirtualMachine.Network0.Address</i> 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 <i>VirtualMachine.SoftwareN.ScriptPath</i> formattata in precedenza alla riga di comando <i>gugent</i>.</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 <i>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat password</i> non è sicura in quanto contiene effettivamente una password.</p>

Tavola 1-6. 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 <code>[MyPassword]</code> 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*.

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.

Procedura

- 1 Aprire la pagina d'installazione della console di gestione di vCloud Automation Center Appliance.
Ad esempio `https://vcac-hostname.domain.name:5480/installer/`.
- 2 Scaricare e salvare i pacchetti degli agenti guest di Linux.
- 3 Decomprimere il file `LinuxGuestAgentPkgs`.

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

- a Passare alla sottodirectory `LinuxGuestAgentPkgs` relativa al sistema operativo guest.
- 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 gugent-7.0.0-012715.x86_64.rpm`.

- 5 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>

- 6 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	In qualità di utente root sulla macchina di riferimento, eseguire il comando seguente: <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	In qualità di utente root sulla macchina di riferimento, eseguire il comando seguente: <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 7 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>

Passi successivi

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 su una macchina di riferimento Windows da eseguire come servizio Windows e per attivare l'ulteriore personalizzazione delle macchine.

Prerequisiti

- Identificare o creare la macchina di riferimento.

- Se si desidera adottare l'approccio più sicuro per stabilire attendibilità fra l'agente guest e la macchina del servizio di gestione, ottenere il certificato SSL in formato PEM dalla macchina del servizio di gestione. Per ulteriori informazioni su come l'agente guest stabilisce l'attendibilità, consultare [Configurazione di un agente guest Windows in modo che consideri attendibile un server](#).

Procedura

- 1 Aprire la pagina d'installazione della console di gestione di vCloud Automation Center Appliance.
Ad esempio `https://vcac-hostname.domain.name:5480/installer/`.
- 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 Scaricare e salvare il file di installazione dell'agente guest di Windows sull'unità C della macchina di riferimento.
 - File agente guest Windows (**32 bit**).
 - File agente guest Windows (**64 bit**).
- 4 Installare l'agente guest sulla macchina di riferimento.
 - a Fare clic con il pulsante destro del mouse sul file e scegliere **Proprietà**.
 - b Fare clic su **Generale**.
 - c Fare clic su **Sblocca**.
 - d Estrarre i file.

Verrà creata la directory `C:\VRMGuestAgent`. Non cambiare il nome di questa directory.
- 5 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 Configurare l'agente guest per cui rendere attendibile la macchina del servizio di gestione.

Opzione	Descrizione
Consente all'agente guest di considerare attendibile la prima macchina alla quale si collega.	Nessuna configurazione richiesta.
Installare manualmente il file PEM attendibile.	Inserire il file PEM del servizio di gestione nella directory C:\VRMGuestAgent\.

- d Eseguire `win service -i -h Manager_Service_Hostname_fdn: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>

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

Passi successivi

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.

Configurazione di un agente guest Windows in modo che consideri attendibile un server

L'approccio più sicuro consiste nell'installare manualmente il file PEM attendibile su ciascun modello che utilizza l'agente guest, ma è possibile anche configurare l'agente guest affinché consideri attendibile la prima macchina con cui si connette.

L'installazione del file PEM relativo al server attendibile su ciascun modello insieme all'agente guest è l'approccio più sicuro. Per motivi di sicurezza, l'agente guest non effettua la verifica di un certificato se nella directory VRMGuestAgent è già presente un file PEM. Se i certificati dei server cambiano, è necessario rigenerare manualmente i modelli con i nuovi file PEM.

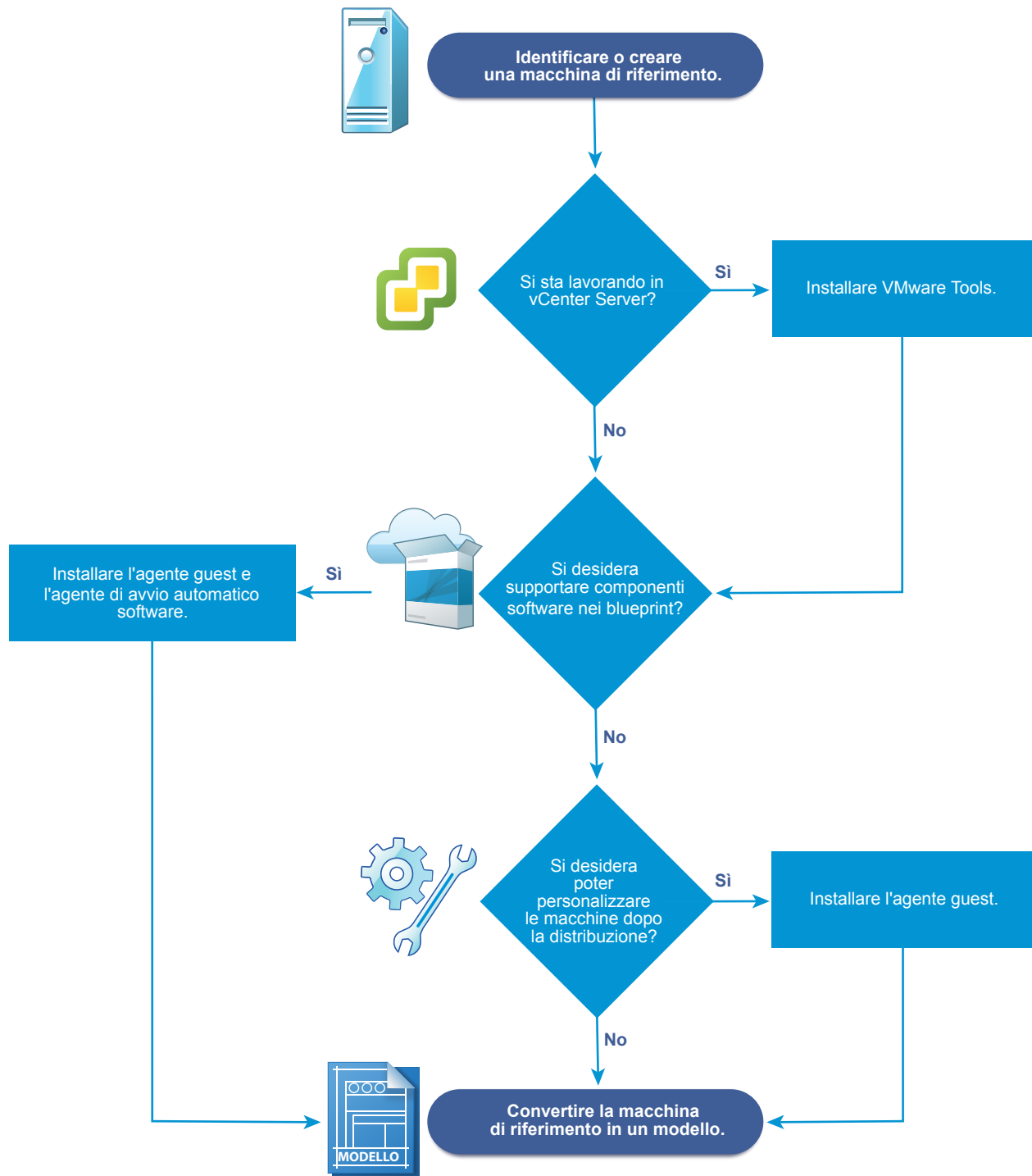
È possibile anche configurare l'agente guest per popolare il file PEM attendibile al primo utilizzo. Si tratta di un'opzione meno sicura rispetto all'installazione manuale dei file PEM su ogni modello, ma più flessibile in quegli ambienti in cui può essere preferibile utilizzare un singolo modello per più server. Per consentire all'agente guest di considerare attendibile il primo server a cui si connette, creare un modello senza file PEM nella directory VRMGuestAgent. L'agente guest popolerà il file PEM la prima volta che si conatterà

a un server. Un modello considera sempre attendibile il primo sistema a cui si connette. Per motivi di sicurezza, l'agente guest non effettua la verifica di un certificato se nella directory VRMGuestAgent è già presente un file PEM. Se il certificato del server cambia, è necessario rimuovere il file PEM dalla directory VRMGuestAgent. L'agente guest installerà il nuovo file PEM la prima volta che si conatterà al server.

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.

Tavola 1-7. 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

Tavola 1-8. 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"> ■ Clone ■ Clone collegato ■ NetApp FlexClone
Nome specifico della personalizzazione (obbligatorio per la clonazione con indirizzi IP statici)		Non è possibile eseguire personalizzazioni di macchine Windows senza un oggetto specifica di personalizzazione.
(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.

Tavola 1-9. 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.

Tavola 1-10. 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. %System Drive %Programmi (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs.
ExternalPostProvisioningVbScript		Eseguire uno script al termine del provisioning. Immettere il percorso completo dello script includendo il nome del file e l'estensione. %System Drive %Programmi (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs

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.

Tavola 1-11. 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.

Tavola 1-12. 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 disabilitare 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.

Tavola 1-12. Foglio di calcolo delle proprietà personalizzate per la personalizzazione delle macchine clonate con un agente guest (Continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.DiskN.Size		<p>Definisce la dimensione in GB del disco <i>N</i>. Ad esempio, per assegnare una dimensione pari a 150 GB a un disco G, definire la proprietà personalizzata VirtualMachine.Disk0.Size e immettere il valore 150. La numerazione dei dischi deve essere sequenziale. Per impostazione predefinita, una macchina ha un solo disco a cui si fa riferimento mediante VirtualMachine.Disk0.Size, dove la dimensione è specificata dal valore dello storage sul blueprint da cui è stato eseguito il provisioning della macchina. Il valore dello storage dell'interfaccia utente del blueprint sovrascrive il valore nella proprietà VirtualMachine.Disk0.Size. La proprietà VirtualMachine.Disk0.Size non è disponibile come proprietà personalizzata per via della sua relazione con l'opzione di storage sul blueprint. È possibile aggiungere altri dischi specificando VirtualMachine.Disk1.Size, VirtualMachine.Disk2.Size e così via. VirtualMachine.Admin.TotalDiskUsag e rappresenta sempre il totale delle proprietà .DiskN.Size più l'allocazione della dimensione di VMware.Memory.Reservation.</p>
VirtualMachine.DiskN.Label		<p>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.</p>

Tavola 1-12. Foglio di calcolo delle proprietà personalizzate per la personalizzazione delle macchine clonate con un agente guest (Continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.DiskN.Letter		Specifica la lettera di unità o il punto di montaggio del disco N 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.
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.

Tavola 1-12. Foglio di calcolo delle proprietà personalizzate per la personalizzazione delle macchine clonate con un agente guest (Continua)

Proprietà personalizzata	Valore personale	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 <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 <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>
VirtualMachine.SoftwareN.ISOName		<p>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.</p>
VirtualMachine.SoftwareN.ISOLocation		<p>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 <code>netapp-1:it_nfs_1</code>. Se il valore non viene specificato, l'immagine ISO non viene montata.</p>

Proprietà personalizzate di rete

Se non si sta eseguendo l'integrazione con NSX, è comunque possibile specificare una configurazione per dispositivi di rete specifici su una macchina utilizzando proprietà personalizzate.

Tavola 1-13. 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.</p>

Tavola 1-13. 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 <i>N</i>. 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.Network<i>N</i> 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.</p>

Tavola 1-13. 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 <i>N</i>= 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.</p> <p>È possibile aggiungere questa proprietà a un componente macchina vCloud Air o vCloud Director in un blueprint.</p>
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 <code>VirtualMachine.NetworkN</code> 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.</p>

Tavola 1-13. Proprietà personalizzate per la configurazione del networking (Continua)

Proprietà personalizzata	Valore personale	Descrizione
VirtualMachine.NetworkN.ProfileName		<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>Quando si utilizza la proprietà VirtualMachine.NetworkN.ProfileName, il profilo di rete a cui fa riferimento viene utilizzato per allocare un indirizzo IP. Tuttavia, la macchina di cui è stato eseguito il provisioning viene collegata a qualsiasi rete selezionata nella prenotazione utilizzando un modello di tipo round robin.</p>
<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.ProfileName.</p>

Tavola 1-13. Proprietà personalizzate per la configurazione del networking (Continua)

Proprietà personalizzata	Valore personale	Descrizione
VCNS.LoadBalancerEdgePool.Name <i>s.name</i>		<p>Specifica i pool di bilanciamento del carico di vCloud Networking and Security 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

Tavola 1-13. 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 vCloud Networking and Security 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 vCloud Networking and Security 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

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.

vRealize Automation richiede che il proprio catalogo pubblicato sia condiviso con tutte le organizzazioni di vCloud Director. La raccolta dei dati non viene eseguita se il catalogo pubblicato non viene condiviso con tutte le organizzazioni di vCloud Director.

Nei punti seguenti vengono descritti a grandi linee i passaggi da eseguire prima di utilizzare vRA 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 d'installazione della console di gestione di vCloud Automation Center Appliance.
Ad esempio `https://vcac-hostname.domain.name:5480/installer/`.

- 2 Scaricare e salvare i pacchetti degli agenti guest di Linux.
- 3 Decomprimere il file `LinuxGuestAgentPkgs`.
- 4 Aprire la directory contenente il file `LinuxGuestAgentPkgs` e individuare la sottodirectory corrispondente al sistema operativo guest distribuito durante il provisioning.
- 5 Aprire il file `sample-https.cfg`.
- 6 Sostituire tutte le ricorrenze della stringa `host=dcac.example.net` con l'indirizzo IP o il nome di dominio completo e il numero di porta dell'host del server vRealize Automation.

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>

- 7 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
```

- 8 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
```

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.

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

- 1 Consultare l'amministratore di rete per assicurarsi che siano soddisfatti i seguenti requisiti della rete:
 - La comunicazione con SCCM richiede il nome NetBios del server SCCM. Almeno un Distributed Execution Manager (DEM) deve essere in grado di risolvere il nome di dominio completo del server SCCM nel suo nome NetBios.
 - Il server SCCM e il server vRealize Automation devono trovarsi nella stessa rete e poter comunicare tra loro.
- 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.

Nota: è possibile creare un gruppo di proprietà con la proprietà `SCCMProvisioningProperties` impostata per includere tutte queste informazioni richieste. In questo modo sarà più semplice includere le informazioni nei blueprint.

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 d'installazione della console di gestione di vCloud Automation Center Appliance.
Ad esempio `https://vcac-hostname.domain.name:5480/installer/`.
- 2 Scaricare e salvare i file dell'agente guest Windows.
 - File agente guest Windows (**32 bit**).
 - File agente guest Windows (**64 bit**).
- 3 Estrarre i file dell'agente guest Windows in una posizione accessibile da SCCM.
- 4 Creare un pacchetto software dal file di definizione `SCCMPackageDefinitionFile.sms`.
- 5 Rendere il pacchetto software disponibile nel punto di distribuzione in uso.
- 6 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 deve essere costituita da una directory di rete che può essere specificata come percorso UNC o montata come unità di rete dalla macchina di riferimento, il sistema su cui creare l'immagine WinPE e l'host di virtualizzazione su cui viene eseguito il provisioning delle macchine.
- 2 Assicurarsi che nella rete sia disponibile un server DHCP. vRealize Automation non può eseguire il provisioning di macchine utilizzando un'immagine WIM se non è disponibile il servizio DHCP.
- 3 Identificare o creare la macchina di riferimento all'interno della 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. È possibile utilizzare vRealize Automation PEBuilder per creare un'immagine WinPE che include l'agente guest.
 - [Installazione PEBuilder](#).
 - (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 per la specifica installazione di PEBuilder. Vedere [Definizione di script personalizzati in un WinPE di PEBuilder](#).
 - 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](#).
 - [Creazione di un'immagine WinPE utilizzando PEBuilder](#).

È possibile creare l'immagine WinPE con un altro metodo, ma in quel caso sarà necessario inserire 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 fornita dall'hypervisor.

8 Raccogliere le seguenti informazioni in modo da poterle 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.

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 7.1*.

Requisiti di SysPrep per la macchina di riferimento

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

Tavola 1-14. 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.

Tavola 1-15. 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

Tavola 1-15. Impostazioni di SysPrep richieste per la macchina di riferimento che non utilizzano Windows Server 2003 o Windows XP: (Continua)

Impostazioni di AutoLogon	Valore
Username	<p><i>username</i></p> <p>(<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).</p>
Password	<p><i>password</i></p> <p>(<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).</p> <p>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.</p>

Installazione PEBuilder

Lo strumento PEBuilder fornito da vRealize Automation è un modo semplice di includere l'agente guest di vRealize Automation nelle immagini WinPE.

PEBuilder ha un agente guest a 32 bit. Se occorre eseguire comandi specifici per i 64 bit, installare PEBuilder e quindi recuperare i file a 64 bit dal file `GugentZipx64.zip`.

Installare PEBuilder in una posizione da cui è possibile accedere all'ambiente di staging.

Prerequisiti

- Installare NET Framework 4.5.
- Windows Automated Installation Kit (AIK) per Windows 7 (incluso WinPE 3.0) deve essere installato.

Procedura

- 1 Aprire la pagina d'installazione della console di gestione di vCloud Automation Center Appliance.
Ad esempio `https://vcac-hostname.domain.name:5480/installer/`.
- 2 Scaricare PEBuilder.
- 3 (Facoltativo) Scaricare il pacchetto dell'agente guest di Windows a 64 bit se si desidera includere l'agente guest di Windows 64 bit nell'immagine WinPE al posto dell'agente guest di Windows 32 bit.
- 4 Eseguire `VCAC-WinPEBuilder-Setup.exe`.

- 5 Attenersi alle istruzioni visualizzate per installare PEBuilder.
- 6 (Facoltativo) Sostituire i file dell'agente guest di Windows a 32 bit situato in \PE Builder\Plugins\VRM Agent\VRMGuestAgent con i file a 64 bit per includere l'agente a 64 bit in WinPE.

È possibile utilizzare PEBuilder per creare un WinPE da utilizzare nel provisioning WIM.

Definizione di script personalizzati in un WinPE di PEBuilder

È possibile utilizzare PEBuilder per personalizzare le macchine eseguendo script bat personalizzati in punti specifici del workflow di provisioning.

Prerequisiti

[Installazione PEBuilder.](#)

Procedura

- 1 Creare o identificare lo script bat da utilizzare.

Lo script deve restituire un valore diverso da zero in caso di errore per evitare che il provisioning della macchina abbia esito negativo.

- 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 Collocare gli script nella sottodirectory degli elementi di lavoro corrispondente al punto del workflow di provisioning in cui si desidera eseguire lo script.

Ad esempio C:\Programmi (x86)\VMware\vRA\PE Builder\Plugins\VRM Agent\VRMGuestAgent\site\SetupOS.

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

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 nella sottodirectory `Plugins` della directory d'installazione di PEBuilder prima di creare un'immagine WinPE, o inserire i driver in un'immagine WinPE già creata impiegando altri sistemi.
- 3 Caricare l'ISO dell'immagine WinPE nei domini di storage ISO di Red Hat Enterprise Virtualization utilizzando il comando `rhevms-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).

Creazione di un'immagine WinPE utilizzando PEBuilder

Utilizzare lo strumento PEBuilder fornito da vRealize Automation per creare un file ISO di WinPE che includa l'agente guest di vRealize Automation.

Prerequisiti

- [Installazione PEBuilder](#).
- (Facoltativo) Configurare PEBuilder per includere l'agente guest di Windows 64 bit nell'immagine WinPE al posto dell'agente guest di Windows 32 bit. Vedere [Installazione PEBuilder](#).
- (Facoltativo) Aggiungere nella sottodirectory `PlugIns` della directory d'installazione di PEBuilder tutti i plug-in di terze parti da includere nell'immagine di WinPE.
- (Facoltativo) [Definizione di script personalizzati in un WinPE di PEBuilder](#).

Procedura

- 1 Avviare PEBuilder.

2 Immettere le informazioni sull'host del servizio di gestione di IaaS.

Opzione	Descrizione
Se si utilizza il bilanciamento del carico	a Specificare il nome di dominio completo del bilanciamento del carico per il servizio di gestione di IaaS nella casella di testo Nome host vCAC . Ad esempio manager_service_LB.mycompany.com .
	b Specificare il numero di porta del bilanciamento del carico del servizio di gestione di IaaS nella casella di testo Porta vCAC . Ad esempio 443 .
Senza bilanciamento del carico	a Specificare il nome di dominio completo della macchina del servizio di gestione di IaaS nella casella di testo Nome host vCAC . Ad esempio manager_service.mycompany.com .
	b Specificare il numero di porta della macchina del servizio di gestione di IaaS nella casella di testo Porta vCAC . Ad esempio 443 .

3 Immettere il percorso della directory dei plug-in di PEBuilder.

Esso dipende dalla directory d'installazione selezionata durante l'installazione. Il percorso predefinito è C:\Programmi (x86)\VMware\vCAC\PE Builder\PlugIns.

4 Immettere il percorso di output del file ISO da creare nella casella di testo **ISO Output Path**.

È preferibile che questa posizione si trovi nell'area di staging preparata.

5 Fare clic su **File > Avanzate**.

Nota: non modificare le impostazioni di **Architettura WinPE** o **Protocollo**.

6 Selezionare la casella di controllo **Includi agente guest di vCAC in ISO WinPE**.

7 Fare clic su **OK**.

8 Fare clic su **Build**.

Passi successivi

Collocare l'immagine di WinPE nella posizione richiesta dalla piattaforma di integrazione utilizzata. Se non si conosce la posizione, consultare la documentazione fornita a corredo con la piattaforma.

Se si sta eseguendo il provisioning di macchine HP iLO, collocare l'immagine di WinPE in una posizione accessibile via Web. Per le macchine Dell iDRAC, collocare l'immagine in una posizione disponibile a NFS o CIFS. Registrare l'indirizzo.

Inserimento manuale dell'agente guest in un'immagine WinPE

Non è necessario utilizzare PEBuilder di vRealize Automation per creare il proprio WinPE. Tuttavia, se non si utilizza PEBuilder, è necessario inserire manualmente l'agente guest di 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

Se si sceglie di non utilizzare PEBuilder di vRealize Automation per creare il WinPE, è necessario installare PEBuilder per copiare manualmente i file dell'agente guest nell'immagine WinPE.

2 Configurazione del file doagent.bat

Se si sceglie di non utilizzare vRealize Automation PEBuilder, è necessario configurare manualmente il file doagent.bat.

3 Configurazione del file doagentc.bat

Se si sceglie di non utilizzare vRealize Automation PEBuilder, è necessario configurare manualmente il file doagentc.bat.

4 Configurazione dei file di proprietà dell'agente guest

Se si sceglie di non utilizzare vRealize Automation PEBuilder, è necessario configurare manualmente il file di proprietà dell'agente guest.

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

Se si sceglie di non utilizzare PEBuilder di vRealize Automation per creare il WinPE, è necessario installare PEBuilder per copiare manualmente i file dell'agente guest nell'immagine WinPE.

PEBuilder ha un agente guest a 32 bit. Se occorre eseguire comandi specifici per i 64 bit, installare PEBuilder e quindi recuperare i file a 64 bit dal file GugentZipx64.zip.

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 Aprire la pagina d'installazione della console di gestione di vCloud Automation Center Appliance.

Ad esempio <https://vcac-hostname.domain.name:5480/installer/>.

2 Scaricare PEBuilder.

3 (Facoltativo) Scaricare il pacchetto dell'agente guest di Windows a 64 bit se si desidera includere l'agente guest di Windows 64 bit nell'immagine WinPE al posto dell'agente guest di Windows 32 bit.

- 4 Eseguire `vCAC-WinPEBuilder-Setup.exe`.
- 5 Deselezionare sia **Plugins** che **PEBuilder**.
- 6 Espandere **Plugins** e selezionare **VRMAgent**.
- 7 Seguire le istruzioni presentate per completare l'installazione.
- 8 (Facoltativo) Dopo aver completato l'installazione, sostituire i file dell'agente guest di Windows a 32 bit situato in `\PE Builder\Plugins\VRM Agent\VRMGuestAgent` con i file a 64 bit per includere l'agente a 64 bit in WinPE.
- 9 Copiare il contenuto di `%SystemDrive%\Programmi (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent` in una nuova posizione all'interno dell'immagine WinPE.

Ad esempio: `C:\Programmi (x86)\VMware\PE Builder\Plugins\VRM Agent\VRMGuestAgent`.

Passi successivi

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

Configurazione del file `doagent.bat`

Se si sceglie di non utilizzare vRealize Automation PEBuilder, 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\PE Builder\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 s_client -connect`.

```
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.

Passi successivi

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

Configurazione del file `doagentc.bat`

Se si sceglie di non utilizzare vRealize Automation PEBuilder, 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\PE Builder\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, <pre>load_balancer_manager_service.mycompany.com:443</pre>
Senza bilanciamento del carico	Specificare il nome di dominio completo e la porta relativi al servizio di gestione. Ad esempio, <pre>manager_service.mycompany.com:443</pre>

- 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.

Passi successivi

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

Configurazione dei file di proprietà dell'agente guest

Se si sceglie di non utilizzare vRealize Automation PEBuilder, è necessario configurare manualmente il file di proprietà dell'agente guest.

Prerequisiti

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

Procedura

- 1 Passare alla directory VRMGuestAgent all'interno dell'immagine WinPE.
Ad esempio: C:\Programmi (x86)\VMware\PE Builder\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 disabilitato 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.

vRealize Automation supporta diverse caratteristiche di OpenStack. Per informazioni recenti sul supporto delle caratteristiche di OpenStack, vedere *Matrice di supporto di vRealize Automation* all'indirizzo <https://www.vmware.com/support/pubs/vcac-pubs.html>.

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 7.1*.
- 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 alla console di vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Fare clic su **Infrastruttura > Amministrazione > Tipi di istanze**.
- 2 Fare clic su **Nuovo tipo di istanza**.
- 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** (✓).

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

Passi successivi

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 in Rainpole

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.



È possibile convertire una macchina di riferimento CentOS esistente in un modello di vSphere così da consentire anche agli architetti di Rainpole 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.

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 in Rainpole](#)
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 Spegnere 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**.

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

Passi successivi

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 in Rainpole

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**.
Ad esempio **rainpole.local**.
 - 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**.

È disponibile una specifica di personalizzazione generale che è possibile utilizzare per creare blueprint per la clonazione di macchine Linux.

Passi successivi

Accedere alla console vRealize Automation come l'amministratore della configurazione creato durante l'installazione e richiedere gli elementi del catalogo con cui impostare rapidamente il prototipo.

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 e Amazon AWS.

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 di macchine Amazon.

Tavola 1-16. Metodi di provisioning che supportano Software

Tipo di macchina	Metodo di provisioning	Preparazione richiesta
vSphere	Clone	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	Clone collegato	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	Clone	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	Clone	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 AWS	Immagine macchina Amazon	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 AWS 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. Per istruzioni sulla creazione delle AMI Amazon supportate da EBS, vedere la documentazione relativa ad Amazon AWS. Perché l'agente guest e l'agente bootstrap di Software funzionino sulle macchine con provisioning, è necessario configurare la connettività tra rete e VPC.

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

È possibile installare la versione supportata di Java Runtime Environment, l'agente guest e l'agente di avvio automatico di Software sulla macchina di riferimento Windows per creare un modello, uno snapshot o un'istanza di macchina Amazon che supporti i componenti di Software.

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

Importante: poiché il processo di avvio non deve essere interrotto, configurare la macchina virtuale in modo che il processo di avvio non possa essere messo in pausa prima della richiesta di accesso del sistema operativo. 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.
- Se è presente un agente guest o un agente di avvio automatico di Software precedentemente installato sulla macchina, rimuovere gli agenti e i registri di runtime. Vedere [Aggiornamento dei modelli di macchine virtuali esistenti in vRealize Automation](#).
- Se si prevede di accedere in remoto alla macchina virtuale usando Desktop remoto Windows per la risoluzione dei problemi o per altri motivi, installare i servizi RDS (Remote Desktop Services) per Windows.
- Verificare che tutti gli elementi della configurazione di rete siano rimossi dai relativi file di configurazione.
- Se si desidera adottare l'approccio più sicuro per stabilire attendibilità fra l'agente guest e la macchina del servizio di gestione, ottenere il certificato SSL in formato PEM dalla macchina del servizio di gestione. Per informazioni sull'installazione di un agente guest in una macchina Windows, consultare [Installazione dell'agente guest su una macchina di riferimento Windows](#). Per ulteriori informazioni su come l'agente guest stabilisce l'attendibilità, consultare [Configurazione di un agente guest Windows in modo che consideri attendibile un server](#).

Procedura

- 1 Accedere alla macchina di riferimento Windows come amministratore di Windows e aprire un prompt dei comandi.

- 2 Scaricare e installare la versione supportata di Java Runtime Environment da https://vRealize_VA_Hostname_fqdn/software/index.html.
 - a Scaricare il file .zip di Java SE Runtime Environment da https://vRealize_VA_Hostname_fqdn/software/download/jre-version-win64.zip.
 - b Creare una cartella `c:\opt\vmware-jre` e decomprimere il file .zip JRE nella cartella.
 - c Aprire una finestra del prompt dei comandi e immettere `c:\opt\vmware-jre\bin\java -version` per verificare l'installazione.
Viene visualizzata la versione di Java installata.
- 3 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.
- 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 Configurare l'agente guest per cui rendere attendibile la macchina del servizio di gestione.

Opzione	Descrizione
Consente all'agente guest di considerare attendibile la prima macchina alla quale si collega.	Nessuna configurazione richiesta.
Installare manualmente il file PEM attendibile.	Inserire il file PEM del servizio di gestione nella directory C:\VRMGuestAgent\.

- d Eseguire il comando seguente: `winservice -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>winservice -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>winservice -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>winservice -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code>

- 5 Scaricare il file bootstrap agente Software da https://vRealize_VA_Hostname_fqdn/software/index.html.

- a Scaricare il file dell'agente di avvio automatico Software https://vRealize_VA_Hostname_fqdn/software/download/vmware-vra-software-agent-bootstrap-windows_version.zip.
- b Fare clic con il pulsante destro del mouse sul file e scegliere **Proprietà**.
- c Fare clic su **Generale**.
- d Fare clic su **Sblocca**.

Importante: Se la funzionalità di sicurezza Windows non viene disattivata, non è possibile utilizzare il file di bootstrap dell'agente di Software.

- e Decomprimere il file `vmware-vra-software-agent-bootstrap-windows_version.zip` nella cartella `c:\temp`.

6 Installare l'agente di avvio automatico Software.

- a Aprire una console CMD di Windows e accedere alla cartella `c:\temp`.
- b Immettere il comando per installare l'agente di avvio automatico.

```
install.bat password=Password managerServiceHost=manager_service_machine.mycompany.com
managerServicePort=443 httpsMode=true cloudProvider=ec2|vca|vcd|vsphere
```

Il numero di porta predefinito per il servizio di gestione è 443. I valori accettati per `cloudprovider` sono `ec2`, `vca`, `vcd` e `vsphere`. Lo script `install.bat` crea un account utente denominato `darwin` per l'agente di avvio automatico software utilizzando la password impostata nel comando d'installazione. La *password* impostata deve soddisfare i requisiti per le password di Windows.

Se l'installazione non riesce a causa di una dipendenza .NET, consultare il seguente articolo per ricevere assistenza: <https://technet.microsoft.com/en-us/library/dn482071.aspx>

7 Verificare che sia presente l'utente **darwin**.

- a Immettere `lusrmgr.msc` al prompt dei comandi.
- b Verificare che sia presente l'utente **darwin_user** e che appartenga al gruppo amministratore.
- c Impostare la password senza scadenza.

L'impostazione assicura che il modello rimanga utilizzabile dopo 30 giorni.

Se l'utente non è disponibile, verificare che la password del server Windows sia corretta.

8 Arrestare la macchina virtuale Windows.

Passi successivi

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.

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

È possibile utilizzare un singolo script per installare le versioni supportate di Java Runtime Environment, agente guest e agente di avvio automatico di Software sulla macchina di riferimento Linux per creare un modello, uno snapshot o un'istanza di macchina Amazon che supporta componenti di Software.

Software supporta l'esecuzione di script con Bash.

Importante: poiché il processo di avvio non deve essere interrotto, configurare la macchina virtuale in modo che il processo di avvio non possa essere messo in pausa prima della richiesta di accesso del sistema operativo. 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 e 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

Per informazioni correlate sui requisiti preliminari di Linux, vedere lo script `prepare_vra_template.sh`.

- Se si prevede di accedere in remoto alla macchina virtuale usando l'accesso Linux `ssh` per la risoluzione dei problemi o per altri motivi, installare il server OpenSSH e il client per Linux.
- Rimuovere gli elementi della configurazione di rete dai relativi file di configurazione.

Procedura

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

```
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.

6 Arrestare la macchina virtuale Linux.

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

Passi successivi

Sull'hypervisor o provider di cloud, convertire la macchina di riferimento in un modello, uno snapshot o un'immagine di macchina Amazon che gli architetti dell'infrastruttura possono utilizzare nella creazione di 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\agent_bootstrap_removal.bat
c:\opt\vmware-appdirector\agent-bootstrap\agent_reset.bat
```

Scenario: preparazione di un modello CentOS di vSphere per clonare blueprint di componenti software e macchine

Un amministratore di vCenter Server procede alla preparazione di un modello di vSphere che gli architetti di vRealize Automation possono utilizzare per clonare 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`.

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.

Passi successivi

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 [Scenario: creazione di un blueprint CentOS di vSphere per la clonazione in Rainpole](#).

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 Nel browser web, aprire il seguente URL.

`https://vrealize-automation-appliance-FQDN/software/index.html`

- 2 Salvare lo script `prepare_vra_template.sh` nella macchina di riferimento.
- 3 Nella macchina di riferimento, rendere eseguibile `prepare_vra_template.sh`.

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

- 4 Eseguire `prepare_vra_template.sh`.

```
./prepare_vra_template.sh
```

- 5 Seguire le istruzioni visualizzate.

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

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 Spegnerla 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**.

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**.

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. Disabilitare SELinux sulla macchina di riferimento per assicurarsi che il modello supporti l'implementazione specifica di MySQL utilizzata nell'applicazione campione Dukes Bank.

Prerequisiti

- Installare e configurare completamente vRealize Automation. Vedere *Installazione e configurazione di vRealize Automation per lo scenario Rainpole*.
- 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, disabilitare 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.

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 d'installazione da vRealize Automation appliance.

```
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.

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, disabilitare 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` per disabilitare SELinux.

```
SELINUX=disabled
```

Se non si disabilita 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 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 **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**.

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**.

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

Passi successivi

- 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 esterno](#).
- 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](#).

Configurazione delle impostazioni del tenant

2

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.

Tavola 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	Per un esempio di creazione di account utente locali, vedere Scenario: creazione degli account utente locali per Rainpole .
<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
<input type="checkbox"/> (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 di sistema■ Amministratore tenant	Configurazione del branding personalizzato
<input type="checkbox"/> (Facoltativo) Configurare vRealize Automation per inviare notifiche agli utenti quando si verificano eventi specifici.	<ul style="list-style-type: none">■ Amministratore di sistema■ Amministratore tenant	Elenco di controllo per la configurazione delle notifiche

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

Attività	Ruolo di vRealize Automation	Dettagli
<input type="checkbox"/> (Facoltativo) Configurare vRealize Orchestrator per il supporto di XaaS e di altre opzioni di estendibilità.	<ul style="list-style-type: none"> ■ Amministratore di sistema ■ Amministratore tenant 	Configurazione di vRealize Orchestrator e dei plug-in
<input type="checkbox"/> (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
<input type="checkbox"/> (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 .

Questo capitolo include i seguenti argomenti:

- [Scelta delle opzioni di configurazione di Gestione directory](#)
- [Scenario: configurazione di un collegamento Active Directory per un vRealize Automation ad alta disponibilità](#)
- [Configurazione dell'autenticazione smart card per vRealize Automation](#)
- [Creazione di un link di Active Directory multidominio o a più foreste](#)
- [Configurazione dei ruoli di utenti e gruppi](#)
- [Scenario: configurazione del tenant predefinito per Rainpole](#)
- [Creazione di tenant aggiuntivi](#)
- [Eliminazione di un tenant](#)
- [Configurazione del branding personalizzato](#)
- [Elenco di controllo per la configurazione delle notifiche](#)
- [Creazione di un file RDP personalizzato per il supporto di connessioni RDP per le macchine di cui è stato eseguito il provisioning](#)
- [Scenario: aggiunta di posizioni di data center per distribuzioni tra più regioni](#)
- [Configurazione di vRealize Orchestrator e dei plug-in](#)

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.

Tavola 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 ad Active Directory. 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 .
(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.

Tavola 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. È possibile creare una o più directory e quindi sincronizzarle 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 vRealize Automation appliance contiene un connettore. Vedere Gestione dei 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>
Provider di identità	<p>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.</p> <p>Vedere Configurazione di un'istanza di provider di identità.</p>
Criteri	<p>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.</p>

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 di un'Active Directory o directory LDAP nel 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: Se si utilizzano provider di identità di terze parti, è possibile configurare il connettore per la sincronizzazione dei dati di utenti e gruppi o per configurare il provisioning Just-in-Time degli utenti. Per ulteriori informazioni, vedere la sezione relativa al provisioning Just-in-Time degli utenti nella guida *VMware Identity Manager Administration*.

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 ha un proprio concetto di directory, corrispondente all'Active Directory o directory LDAP nell'ambiente dell'utente. Tale directory utilizza attributi per definire utenti e gruppi.

- Active Directory
 - 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.

- Directory LDAP

Il servizio non ha accesso diretto all'Active Directory o directory LDAP dell'utente. Solo il connettore dispone di accesso diretto. 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. Ciascun Worker agisce come 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 l'Active Directory o la directory LDAP dell'utente e il servizio tramite uno o più Worker.

Importante: In un'istanza del connettore non possono essere presenti due Worker di Active Directory 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 ad Active Directory](#). 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 ad Active Directory](#). 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 ad Active Directory](#). 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 ad Active Directory](#). 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.

Configurazione di un collegamento ad Active Directory

È necessario utilizzare la funzionalità Directories Management per configurare un collegamento ad Active Directory che consenta di usufruire dell'autenticazione utente per tutti i tenant e selezionare utenti e gruppi da sincronizzare con la directory di Directories Management.

Sono disponibili due opzioni di protocollo di comunicazione ad Active Directory: Active Directory su LDAP e Active Directory (autenticazione integrata di Windows). Per impostazione predefinita una connessione Active Directory su protocollo LDAP supporta la ricerca della posizione del servizio DNS. 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.

Dopo aver selezionato un protocollo di comunicazione 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.

Prerequisiti

- Connettore installato e codice di attivazione attivato.
- 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.
- 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.
- 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.
- Accedere alla console vRealize Automation come **amministratore tenant**.

Procedura

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

- 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 vRealize Automation appliance 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.

- 6 Immettere le informazioni necessarie nella casella di testo Posizione server se è stata selezionata l'opzione Active Directory su LDAP o nelle caselle di testo 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	<ul style="list-style-type: none"> ■ 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. ■ 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. ■ 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.
Dettaglio unione al dominio - Visualizzata quando l'opzione Active Directory (autenticazione Windows integrata) è selezionata	Immettere le credenziali necessarie nelle caselle di testo Nome dominio , Nome utente amministratore di dominio e Password amministratore di dominio .

- 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.

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. 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.

- 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.

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

La connessione ad Active Directory è completa e gli utenti e i gruppi selezionati vengono aggiunti alla directory.

Passi successivi

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 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 vRealize Automation appliance include un connettore che supporta l'autenticazione utente, sebbene 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 vRealize Automation appliance, si connetta al provider di identità e punti alla stessa 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

- Configurare la distribuzione vRealize Automation con almeno due istanze di vRealize Automation appliance.
- Installare vRealize Automation in modalità Enterprise operando in un singolo dominio con due istanze di vRealize Automation appliance.
- 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 di vRealize Automation appliance. Per informazioni sulla configurazione dei tenant, vedere [Capitolo 2 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 alla vRealize Automation appliance 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.

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 o modificare 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 alla console 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 (URI 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.clic
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 + sotto l'intestazione **Regole criterio** per aggiungere una nuova regola.

Utilizzare i campi 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 dell'utente è "**Mie macchine**" e l'utente ha necessità di accedere ai contenuti provenienti da "**Tutti i tipi di dispositivi**", per una distribuzione tipica l'utente dovrà autenticarsi con il metodo seguente: **Nome utente e password ADFS**.

- d Fare clic su **Salva** per salvare gli aggiornamenti al 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 sarà necessario modificarla aggiungendo il seguente testo:

```
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.

Tavola 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 alla console 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'intestazione 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 idp.xml di SSO2 nella casella di testo e fare clic su Elabora metadati IDP .
Nome del criterio ID nome nella richiesta SAML (facoltativo)	Immettere http://schemas.xmlsoap.org/claims/UPN.
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 urn:oasis:names:tc:SAML:2.0:ac:classes:Password.
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.

Quando si aggiungono gruppi e utenti, il sistema di autenticazione degli utenti di Gestione directory importa i dati da Active Directory. La velocità del sistema è limitata dalle capacità 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, chiudere tutte le applicazioni non necessarie e verificare che nella propria distribuzione la quantità di memoria allocata ad Active Directory sia appropriata. Se i problemi persistono, aumentare la quantità di memoria allocata ad Active Directory in base alle necessità. 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 si esegue un'operazione di sincronizzazione per una distribuzione di vRealize Automation con molti utenti e gruppi, potrebbe verificarsi un ritardo dopo che il messaggio Sincronizzazione in corso scompare, prima della visualizzazione dei dettagli del registro di sincronizzazione. Inoltre, il timestamp del file di registro potrebbe essere diverso dall'ora di completamento dell'operazione di sincronizzazione indicata nell'interfaccia utente.

Nota: Non è possibile annullare un'operazione di sincronizzazione dopo che è stata avviata.

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.
- Per l'autenticazione integrata di Windows in Active Directory, se sono configurate più foreste Active Directory e il gruppo Dominio locale contiene membri di domini di foreste diverse, verificare che l'utente di binding sia aggiunto al gruppo Administrators del dominio in cui risiede il gruppo Dominio locale. In caso contrario, tali membri risulteranno mancanti dal gruppo Dominio locale.
- Accedere alla console 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 nuova riga per le definizioni DN dei gruppi e inserire il DN del gruppo desiderato.
- 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 nuova riga per la definizione DN degli utenti e inserire il DN utente desiderato.

Per eliminare la definizione DN di un utente, fare clic sull'icona **x** corrispondente.

- 5 Fare clic su **Salva** per salvare le modifiche senza sincronizzazione, oppure fare clic su **Salva e sincronizza** per salvare le modifiche ed eseguire la sincronizzazione in modo da implementare 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**.

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, VMware consiglia di aumentare a 6 GB l'allocazione di memoria di Directories Management.

La memoria di Gestione directory è calcolata in base alla memoria totale allocata per vRealize Automation appliance. Nella tabella seguente sono elencate le allocazioni di memoria corrispondenti ai componenti rilevanti.

Tavola 2-5. Allocazione di memoria di vRealize Automation appliance

Memoria 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 su cui è in esecuzione una vRealize Automation appliance.
- 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 vRealize Automation appliance.

Creazione di un file di ricerca host di dominio per bypassare la ricerca DNS di Posizione servizio (SRV)

Quando si abilita l'autenticazione integrata di Windows, la configurazione della Directory cambia per attivare il campo relativo alla ricerca DNS di Posizione servizio. La ricerca di Posizione servizio del connettore non è basata sul sito. Se si desidera scavalcare la sezione DC casuale, è possibile creare un file chiamato `domain_krb.properties` e aggiungere i valori che consentiranno di risolvere domini in host ignorando la ricerca di SRV.

Procedura

- 1 Dalla riga di comando di `appliance-va`, accedere utilizzando un utente dotato di privilegi root.
- 2 Passare alla directory `/usr/local/horizon/conf` e creare un file chiamato `domain_krb.properties`.
- 3 Aprire il file `domain_krb.properties` in modifica e aggiungere l'elenco dei valori da dominio a host. Aggiungere le informazioni nella forma `<AD Domain>=<host:port>, <host2:port2>, <host2:port2>`.

Ad esempio, inserire un elenco come questo: `example.com=examplehost.com:636, examplehost2.example.com:389`
- 4 Cambiare il proprietario del file `domain_krb.properties` in `horizon` e il gruppo in `www`. Immettere il comando `chown horizon:www /usr/local/horizon/conf/domain_krb.properties`.
- 5 Riavviare il servizio. Immettere il comando `service horizon-workspace restart`.

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 possono essere mappati con gli attributi di Active Directory. È possibile selezionare gli attributi necessari e aggiungere altri attributi di Active Directory che si desidera sincronizzare con la directory.

Tavola 2-6. Attributi di Active Directory predefiniti da sincronizzazione nella directory

Nome attributo directory	Mappatura predefinita nell'attributo di Active Directory
<code>userPrincipalName</code>	<code>userPrincipalName</code>
<code>distinguishedName</code>	<code>distinguishedName</code>
<code>employeeId</code>	<code>employeeID</code>
<code>domain</code>	<code>canonicalName</code> . Aggiunge il nome di dominio completo dell'oggetto.

Tavola 2-6. Attributi di Active Directory predefiniti da sincronizzazione nella directory (Continua)

Nome attributo directory	Mappatura predefinita nell'attributo di Active Directory
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

La pagina Attributi utente elenca gli attributi di directory predefiniti che possono essere mappati con gli attributi di Active Directory. È possibile selezionare gli attributi necessari e aggiungere altri attributi di Active Directory che si desidera sincronizzare con la directory.

Tavola 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 dei 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 vRealize Automation appliance 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 Worker, 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 disabilitare. Vedere [Configurazione di un'istanza di provider di identità](#).
- 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.

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

Il file `domain_krb.properties` determina i controller di dominio che vengono utilizzati per le directory in cui è abilitata la ricerca della posizione del servizio DNS (record SRV). Contiene un elenco dei controller di dominio relativi a ciascun dominio. Il connettore crea inizialmente il file e l'utente deve successivamente mantenerlo. Il file sovrascrive la ricerca della posizione del servizio DNS (SRV).

La ricerca della posizione del servizio DNS è abilitata nei seguenti tipi di directory.

- Active Directory su LDAP con l'opzione relativa al **supporto della posizione del servizio DNS da parte della directory** selezionata
- Active Directory (autenticazione integrata di Windows), dove la ricerca della posizione del servizio DNS è sempre abilitata

La prima volta che si crea una directory con la ricerca della posizione del servizio DNS abilitata, viene automaticamente creato un file `domain_krb.properties` nella directory `/usr/local/horizon/conf` della macchina virtuale e viene popolato in automatico con i controller di dominio relativi a ciascun dominio. Per popolare il file, il connettore tenta di trovare i controller di dominio che si trovano sullo stesso sito del connettore e ne seleziona due tra quelli raggiungibili e con la risposta più rapida.

Quando si creano ulteriori directory con la posizione del servizio DNS abilitata o si aggiungono nuovi domini a una directory Autenticazione integrata di Windows, i nuovi domini vengono aggiunti al file insieme a un elenco dei relativi controller di dominio.

È possibile sovrascrivere la selezione predefinita in qualsiasi momento modificando il file `domain_krb.properties`. Come procedura consigliata, visualizzare il file `domain_krb.properties` dopo aver creato una directory e verificare che i controller di dominio elencati siano ottimali per la configurazione. Per una distribuzione globale di Active Directory con più controller di dominio in diverse posizioni geografiche, l'utilizzo di un controller di dominio in prossimità del connettore garantisce una comunicazione più veloce con Active Directory.

In caso di altre modifiche, è necessario inoltre aggiornare manualmente il file. Sono valide le seguenti regole.

- Il file `domain_krb.properties` viene creato nella macchina virtuale che contiene il connettore. In una distribuzione tipica, senza altri connettori distribuiti, il file viene creato nella macchina virtuale del servizio di Directories Management. Se si sta utilizzando un connettore aggiuntivo per la directory, il file viene creato nella macchina virtuale del connettore. Una macchina virtuale può avere solo un file `domain_krb.properties`.
- La prima volta che viene creata una directory con la ricerca della posizione del servizio DNS abilitata, il file viene creato e popolato automaticamente con i controller di dominio relativi a ciascun dominio.
- I controller di dominio relativi a ciascun dominio sono elencati in ordine di priorità. Per collegarsi ad Active Directory, il connettore prova a utilizzare il primo controller di dominio dell'elenco. Se non è raggiungibile, prova con il secondo e così via.
- Il file viene aggiornato solo quando si crea una nuova directory con la ricerca della posizione del servizio DNS abilitata o quando si aggiunge un dominio a una directory Autenticazione integrata di Windows. Quando il nuovo dominio viene aggiunto al file insieme a un elenco dei relativi controller di dominio.

La voce corrispondente a un dominio, se esiste già nel file, non viene aggiornata. Ad esempio, se si crea una directory e poi la si elimina, la voce del dominio originale resta nel file e non viene aggiornata.

- In qualsiasi altro scenario, il file non viene aggiornato automaticamente. Ad esempio, eliminando una directory, la voce del dominio non viene eliminata dal file.
- Se il controller di un dominio elencato nel file non è raggiungibile, modificare il file e rimuoverlo.
- Se la voce di un dominio viene aggiunta o modificata manualmente, le modifiche non saranno sovrascritte.

Selezione dei controller di dominio per popolare automaticamente il file `domain_krb.properties`

Per popolare automaticamente il file `domain_krb.properties`, i controller di dominio vengono innanzitutto selezionati determinando la subnet in cui risiede il connettore (sulla base dell'indirizzo IP e della netmask); poi si utilizza la configurazione di Active Directory per identificare il sito della subnet, ottenendo l'elenco dei controller di dominio relativi al sito in questione; è necessario infine filtrare l'elenco a seconda del dominio adeguato e scegliere i due controller di dominio con la risposta più rapida.

I requisiti di VMware Identity Manager per rilevare i controller di dominio più vicini sono i seguenti.

- La subnet del connettore deve essere presente nella configurazione di Active Directory oppure è necessario specificare una subnet nel file `runtime-config.properties`.

La subnet viene utilizzata per determinare il sito.

- La configurazione di Active Directory deve disporre di informazioni sulla presenza del sito.

Se non è possibile determinare la subnet o se la configurazione di Active Directory non dispone di informazioni sulla presenza del sito, la ricerca della posizione del servizio DNS viene utilizzata per trovare i controller di dominio e il file viene popolato con alcuni controller di dominio raggiungibili. Questi controller di dominio potrebbero non trovarsi nella stessa posizione geografica del connettore e potrebbero di conseguenza verificarsi ritardi o timeout durante la comunicazione con Active Directory. In questo caso, modificare manualmente il file `domain_krb.properties` e specificare i controller di dominio corretti da utilizzare per ciascun dominio.

File `domain_krb.properties` di esempio

```
example.com=host1.example.com:389,host2.example.com:389
```

- [Sovrascrittura della selezione predefinita della subnet](#)

Per popolare automaticamente il file `domain_krb.properties`, il connettore tenta di trovare i controller di dominio che si trovano nello stesso sito, in modo che la latenza tra il connettore e Active Directory sia minima.

- [Modifica del file `domain_krb.properties`](#)

Il file `/usr/local/horizon/conf/domain_krb.properties` determina quali controller di dominio utilizzare per le directory che dispongono della ricerca della posizione del servizio DNS abilitata. È possibile modificare il file in qualsiasi momento per aggiornare l'elenco dei controller relativi a un dominio oppure per aggiungere o eliminare le voci di dominio. Le modifiche non saranno sovrascritte.

- [Risoluzione dei problemi relativi a `domain_krb.properties`](#)

Utilizzare queste informazioni per risolvere i problemi relativi al file `domain_krb.properties`.

Sovrascrittura della selezione predefinita della subnet

Per popolare automaticamente il file `domain_krb.properties`, il connettore tenta di trovare i controller di dominio che si trovano nello stesso sito, in modo che la latenza tra il connettore e Active Directory sia minima.

Per individuare il sito, il connettore determina la subnet in cui risiede sulla base del suo indirizzo IP e della netmask, quindi utilizza la configurazione di Active Directory per identificare il sito della subnet. Se la subnet della macchina virtuale non si trova in Active Directory oppure se si desidera sovrascrivere la selezione automatica della subnet, è possibile specificare una subnet nel file `runtime-config.properties`.

Procedura

- 1 Accedere alla macchina virtuale del di Directories Management come utente radice.

Nota: Se si sta utilizzando un connettore aggiuntivo per la directory, accedere alla macchina virtuale del connettore.

- 2 Modificare il file `/usr/local/horizon/conf/runtime-config.properties` e aggiungere il seguente attributo.

`siteaware.subnet.override=subnet`

dove *subnet* è una subnet del sito di cui l'utente desidera utilizzare i controller di dominio. Ad esempio:

`siteaware.subnet.override=10.100.0.0/20`

- 3 Salvare e chiudere il file.

- 4 Riavviare il servizio.

```
service horizon-workspace restart
```

Modifica del file `domain_krb.properties`

Il file `/usr/local/horizon/conf/domain_krb.properties` determina quali controller di dominio utilizzare per le directory che dispongono della ricerca della posizione del servizio DNS abilitata. È possibile modificare il file in qualsiasi momento per aggiornare l'elenco dei controller relativi a un dominio oppure per aggiungere o eliminare le voci di dominio. Le modifiche non saranno sovrascritte.

Il connettore crea inizialmente il file e lo popola automaticamente. In alcuni scenari, è necessario aggiornarlo manualmente.

- Se i controller di dominio selezionati per impostazione predefinita non sono ottimali per la configurazione dell'utente, modificare il file e specificare i controller di dominio da utilizzare.
- Se una directory viene eliminata, eliminare dal file la voce di dominio corrispondente.
- Se alcuni controller di dominio presenti nel file non sono raggiungibili, rimuoverli dal file.

Vedere anche [Informazioni sulla selezione dei controller di dominio](#).

Procedura

- 1 Accedere alla macchina virtuale del di Directories Management come utente radice.

Nota: Se si sta utilizzando un connettore aggiuntivo per la directory, accedere alla macchina virtuale del connettore.

- 2 Modificare le directory in `/usr/local/horizon/conf`.

- 3 Modificare il file `domain_krb.properties` per aggiungere o aggiornare l'elenco dei valori da dominio a host.

Utilizzare il seguente formato:

dominio=host:porta,host2:porta,host3:porta

Ad esempio:

`example.com=examplehost1.example.com:389,examplehost2.example.com:389`

Elencare i controller di dominio in ordine di priorità. Per collegarsi ad Active Directory, il connettore prova a utilizzare il primo controller di dominio dell'elenco. Se non è raggiungibile, prova con il secondo e così via.

Importante: I nomi dei domini devono essere in minuscolo.

- 4 Modificare il proprietario del file `domain_krb.properties` in horizon e il gruppo in www attraverso il seguente comando:

`chown horizon:www /usr/local/horizon/conf/domain_krb.properties`

- 5 Riavviare il servizio.

`service horizon-workspace restart`

Risoluzione dei problemi relativi a `domain_krb.properties`

Utilizzare queste informazioni per risolvere i problemi relativi al file `domain_krb.properties`.

Errore di risoluzione del dominio

Se il file `domain_krb.properties` include già una voce di dominio e si cerca di creare una nuova directory per un tipo diverso dello stesso dominio, viene visualizzato un errore di risoluzione del dominio. È necessario modificare il file `domain_krb.properties` e rimuovere manualmente la voce di dominio prima di creare la nuova directory.

I controller di dominio non sono raggiungibili

Una volta aggiunta la voce di dominio al file `domain_krb.properties`, questo non viene aggiornato automaticamente. Se uno dei controller di dominio elencati nel file non è raggiungibile, modificare il file manualmente e rimuoverlo.

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.

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 inizino 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.

* 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, l'intervallo di tempo, i metodi e l'ordine di autenticazione e il numero massimo di ore per cui gli utenti possono utilizzare l'applicazione.

	Intervallo di rete	Tipo di dispositivo	Metodo di autenticazione
☰	TUTTI GLI INTERVALLI	Browser Web	Password
☰	TUTTI GLI INTERVALLI	Applicazione client Identity Manager	Password

- 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.


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*

Sensitive Web Application

Descrizione

To be applied to Web application that should have limited access

Applicabile a

Selezionare nel catalogo le applicazioni per cui questo criterio è valido.

AirWatch
Content Locker

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 un'istanza di provider di identità](#).
- 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 alla console 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**.

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 Management connettore, 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.

Tavola 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.

Tavola 2-8. Tipi di autenticazione utente supportati da Gestione directory (Continua)

Tipi di autenticazione	Descrizione
Certificato (distribuzione in loco)	È possibile configurare l'autenticazione basata su certificato per consentire ai clienti di autenticarsi con i certificati sul desktop e sui dispositivi mobili o di utilizzare una scheda smart card per l'autenticazione. 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.
RSA SecurID (distribuzione in loco)	Quando si configura l'autenticazione RSA SecurID, Directories Management viene configurato come agente di autenticazione nel server RSA SecurID. 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.
RADIUS (distribuzione in loco)	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.
Autenticazione adattiva RSA (distribuzione in loco)	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.
Mobile SSO (per iOS)	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.
Mobile SSO (per Android)	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.
Password (AirWatch Connector)	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.

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.

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 come agente di autenticazione con informazioni sull'appliance Directories Management. 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 come agente di autenticazione con informazioni sull'appliance Directories Management. 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 Su una versione supportata del server RSA SecurID, aggiungere il connettore Directories Management 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.

Passi successivi

Passare alla console di amministrazione e nelle pagine Impostazione della scheda Gestione accesso e identità selezionare il connettore, quindi nella pagina AuthAdapters configurare SecurID.

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 SecurIDIdpAdapter, ma è possibile modificarlo.
Abilita SecurID	Selezionare questa casella per abilitare l'autenticazione SecurID.
Numero di tentativi di autenticazione e 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.

Opzione	Azione
Configurazione e 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**.

Passi successivi

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 alla console 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 e 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.
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 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**.

Passi successivi

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 una scheda smart card da utilizzare con Directories Management

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 dei certificati locale sono disponibili per tutti i browser in esecuzione sul computer dell'utente, con alcune eccezioni, e quindi anche per un'istanza di Directories Management nel browser.

- [Uso del nome dell'entità utente per l'autenticazione del 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 provano ad autenticarsi nel servizio Directories Management devono disporre di un nome UPN valido corrispondente al nome UPN del certificato.

- [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.

- [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.

- [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.

Uso del nome dell'entità utente per l'autenticazione del 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 provano ad autenticarsi nel servizio Directories Management devono disporre di un nome UPN valido corrispondente al nome UPN del certificato.

È possibile configurare il 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.

Prerequisiti

- Ottenere il certificato radice e i certificati intermedi dall'autorità di certificazione che ha firmato i certificati presentati dagli utenti.
- (Facoltativo) Un elenco degli identificatori di oggetto (OID) dei criteri di certificato validi per l'autenticazione dei certificati.
- Per il controllo della revoca, la posizione del file dell'elenco di revoche di certificati e l'URL del server OCSP.
- (Facoltativo) La posizione del file del certificato Firma risposta OCSP.
- Contenuto del modulo di consenso, se è richiesto 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 Configurare la pagina Scheda di autenticazione certificato.

Nota: Un asterisco indica che l'informazione è obbligatoria.

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	I file di certificato caricati sono elencati nella sezione Certificati autorità di certificazione caricati del modulo.
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	Creare un elenco di identificatori di oggetto accettati nelle estensioni dei criteri di certificato. 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.
Abilita revoca certificato	Selezionare la casella di controllo per abilitare il controllo della revoca del certificato. Il controllo della revoca del certificato impedisce l'autenticazione degli utenti che hanno certificati revocati.
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 configura sia CRL che OCSP. Si seleziona questa casella di controllo per utilizzare 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.

5 Fare clic su **Salva**.

Passi successivi

- 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 un'istanza di provider di identità

vRealize Automation viene fornito con un'istanza di provider di identità predefinita. Gli utenti possono tuttavia creare istanze di provider di identità aggiuntive.

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 tuttavia 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.

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 alla console vRealize Automation come **amministratore tenant**.

Procedura

1 Passare ad **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** e modificare le impostazioni dell'istanza del provider di identità.

Elemento del modulo	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.
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.

3 Fare clic su **Aggiungi**.

Passi successivi

- 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 alla console 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.

Passi successivi

- 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**.

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 aprire una pagina delle regole dei criteri, fare clic sul nome di autenticazione nella colonna del metodo di autenticazione oppure, per aggiungere una nuova regola per il criterio, fare clic sull'icona **+**.
 - a Verificare che l'intervallo di rete sia corretto. Se si aggiunge una nuova regola, selezionare l'intervallo di rete per tale regola del criterio.
 - b Selezionare il tipo di dispositivo che sarà gestito dalla regola dal menu a discesa **e l'utente tenta di accedere ai contenuti da**.
 - c Configurare l'ordine di autenticazione. Nel menu a discesa **quindi l'utente deve autenticarsi utilizzando il metodo seguente**, selezionare il metodo di autenticazione da applicare per primo.
Per richiedere agli utenti di autenticarsi usando due metodi di autenticazione, fare clic su **+** e aggiungere un secondo metodo di autenticazione.
 - d (Facoltativo) Per configurare altri metodi di autenticazione in caso di esito negativo della prima autenticazione, selezionare un altro metodo di autenticazione abilitato dal menu a discesa successivo.
È possibile aggiungere più metodi di autenticazione di fallback a una regola.
 - e Nella casella di testo del valore **Ripeti autenticazione dopo**, immettere il numero di ore dopo le quali gli utenti dovranno eseguire di nuovo l'autenticazione.
 - f (Facoltativo) Creare un messaggio di accesso negato che viene visualizzato quando l'autenticazione dell'utente non riesce. È possibile utilizzare fino a 4000 caratteri, che corrispondono all'incirca a 650 parole. Se si desidera indirizzare gli utenti a un'altra pagina, aggiungere il collegamento dell'URL nella casella di testo **URL collegamento**). Nella casella di testo **Testo collegamento**, immettere il testo visualizzato per il collegamento. Se si lascia vuoto questo campo, viene visualizzata la parola Continua.
 - g Fare clic su **Salva**.

4 Fare clic su **Salva**.

Modifica regola del criterio

Se l'intervallo di rete di un utente è... TUTTI GLI INTERVALLI

e l'utente tenta di accedere a contenuti da... Browser Web

l'utente deve autenticarsi utilizzando il seguente metodo...

Password e

Se il precedente metodo di autenticazione non va a buon fine:

-Seleziona metodo di autenticazione- solo

+ Metodi di fallback:

Nuova autenticazione dopo: 8 ore

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.

Procedura

- 1 In qualità di amministratore del tenant, passare ad **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 e 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**.

Passi successivi

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 Kerberos alla regola nell'ordine di autenticazione corretto.

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.

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.

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.

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.

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 vRealize Automation appliance include un connettore che supporta l'autenticazione utente, sebbene 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 vRealize Automation appliance, si connetta al provider di identità e punti alla stessa 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 7.1*.
- Accedere alla console 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 vRealize Automation appliance contiene 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 .
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 al vRealize Automation appliance secondario.
- 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.

È stata effettuata la connessione dell'Active Directory aziendale a vRealize Automation ed è stato configurato Gestione directory per l'alta disponibilità.

Passi successivi

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 dell'autenticazione smart card per vRealize Automation

Come amministratore di sistema, è necessario configurare l'autenticazione smart card per la distribuzione di vRealize Automation mediante Gestione directory.

Gestione directory supporta più provider di identità e cluster di connettori per ciascun Active Directory configurato. Per utilizzare l'autenticazione smart card, 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.

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 una scheda smart card da utilizzare con Directories Management](#).

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 alla console 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 alla console vRealize Automation come **amministratore tenant**.

Procedura

1 Selezionare **Amministrazione > Gestione directory > Connettori**.

2 Nella casella di testo relativa al **nome dell'ID del connettore**, digitare un nome per il nuovo connettore.

3 Premere **Invio**.

Nella casella del **codice di attivazione del connettore**, viene visualizzato il codice di attivazione relativo al connettore.

4 Copiare il codice di attivazione da utilizzare durante la configurazione del connettore mediante il file OVA.

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.
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.

Pagina	Descrizione
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> <hr/> <p>Importante: Se uno dei quattro campi relativi agli indirizzi viene lasciato vuoto, incluso Nome host, viene utilizzato il DHCP.</p> <hr/> <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.

Passi successivi

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

- 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	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. Importante: La password dell'utente admin deve essere di almeno 6 caratteri.
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 necessario immettere anche le informazioni relative al **certificato di un'autorità di certificazione radice**.

È possibile ottenere l'autorità di certificazione radice da <https://:8443/cfg/ssl>. 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.

Passi successivi

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.

Nota: Se sceglie un bilanciamento del carico per il Directories Management, il certificato SSL viene applicato al bilanciamento del carico.

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:
`Https://myconnector.mycompany:8443/cfg`
- 2 Nella console di amministrazione, fare clic sulle **impostazioni dell'appliance**.

La configurazione dell'appliance virtuale viene selezionata per impostazione predefinita.
- 3 Fare clic su **Gestisci configurazione**.
- 4 Nella finestra di dialogo visualizzata, immettere la password dell'utente amministratore per il server di Directories Management.
- 5 Selezionare l'opzione per **installare il certificato**.
- 6 Nella scheda per terminare l'SSL nell'Identity Manager Appliance, selezionare il pulsante per **personalizzare il certificato**.
- 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+C3HU17bUOvwHP/r0+
```

```
...
```

```
...
```

```
...
```

```
W53+O05j5xsxzDJfWr1IqBiff/OkIYCPcyK1
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```


Esempio di catena di certificati

```
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjQvt90+
```

```
...
```

```
...
```

```
...
```

```
O05j5xsxzDjFwr1lqBIFF/OkIYCPW53+cyK1
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

```
dR9Vpg3WQTjQvt9W5+C3HU17bUOwvhp/r0+
```

```
...
```

```
...
```

```
...
```

```
5j5xsxzDjFwr1lqW53+O0BIFF/OkIYCPcyK1
```

```
-----END CERTIFICATE-----
```

Esempio di chiave privata

```
-----BEGIN RSA PRIVATE KEY-----
```

```
jQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+
```

```
...
```

```
...
```

```
...
```

```
1lqBIFFW53+O05j5xsxzDjFwr/OkIYCPcyK1
```

```
-----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 alla console vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Gestione directory > Provider di identità**.
- 2 Selezionare **Aggiungi provider di identità**.
- 3 Selezionare l'opzione per **creare l'IDP dell'area di lavoro** nel menu visualizzato.
- 4 Digitare 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 visualizzare per la selezione con questo 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 per accedere a questo 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 alla console 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 7.1*.
- Accedere alla console 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 vRealize Automation appliance 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.

Passi successivi

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 e gruppi.

Prerequisiti

Accedere alla console 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 Fare clic su **Aggiorna**.

Gli utenti che sono attualmente connessi alla console di vRealize Automation devono disconnettersi e riaccedere alla console di vRealize Automation prima di poter visualizzare le pagine per cui hanno ricevuto le autorizzazioni di accesso.

Passi successivi

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.

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 alla console vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Utenti e gruppi > Gruppi personalizzati**.
- 2 Fare clic sull'icona **Aggiungi** (+).
- 3 Specificare il nome del gruppo nella casella di testo **Nome nuovo gruppo**.
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 nuovo gruppo**.
- 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 **Aggiungi**.

Gli utenti che sono attualmente connessi alla console di vRealize Automation devono disconnettersi e riaccedere alla console di vRealize Automation prima di poter visualizzare le pagine per cui hanno ricevuto le autorizzazioni di accesso.

Creazione di un gruppo di business

I gruppi di business sono utilizzati per associare un insieme di servizi e di risorse a un gruppo di utenti spesso corrispondente a una linea di business, un reparto o a un'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 alla console 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 da anteporre ai nomi delle macchine con provisioning eseguito da un membro del gruppo di business, richiedere un prefisso macchina da 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 manager a	Immettere uno o più nomi di utente o di gruppo. Separare più voci con una virgola. Ad esempio <code>JoeAdmin@mycompany.com,WeiMgr@mycompany.com</code> .
Criterio di Active Directory	Selezionare il criterio di Active Directory predefinito per il gruppo di business.

- 4 Aggiungere proprietà personalizzate.

- 5 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. In questa fase non è strettamente necessario specificare gli utenti. È possibile 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.
Ruolo utente	Può richiedere elementi del catalogo dei servizi per cui è autorizzato.

- 6 Fare clic su **Avanti**.
- 7 Configurare le opzioni dell'infrastruttura predefinita.

Opzione	Descrizione
Prefisso macchina predefinito	<p>Selezionare un prefisso macchina preconfigurato per il gruppo di business.</p> <p>Il prefisso è utilizzato dai blueprint delle macchine. Se il blueprint è configurato per utilizzare il prefisso predefinito e in questo campo non viene specificato il valore predefinito, il sistema crea automaticamente un prefisso predefinito 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>

- 8 Fare clic su **Aggiungi**.

Gli amministratori di struttura 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.

Passi successivi

- 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 correlati a dati mancanti dei gruppi di business

Mancano gruppi di business o dati dai gruppi di business.

Problema

Quando si cercano gruppi di business conosciuti, il gruppo di business desiderato risulta mancante da **Amministrazione > Utenti e gruppi > Gruppi di business** o il gruppo di business non interagisce come previsto con prenotazioni o permessi.

Causa

Le informazioni sui gruppi di business sono conservate in due database, CAFE e IaaS, e devono essere uguali nei due database. Nel normale funzionamento, i database sono sempre sincronizzati. Nel caso in cui dovesse sorgere questo problema potrebbe essere necessario forzare una sincronizzazione.

Il problema può presentarsi dopo aver effettuato un aggiornamento ed è dovuto a una sincronizzazione non eseguita come previsto. Può inoltre presentarsi se si utilizza l'interfaccia API per aggiornare il database di IaaS con un gruppo di business nuovo o modificato.

Soluzione

Prerequisiti

Verificare di poter eseguire comandi dalla riga di comando. Vedere *Guida alla programmazione*.

Procedura

- ◆ Immettere la stringa di comando nella riga del comando vcac-cli.

Cosa viene aggiornato dal comando	Comando	Versione abbreviata del comando
Sincronizzazione del database CAFE con i valori del database IaaS.	Vcac-Config.exe SynchronizeDatabases -- DatabaseSyncSource IaaS -v	Vcac-Config.exe SynchronizeDatabases -dss IaaS -v
Sincronizzazione del database IaaS con i valori del database CAFE.	Vcac-Config.exe SynchronizeDatabases -- DatabaseSyncSource Cafe -v	Vcac-Config.exe SynchronizeDatabases -dss Cafe -v

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 utenti, il caricamento dei nomi degli utenti nell'interfaccia è particolarmente lenta.

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.

Scenario: configurazione del tenant predefinito per Rainpole

Si supponga che un amministratore di sistema desideri configurare l'istanza vRealize Automation come ambiente di sviluppo continuo. Creerà account utente locali e assegnerà a se stesso il ruolo di amministratore tenant. Utilizzando i privilegi di amministratore tenant, inizierà a configurare vRealize Automation come ambiente di sviluppo per creare e collaudare blueprint.



Procedura

1 Scenario: creazione degli account utente locali per Rainpole

Utilizzando i privilegi di amministratore di sistema predefiniti, creare due account utente locali nel tenant predefinito. Assegnare uno di questi account al ruolo di amministratore tenant così da poter iniziare la configurazione del tenant predefinito. È possibile utilizzare il secondo account in un momento successivo come accesso condiviso per consentire agli architetti di testare il blueprint e l'accesso al catalogo.

2 Scenario: connessione di Active Directory aziendale a vRealize Automation per Rainpole

Si supponga che un amministratore tenant voglia che vRealize Automation autentichi gli accessi con l'Active Directory aziendale. Configurerà la connessione tra vRealize Automation e Active Directory a dominio singolo su LDAP.

3 Scenario: configurazione del branding per il tenant predefinito per Rainpole

Utilizzando i privilegi di amministratore tenant, è possibile personalizzare l'aspetto della console di vRealize Automation. È possibile caricare un nuovo logo, cambiare i colori, aggiornare le informazioni contenute in intestazione e piè di pagina e configurare il branding della schermata di accesso.

4 Scenario: creazione di un gruppo personalizzato per gli architetti Rainpole

Utilizzando i privilegi di amministratore tenant, è possibile creare un gruppo personalizzato per i membri dell'organizzazione IT che richiedono un accesso privilegiato a vRealize Automation. I ruoli a questo gruppo personalizzato vanno assegnati mentre si configura vRealize Automation.

5 Scenario: assegnazione di privilegi di amministratore IaaS al gruppo personalizzato di architetti Rainpole

Utilizzando i privilegi di amministratore di sistema predefiniti, assegnare il gruppo personalizzato al ruolo di amministratore IaaS per consentirgli di configurare le risorse IaaS.

Scenario: creazione degli account utente locali per Rainpole

Utilizzando i privilegi di amministratore di sistema predefiniti, creare due account utente locali nel tenant predefinito. Assegnare uno di questi account al ruolo di amministratore tenant così da poter iniziare la configurazione del tenant predefinito. È possibile utilizzare il secondo account in un momento successivo come accesso condiviso per consentire agli architetti di testare il blueprint e l'accesso al catalogo.

Procedura

- 1 Passare alla console di vRealize Automation, <https://vra01svr01.rainpole.local/vcac>.
- 2 Inserire il nome utente dell'amministratore di sistema predefinito **administrator** e la password **VMware1!**.
- 3 Selezionare **Amministrazione > Tenant**.
- 4 Fare clic su **vsphere.local**.
- 5 Selezionare la scheda **Utenti locali**.
- 6 Fare clic sull'icona **Nuovo** (+).
- 7 Creare un account utente locale da assegnare al ruolo di amministratore tenant.

Opzione	Input
Nome	Rainpole
Cognome	tenant admin
Email	Immettere l'indirizzo e-mail o utilizzare il segnaposto rainpole_tenant_admin@rainpole.com .
Nome utente	Rainpole tenant admin
Password	VMware1!

- 8 Fare clic su **OK**.
- 9 Fare clic sull'icona **Nuovo** (+).
- 10 Creare un account utente locale che anche gli architetti possano successivamente configurare per testare i blueprint e l'accesso al catalogo.

Opzione	Input
Nome	test
Cognome	user
Email	Immettere l'indirizzo e-mail o utilizzare il segnaposto test_user@rainpole.com .

Opzione	Input
Nome utente	test_user
Password	VMware1!

- 11 Fare clic su **OK**.
- 12 Fare clic sulla scheda **Amministratori**.
- 13 Immettere **Rainpole** nella casella di ricerca **Amministratori tenant** e premere Invio. Selezionare l'utente amministratore tenant Rainpole.

Il ruolo di amministratore utente è assegnato all'utente amministratore tenant.

- 14 Fare clic su **Fine**.
- 15 Uscire dalla console.

È possibile utilizzare l'utente locale amministratore tenant Rainpole per accedere alle impostazioni di amministrazione tenant e configurare il tenant. L'account test_user è utile come accesso condiviso per architetti e amministratori di catalogo. Questi possono configurare l'account come utente di base, verificare il blueprint e l'accesso al catalogo e testare i comportamenti di approvazione.

Passi successivi

Configurare vRealize Automation per autenticare gli accessi con l'Active Directory aziendale esistente.

Scenario: connessione di Active Directory aziendale a vRealize Automation per Rainpole

Si supponga che un amministratore tenant voglia che vRealize Automation autentichi gli accessi con l'Active Directory aziendale. Configurerà la connessione tra vRealize Automation e Active Directory a dominio singolo su LDAP.

Procedura

- 1 Passare alla console di vRealize Automation, <https://vra01svr01.rainpole.local/vcac>.
- 2 Immettere il nome utente **Rainpole tenant admin** e la password **VMware1!**
- 3 Selezionare **Amministrazione > Gestione directory > Directory**.
- 4 Fare clic su **Aggiungi directory**.
- 5 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 sincronizzazione	vra01svr01.rainpole.local
DN di base	Immettere il DN (Distinguished Name) del punto di inizio per le ricerche nel server della directory. Ad esempio cn=users,dc=rainpole,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=rainpole,dc=local .
Password DN di binding	Immettere la password di Active Directory per l'account che può effettuare la ricerca di utenti.

- 6 Fare clic sul pulsante **Prova connessione** per verificare la connessione alla directory configurata.
- 7 Fare clic su **Salva e avanti**.
Verrà visualizzata la pagina Scegli i domini con l'elenco dei domini.
- 8 Accettare l'impostazione del dominio predefinito e fare clic su **Avanti**.
- 9 Verificare che i nomi di attributo siano mappati agli attributi di Active Directory corretti e fare clic su **Avanti**.
- 10 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=rainpole,dc=local**.
 - c Selezionare la casella di controllo **Seleziona tutto**.
 - d Fare clic su **Seleziona**.
 - e Fare clic su **Avanti**.
 - f Accettare i valori predefiniti nella pagina di selezione degli utenti e fare clic su **Avanti**.
- 11 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.

È possibile assegnare privilegi e consentire l'accesso a qualsiasi utente e gruppo Active Directory sincronizzato a vRealize Automation.

Passi successivi

Utilizzando i privilegi di amministratore tenant, personalizzare l'aspetto della console di vRealize Automation.

Scenario: configurazione del branding per il tenant predefinito per Rainpole

Utilizzando i privilegi di amministratore tenant, è possibile personalizzare l'aspetto della console di vRealize Automation. È possibile caricare un nuovo logo, cambiare i colori, aggiornare le informazioni contenute in intestazione e piè di pagina e configurare il branding della schermata di accesso.

Procedura

- 1 Selezionare **Amministrazione > Branding > Branding intestazione e piè di pagina**.
- 2 Deselezionare la casella di controllo **Utilizza predefinito**.
- 3 Seguire le istruzioni per creare un'intestazione.
- 4 Fare clic su **Avanti**.
- 5 Seguire le istruzioni per creare un piè di pagina.
- 6 Fare clic su **Fine**.

La console viene aggiornata con le modifiche.

- 7 Selezionare **Amministrazione > Branding > Branding schermata di accesso**.
- 8 Seguire le istruzioni per personalizzare il branding della schermata di accesso.
- 9 Fare clic su **Salva**.

La console viene aggiornata con le modifiche.

In questo modo l'aspetto della console del tenant predefinito è stato modificato.

Passi successivi

Creare un gruppo personalizzato per i membri dell'organizzazione IT che richiedono un accesso privilegiato a vRealize Automation.

Scenario: creazione di un gruppo personalizzato per gli architetti Rainpole

Utilizzando i privilegi di amministratore tenant, è possibile creare un gruppo personalizzato per i membri dell'organizzazione IT che richiedono un accesso privilegiato a vRealize Automation. I ruoli a questo gruppo personalizzato vanno assegnati mentre si configura vRealize Automation.

Se si desidera aggiungere o disabilitare l'accesso di alto livello per gli utenti, è possibile modificare l'appartenenza del gruppo anziché modificare le impostazioni per ogni utente in più posizioni.

Procedura

- 1 Selezionare **Amministrazione > Utenti e gruppi > Gruppi personalizzati**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere **Rainpole architects** nella casella di testo **Nome**.

- 4 Selezionare i ruoli dall'elenco Aggiungi ruoli a questo gruppo.

Non è possibile assegnare i ruoli utente amministratore IaaS, amministratore struttura, manager gruppo di business o utente business in questa pagina. È possibile assegnare questi ruoli mentre si configura vRealize Automation.

Opzione	Descrizione
Amministratore tenant	Responsabili della gestione dei gruppi e degli utenti, delle notifiche e del branding dei tenant e dei criteri di business quali approvazioni e permessi. Inoltre, essi tengono traccia dell'uso delle risorse da parte di tutti gli utenti all'interno del tenant e avviano le richieste di recupero per le macchine virtuali.
Architetto IaaS	Crea e gestisce i blueprint delle macchine e i blueprint delle applicazioni.
Architetto XaaS	Per utenti con licenza Advanced ed Enterprise, crea e gestisce i blueprint XaaS.
Architetto del software	Per utenti con licenza Enterprise, crea e gestisce i componenti software e i blueprint delle applicazioni.

- 5 Fare clic su **Avanti**.

- 6 Cercare gli utenti Active Directory aziendali e selezionare gli utenti da aggiungere al gruppo personalizzato.

Assegnare a questo gruppo sé stessi e chiunque richieda un livello estremamente elevato di accesso all'ambiente di sviluppo vRealize Automation.

- 7 Fare clic su **Fine**.

In questo modo si concederà al gruppo personalizzato i diritti di gestire il tenant predefinito, creare blueprint e gestire il catalogo di servizi. Mentre si configura vRealize Automation, è possibile aggiungere permessi e ruoli al gruppo personalizzato.

Passi successivi

Assegnare il gruppo personalizzato al ruolo di amministratore IaaS.

Scenario: assegnazione di privilegi di amministratore IaaS al gruppo personalizzato di architetti Rainpole

Utilizzando i privilegi di amministratore di sistema predefiniti, assegnare il gruppo personalizzato al ruolo di amministratore IaaS per consentirgli di configurare le risorse IaaS.

Procedura

- 1 Disconnettersi dalla console di vRealize Automation.
- 2 Selezionare il dominio **vsphere.local** e fare clic su **Avanti**.
- 3 Inserire il nome utente dell'amministratore di sistema predefinito **administrator** e la password **vmware**.
- 4 Selezionare **Amministrazione > Tenant**.
- 5 Fare clic sul nome del tenant predefinito **vsphere.local**.

- 6 Fare clic sulla scheda **Amministratori**.
- 7 Cercare gli **architetti Rainpole** nella casella di ricerca **Amministratori IaaS** e selezionare il gruppo personalizzato.
- 8 Fare clic su **Fine**.
- 9 Uscire dalla console.

Qualsiasi membro del gruppo personalizzato ora potrà gestire l'infrastruttura cloud, di rete e di storage per tutti i tenant dell'istanza di vRealize Automation. È possibile aggiornare l'appartenenza dei membri al gruppo in qualsiasi momento per concedere o revocare tali privilegi.

Passi successivi

Utilizzando i privilegi di amministratore IaaS concessi al gruppo personalizzato è possibile configurare le risorse IaaS.

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 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 Configurazione di utenti locali

L'amministratore di sistema di vRealize Automation deve configurare utenti locali per ciascun tenant applicabile.

3 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.

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 7.1*.

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**.

Il tenant viene eliminato dalla distribuzione di vRealize Automation.

(Facoltativo) 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 le caselle di controllo relative agli effetti visivi desiderati sotto l'intestazione **Effetti**.
Tutti gli effetti sono facoltativi.
- 4 Selezionare **Branding > Branding schermata di accesso**.
- 5 Fare clic su **Carica** sotto al campo Logo, individuare la cartella in cui si trova il file immagine del logo e selezionare il file.
- 6 Fare clic su **Carica** sotto al campo Immagine (facoltativo), individuare la cartella in cui si trova il file immagine aggiuntivo e selezionare il file.
- 7 Se desiderato, immettere i codici esadecimali dei colori 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.
- 8 Fare clic su **Salva** per applicare le impostazioni.

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**.

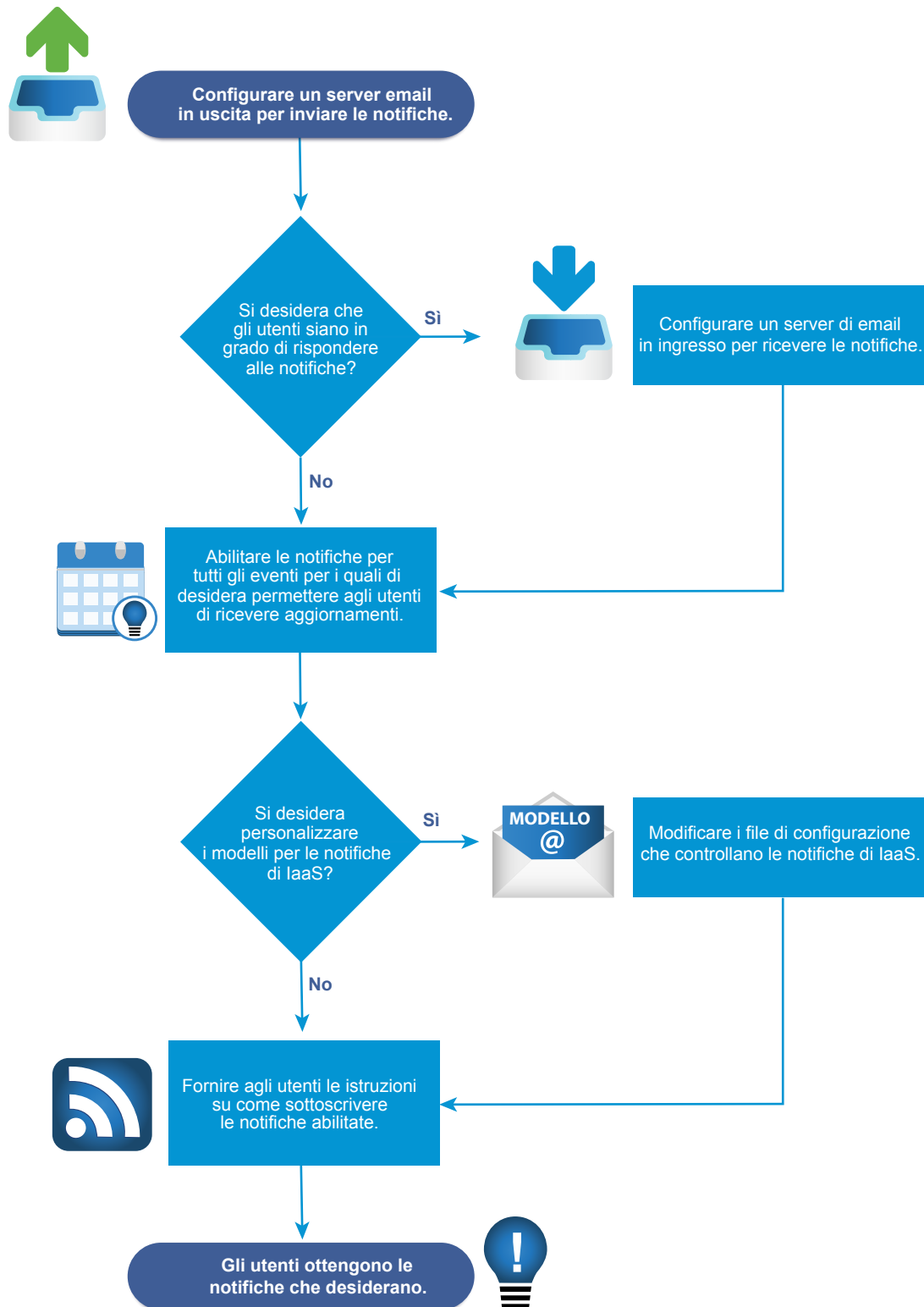
i Immettere nel campo **Collegamento ai contatti** le informazioni di contatto dell'azienda che si desidera mostrare.

7 Fare clic su **Aggiorna** per implementare la configurazione del branding.

Gli utenti del tenant vedranno il branding personalizzato nelle loro pagine dell'applicazione.

(Facoltativo) 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.

Tavola 2-9. 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"/> 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 .

Tavola 2-9. 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 \Temp\ates sotto la directory d'installazione del server di vRealize Automation (generalmente %SystemDrive%\Programmi (x86)\VMware\vCA C\Server) può configurare i modelli di queste notifiche via email.	Vedere Configurazione dei modelli per le email automatiche di IaaS .
<input type="checkbox"/> 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 alla console 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 alla console 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 alla console 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 alla console 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 alla console 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 alla console 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**.

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
```

Passi successivi

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 della Knowledge Base:

- [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 le notifiche, è possibile iscriversi per ricevere notifiche da vRealize Automation. Gli eventi notificati possono includere il corretto completamento di una richiesta di catalogo o di un'approvazione richiesta.

Prerequisiti

Effettuare l'accesso alla console di 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**.

(Facoltativo) 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\Website\Rdp`.

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](#).

(Facoltativo) 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.



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.

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](#).

Configurazione di vRealize Orchestrator e dei plug-in

VMware vRealize™ Orchestrator™ è un motore di automazione e gestione che apporta funzionalità a vRealize Automation, aggiungendo il supporto per XaaS e altre estendibilità.

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.

Privilegi di configurazione

Gli amministratori di sistema e tenant possono configurare vRealize Automation per l'uso di un server vRealize Orchestrator esterno.

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 della cartella di workflow predefinita per un tenant

Gli amministratori di sistema possono raggruppare i workflow in cartelle differenti e quindi definire categorie di workflow per tenant. Facendo in questo modo, un amministratore di sistema può concedere agli utenti provenienti da tenant diversi l'accesso alle diverse cartelle di workflow sullo stesso server vRealize Orchestrator.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore di sistema**.

Procedura

- 1 Selezionare **Amministrazione > Servizi avanzati > Cartella vRO predefinita**.
- 2 Fare clic sul nome del tenant da modificare.
- 3 Sfogliare la libreria di workflow di vRealize Orchestrator e selezionare una cartella.
- 4 Fare clic su **Aggiungi**.

La cartella di workflow di vRealize Orchestrator predefinita per un tenant è stata definita.

Passi successivi

Ripetere la procedura per tutti i tenant per cui si desidera definire una cartella di workflow predefinita.

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 avere le 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 dotato delle autorizzazioni di visualizzazione ed esecuzione o membro del gruppo vcoadmins.

Prerequisiti

- Installare e configurare un server vRealize Orchestrator esterno. È anche possibile distribuire vRealize Orchestrator Appliance. Vedere *Installazione e configurazione di VMware vCenter 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**.
- 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 **Aggiorna**.

La connessione al server vRealize Orchestrator esterno è stata configurata e la cartella dei workflow **vCAC** e le azioni di utilità correlate vengono automaticamente importate. La cartella dei workflow **vCAC > ASD** contiene i workflow per configurare gli endpoint e creare le mappature delle risorse.

Passi successivi

Configurare i plug-in di vRealize Orchestrator come endpoint. Vedere [Configurazione delle risorse XaaS](#).

Accesso all'interfaccia di configurazione di vRealize Orchestrator

Per modificare la configurazione dell'istanza vRealize Orchestrator predefinita incorporata in vRealize Automation, è necessario avviare il servizio di configurazione di vRealize Orchestrator e accedere all'interfaccia di configurazione di vRealize Orchestrator.

Per impostazione predefinita, il servizio di configurazione di vRealize Orchestrator non viene avviato nell'appliance di vRealize Automation. È necessario avviare il servizio di configurazione di vRealize Orchestrator per accedere all'interfaccia di configurazione di vRealize Orchestrator.

Procedura

- 1 Avviare il servizio vRealize Orchestrator Configuration.
 - a Accedere alla console Linux della vRealize Automation appliance come utente root.
 - b Immettere **service vco-configurator start** e premere Invio.
- 2 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, <https://vra-virtual-hostname.domain.name>.
- 3 Fare clic su **vRealize Orchestrator Control Center**.
Si viene reindirizzati a <https://vra-virtual-hostname.domain.name:8283/vco-controlcenter>.
- 4 Accedere a vRealize Orchestrator Control Center.
Il nome utente viene configurato dall'amministratore di vRealize Automation appliance.
- 5 (Facoltativo) Se questo è il primo accesso, cambiare la password predefinita e fare clic su **Applica modifiche**.
La nuova password deve essere lunga almeno otto caratteri e deve contenere almeno un numero, un carattere speciale e una lettera maiuscola.

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 Accedere alla console di gestione della vRealize Automation appliance utilizzando il suo nome di dominio completo, <https://vra-virtual-hostname.domain.name>.
- 2 Fare clic su **vRealize Orchestrator Client**.
Il file del client è stato scaricato.
- 3 Fare clic sul download e seguire le istruzioni visualizzate.

- 4 Nella pagina di accesso di vRealize Orchestrator, immettere l'indirizzo IP o il nome di dominio di vRealize Automation appliance nella casella di testo **Nome host** e **443** come numero di porta predefinito.

Ad esempio immettere `vrealize_automation_appliance_ip:443`.

- 5 Accedere utilizzando il nome utente e la password del client di vRealize Orchestrator.

Le credenziali corrispondono al nome utente e alla password dell'amministratore tenant predefinito.

- 6 Nella finestra **Avviso certificato**, 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 certificato viene visualizzato ogni volta che ci si connette al server di vRealize Orchestrator.

Opzione	Descrizione
Ignora	Continua utilizzando il certificato SSL corrente. Il messaggio di avviso ricompare alla successiva connessione allo stesso server di vRealize Orchestrator o quando si tenta di sincronizzare un workflow con un server Orchestrator remoto.
Annulla	Chiude la finestra e interrompe il processo di accesso.
Installa il certificato e non visualizzare più i messaggi di sicurezza a esso relativi.	Selezionare questa casella di controllo e fare clic su Ignora per installare il certificato e interrompere la visualizzazione degli avvisi di sicurezza.

È possibile sostituire il certificato SSL predefinito con un certificato firmato da un'autorità di certificazione. Per informazioni sul cambio dei certificati SSL, vedere *Installazione e configurazione di VMware vRealize Orchestrator*.

Passi successivi

È possibile importare un pacchetto, sviluppare workflow o impostare diritti di accesso root sul sistema. Vedere *Utilizzo del client di VMware vRealize Orchestrator* e *Sviluppare con VMware 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.

Questo capitolo include i seguenti argomenti:

- [Elenco di controllo per la configurazione di risorse di IaaS](#)
- [Configurazione delle risorse XaaS](#)
- [Installazione di plug-in aggiuntivi sul server vRealize Orchestrator predefinito](#)
- [Utilizzo dei criteri di Active Directory](#)

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.

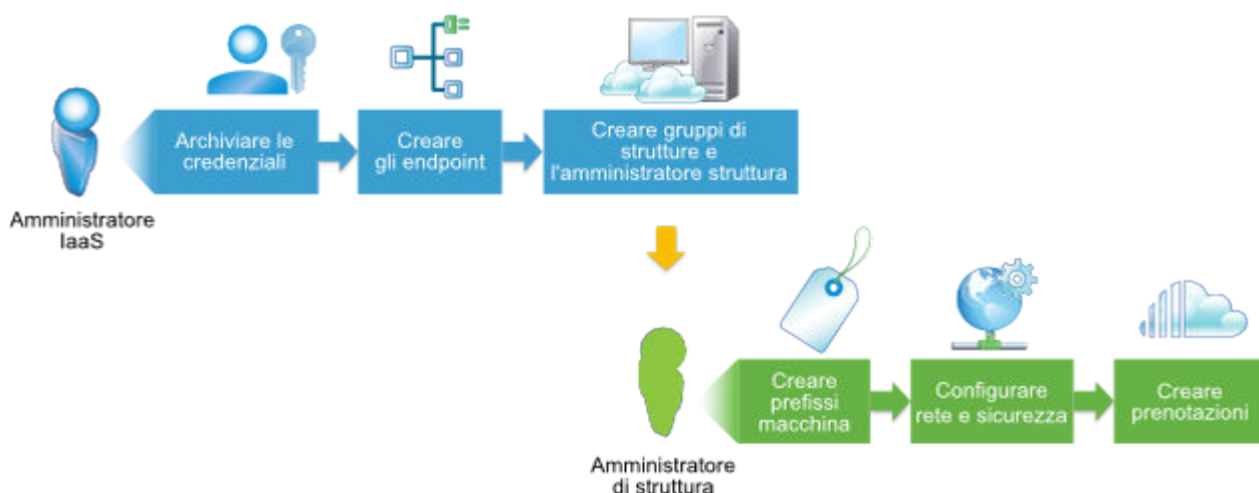


Tavola 3-1. Elenco di controllo per la configurazione di risorse di IaaS

Attività	Ruolo di vRealize Automation	Dettagli
<input type="checkbox"/> Memorizzare le credenziali di livello amministrativo nell'infrastruttura.	Amministratore di IaaS	Archiviazione delle credenziali utente. Non è necessario fornire le credenziali se si sta integrando una delle piattaforme seguenti: <ul style="list-style-type: none"> ■ Pool Xen su un XenServer ■ XenServer ■ vSphere, con la configurazione dell'agente proxy per l'uso di credenziali integrate eseguita dall'amministratore di sistema
<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.
<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 IaaS se configurato anche come amministratore di struttura ■ Amministratore di struttura 	Configurazione di prenotazione e criteri di prenotazione.

Archiviazione delle credenziali utente

Per consentire a vRealize Automation di comunicare con gli endpoint, è necessario memorizzare le credenziali di livello amministrativo del proprio ambiente. Poiché è possibile utilizzare le stesse credenziali per più endpoint, le credenziali vengono gestite separatamente dagli endpoint e poi associate all'atto della creazione o della modifica degli endpoint.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore IaaS**.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Credenziali**.

- 2 Fare clic su **Nuove credenziali**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Immettere il nome utente nella casella di testo **Nome utente**.

Piattaforma	Formato e dettagli
vSphere	domain\username Fornire credenziali con autorizzazione alla modifica di attributi personalizzati.
vCloud Air	username specificato nell'interfaccia utente dell'endpoint Fornire le credenziali di un amministratore di organizzazione con diritti di connessione utilizzando VMware Remote Console.
vCloud Director	username specificato nell'interfaccia utente dell'endpoint Fornire credenziali con diritti di connessione utilizzando VMware Remote Console. <ul style="list-style-type: none"> ■ 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.
vRealize Orchestrator	username@domain Fornire credenziali per ognuna delle istanze di vRealize Orchestrator con autorizzazioni di esecuzione su tutti i workflow che si desidera chiamare da vRealize Automation.
vCloud Networking and Security (solo vSphere)	domain\username
NSX (solo vSphere)	username
Amazon AWS	Inserire l'ID della chiave di accesso. Per informazioni su come ottenere l'ID della chiave di accesso e la chiave di accesso segreta, consultare la documentazione di Amazon AWS.
Cisco UCS Manager	username
Dell iDRAC	username
HP iLO	username
Hyper-V (SCVMM)	domain\username
KVM (RHEV)	username@domain
NetApp ONTAP	username
Red Hat OpenStack	username Fornire le credenziali di un singolo utente che è amministratore in tutti i tenant Red Hat OpenStack o creare credenziali separate per ciascun tenant.

6 Immettere la password nelle caselle di testo **Password**.

Piattaforma	Formato
Amazon AWS	Inserire la chiave di accesso segreta. Per informazioni su come ottenere l'ID della chiave di accesso e la chiave di accesso segreta, consultare la documentazione di Amazon AWS.
Tutte le altre	Specificare la password relativa al nome utente fornito.

7 Fare clic sull'icona **Salva** (✓).

Passi successivi

Ora che le proprie credenziali sono memorizzate, è possibile procedere con la creazione di un endpoint. Vedere [Scelta dello scenario per un endpoint](#).

Scelta dello scenario per un endpoint

È possibile creare gli endpoint che consentono a vRealize Automation di comunicare con l'infrastruttura. La procedura di creazione di un endpoint varia in base alle necessità di provisioning delle macchine.

Scegliere uno scenario di endpoint in base al tipo di endpoint di destinazione.

Tavola 3-2. Scelta dello scenario per un endpoint

Ambiente	Endpoint da creare
vSphere	Creazione di un endpoint vSphere
vSphere con NSX	Creazione di un endpoint vSphere con integrazione di rete e sicurezza
vSphere con tecnologia Net App FlexClone per lo storage	Creazione di un endpoint NetApp ONTAP
vRealize Orchestrator	Creazione di un endpoint vRealize Orchestrator
Endpoint del provider IPAM esterno	Creazione di un endpoint del provider IPAM esterno
Sottoscrizione a vCloud Air o OnDemand	Creazione di un endpoint vCloud Air
vCloud Director	Creazione di un endpoint vCloud Director
Hyper-V autonomo	Creazione di un endpoint autonomo per Hyper-V
Hyper-V con SCVMM (Microsoft Center Virtual Machine Manager)	Creazione di un endpoint Hyper-V (SCVMM)
KVM (RHEV)	Creazione di un endpoint KVM (RHEV)
Account del servizio cloud di Amazon	<ul style="list-style-type: none"> ■ Creazione di un endpoint Amazon ■ (Facoltativo) Aggiunta di un tipo di istanza Amazon
Tenant OpenStack	Creazione di un endpoint OpenStack o PowerVC
PowerVC	Creazione di un endpoint OpenStack o PowerVC
Pool Xen su un XenServer	Creazione di un endpoint per pool Xen

Tavola 3-2. Scelta dello scenario per un endpoint (Continua)

Ambiente	Endpoint da creare
XenServer	Creazione di un endpoint XenServer
Importazione di un elenco di endpoint	<ul style="list-style-type: none"> ■ Preparazione di un file CSV di endpoint per l'importazione ■ Importazione di un elenco di endpoint

Creazione di un endpoint vSphere

È possibile creare endpoint che consentono a vRealize Automation di comunicare con l'ambiente vSphere e di trovare le risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Se l'ambiente vSphere è integrato con NSX, vedere [Creazione di un endpoint vSphere con integrazione di rete e sicurezza](#).

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore laaS**.
- 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 7.1*.
- Se l'amministratore di sistema non ha configurato il proxy per l'uso di credenziali integrate, è necessario memorizzare credenziali di livello amministratore per l'endpoint. Vedere [Archiviazione delle credenziali utente](#).

Procedura

1 Selezionare **Infrastruttura > Endpoint > Endpoint**.

2 Selezionare **Nuovo > Virtuale > vSphere**.

3 Immettere un nome nella casella di testo **Nome**.

Questo deve corrispondere al nome dell'endpoint fornito all'agente proxy di vSphere durante l'installazione, altrimenti non sarà possibile eseguire la raccolta dati.

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 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.

Se l'amministratore di sistema ha configurato l'agente proxy di vSphere affinché utilizzi credenziali integrate, è possibile selezionare le credenziali **Integrated**.

- 7 Non selezionare **Specificare il manager per la rete e la piattaforma di sicurezza** a meno che la configurazione non supporti NSX.

Questa impostazione è correlata alle implementazioni che utilizzano NSX e richiede una configurazione aggiuntiva.

- 8 (Facoltativo) Fare clic su **Nuovo** nella sezione Proprietà personalizzate per aggiungere le proprietà dell'endpoint significative per il fornitore 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.

- 9 Fare clic su **OK**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Importante: Non rinominare i data center di vSphere dopo la raccolta iniziale dei dati, altrimenti il provisioning potrebbe non riuscire.

Passi successivi

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

Creazione di un endpoint vSphere con integrazione di rete e sicurezza

È possibile creare endpoint che consentono a vRealize Automation di comunicare con l'ambiente vSphere e un'istanza di NSX.

Prerequisiti

- Accedere alla console di 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 7.1*.
- Archiviare le credenziali di livello amministrativo per l'endpoint vSphere e l'endpoint di servizi di rete e sicurezza. Vedere [Archiviazione delle credenziali utente](#). Se l'amministratore di sistema ha configurato l'agente proxy affinché utilizzi credenziali integrate, è necessario archiviare solo le credenziali di NSX.
- Configurare le impostazioni di rete. Vedere [Configurazione delle impostazioni dei componenti rete e sicurezza](#).

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Virtuale > vSphere**.

3 Immettere un nome nella casella di testo **Nome**.

Questo deve corrispondere al nome dell'endpoint fornito all'agente proxy di vSphere durante l'installazione, altrimenti non sarà possibile eseguire la raccolta dati.

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 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.

Se l'amministratore di sistema ha configurato l'agente proxy di vSphere affinché utilizzi credenziali integrate, è possibile selezionare le credenziali **Integrated**.

7 Configurare una piattaforma soluzione di networking.

Questo passaggio è necessario per abilitare le funzionalità dei servizi di rete e sicurezza di NSX.

a Selezionare **Specificare il manager per la rete e la piattaforma di sicurezza**.**b** Specificare l'URL dell'istanza di NSX nella casella di testo **Indirizzo**.

L'URL deve essere di tipo **https://hostname** o **https://IP_address**.

Ad esempio **https://nsx-manager**.

c Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.**8** (Facoltativo) Aggiungere eventuali proprietà personalizzate.**9** Fare clic su **OK**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Importante: Non rinominare i data center di vSphere dopo la raccolta iniziale dei dati, altrimenti il provisioning potrebbe non riuscire.

Passi successivi

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

Creazione di un endpoint 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 alla console di vRealize Automation come **amministratore laaS**.
- Configurare le credenziali degli utenti. Vedere *Configurazione di vRealize Automation*.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Orchestrazione > vCenter 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 nella vRealize Automation appliance, immettere **`https://vrealize-automation-appliance-hostname:443/vco`**.

- 5 Specificare la priorità dell'endpoint.
 - a Fare clic su **Nuova proprietà**.
 - b Immettere **VMware.VCenterOrchestrator.Priority** nella casella di testo **Nome**.
Per il nome della proprietà viene fatta distinzione tra lettere maiuscole e minuscole.
 - c Immettere un valore intero maggiore o uguale a 1 nella casella di testo **Valore**.
Valori più bassi rappresentano priorità più elevate.
 - d Fare clic sull'icona **Salva** (✓).

- 6 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 questa come endpoint vRealize Orchestrator per eseguire workflow di vRealize Automation in un ambiente di prova o per la creazione di un ambiente di prototipazione.

È possibile anche installare un plug-in in un server vRealize Orchestrator esterno.

È consigliabile utilizzare questo endpoint vRealize Orchestrator per eseguire workflow vRealize Automation in un ambiente di produzione.

Per installare il plug-in, fare riferimento al file README associato al file del programma d'installazione sul sito del download dei prodotti VMware all'indirizzo <http://vmware.com/web/vmware/downloads> nelle pagine relative a vCloud Networking and Security o NSX.

Creazione di un endpoint del provider IPAM esterno

Se è stato registrato e configurato un tipo di endpoint IPAM in vRealize Orchestrator, è possibile creare un endpoint per detto 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 da parte dell'utente 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

- [Ottenere e importare il pacchetto di provider IPAM esterni in vRealize Orchestrator.](#)
- [Eseguire il workflow per registrare il tipo di endpoint IPAM di Infoblox in vRealize Orchestrator.](#)
- Accedere alla console di vRealize Automation come **amministratore laaS**.
- Configurare le credenziali degli utenti. Vedere *Configurazione di vRealize Automation*.

Per questo esempio, creare un endpoint IPAM Infoblox utilizzando un tipo di endpoint che è stato registrato nel pacchetto di Infoblox VMware Plug-in for vCenter Orchestrator importato.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.

2 Selezionare **Nuovo > 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 Inserire il nome utente e la password richiesti per accedere all'account del provider di soluzioni IPAM.

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 **Nuovo** nella sezione Proprietà personalizzate per aggiungere le proprietà dell'endpoint significative per il fornitore 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**.

Passi successivi

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.

Per informazioni sulla console di gestione di vCloud Air, vedere la documentazione di vCloud Air.

Nota: Le prenotazioni definite per gli endpoint di vCloud Air e gli endpoint di vCloud Director non supportano l'utilizzo di profili di rete per il provisioning di macchine.

Prerequisiti

- Accedere alla console di 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.
- [Archiviazione delle credenziali utente](#).

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 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.

Le credenziali devono essere quelle del servizio di sottoscrizione di vCloud Air o dell'amministratore dell'account di OnDemand.

- 6 (Facoltativo) Selezionare la casella di controllo **Utilizza server proxy** per configurare la protezione aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy.

- a Specificare il nome host del server proxy nella casella di testo **Nome host**.
- b Specificare il numero di porta da utilizzare per la connessione al server proxy nella casella di testo **Porta**.
- c (Facoltativo) Fare clic sull'icona **Sfoglia** accanto alla casella di testo **Credenziali**.

Selezionare o creare le credenziali che rappresentano il nome utente e la password per il server proxy, se richieste dalla configurazione del proxy.

- 7 (Facoltativo) Aggiungere proprietà personalizzate.
- 8 Fare clic su **OK**.

Passi successivi

[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.

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 di vCloud Air e gli endpoint di vCloud Director non supportano l'utilizzo di profili di rete per il provisioning di macchine.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore laaS**.
- [Archiviazione delle credenziali utente](#).

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 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.
 - 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 vCloud Director viene connesso direttamente al livello di sistema, ad esempio lasciando il campo Organizzazione vuoto, 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.

- 7 (Facoltativo) Selezionare la casella di controllo **Utilizza server proxy** per configurare la protezione aggiuntiva e forzare il passaggio delle connessioni attraverso un server proxy.

- a Specificare il nome host del server proxy nella casella di testo **Nome host**.
- b Specificare il numero di porta da utilizzare per la connessione al server proxy nella casella di testo **Porta**.
- c (Facoltativo) Fare clic sull'icona **Sfoglia** accanto alla casella di testo **Credenziali**.

Selezionare o creare le credenziali che rappresentano il nome utente e la password per il server proxy, se richieste dalla configurazione del proxy.

- 8 (Facoltativo) Aggiungere proprietà personalizzate.

- 9 Fare clic su **OK**.

Passi successivi

[Creazione di un gruppo di strutture.](#)

Creazione di un endpoint Hyper-V (SCVMM)

Gli amministratori IaaS possono creare endpoint per consentire a vRealize Automation di comunicare con l'ambiente SCVMM e di trovare le risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore IaaS**.
- [Archiviazione delle credenziali utente.](#)

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 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.

Se le credenziali non sono state già memorizzate, è possibile farlo a questo punto.

- 7 (Facoltativo) Aggiungere proprietà personalizzate.
- 8 Fare clic su **OK**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Passi successivi

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

Creazione di un endpoint autonomo per Hyper-V

È possibile creare endpoint per consentire a vRealize Automation di comunicare con l'ambiente server di Hyper-V e di trovare le risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Prerequisiti

- Accedere alla console di 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 7.1*.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Agenti**.
- 2 Specificare il nome DNS completo del server Hyper-V nella casella di testo **Risorsa di elaborazione**.
- 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**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Passi successivi

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

Creazione di un endpoint NetApp ONTAP

È possibile creare endpoint per consentire a vRealize Automation di comunicare con i dispositivi di storage che utilizzano la tecnologia Net App FlexClone.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore IaaS**.
- [Archiviazione delle credenziali utente](#).

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Storage > NetApp ONTAP**.
- 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 **netapp-1.mycompany.local**.
- 6 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.
Se le credenziali non sono state già memorizzate, è possibile farlo a questo punto.
- 7 (Facoltativo) Aggiungere proprietà personalizzate.
- 8 Fare clic su **OK**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Passi successivi

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

Creazione di un endpoint KVM (RHEV)

È possibile creare endpoint per consentire a vRealize Automation di comunicare con l'ambiente KVM (RHEV) e di trovare le risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore IaaS**.

- [Archiviazione delle credenziali utente.](#)

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Virtuale > KVM (RHEV)**.
- 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 **https://FQDN** o **https://IP_address**

Ad esempio **https://mycompany-kvmrhev1.mycompany.local**.

- 6 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.

Se le credenziali non sono state già memorizzate, è possibile farlo a questo punto.

- 7 (Facoltativo) Aggiungere proprietà personalizzate.
- 8 Fare clic su **OK**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Passi successivi

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

Creazione di un endpoint per pool Xen

È possibile creare endpoint per consentire a vRealize Automation di comunicare con il master del pool Xen e di trovare le risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore laaS**.
- Un amministratore di sistema deve installare un agente proxy con credenziali memorizzate che corrispondono all'endpoint. Vedere *Installazione di vRealize Automation 7.1*.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Agenti**.
- 2 Specificare il nome del master del pool Xen nella casella di testo **Risorsa di elaborazione**.

Nota: non inserire il nome del pool Xen. È necessario inserire il nome del master del pool.

Per evitare voci duplicate nella tabella delle risorse di elaborazione di vRealize Automation, specificare un indirizzo che corrisponda a quello del master del pool Xen configurato. Ad esempio, se l'indirizzo del master del pool Xen utilizza il nome dell'host, immettere quest'ultimo e non il nome di dominio completo (FQDN). Se l'indirizzo del master 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**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Passi successivi

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

Creazione di un endpoint XenServer

È possibile creare endpoint per consentire a vRealize Automation di comunicare con l'ambiente XenServer e di trovare le risorse di elaborazione, raccogliere dati ed eseguire il provisioning delle macchine.

Prerequisiti

- Accedere alla console di 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 7.1*.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Agenti**.
- 2 Specificare il nome DNS completo del server XenServer nella casella di testo **Risorsa di elaborazione**.
- 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**.

vRealize Automation raccoglie i dati dall'endpoint e rileva le risorse di elaborazione utilizzate.

Passi successivi

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

Creazione di un endpoint Amazon

È possibile creare un endpoint da collegare a un'istanza di Amazon Web Services.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore IaaS**.
- [Archiviazione delle credenziali utente](#).

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Selezionare **Nuovo > Cloud > Amazon EC2**.
- 3 Immettere un nome e, facoltativamente, una descrizione.
In genere questo nome indica l'account di Amazon Web Services corrispondente a questo endpoint.
- 4 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.
A un dato ID di chiave di accesso di Amazon è possibile associare un solo endpoint.
- 5 (Facoltativo) Fare clic sulla casella di controllo **Utilizza server proxy** per configurare la protezione aggiuntiva e forzare le connessioni a Amazon Web Services a passare attraverso un server proxy.
 - a Specificare il nome host del server proxy nella casella di testo **Nome host**.
 - b Specificare il numero di porta da utilizzare per la connessione al server proxy nella casella di testo **Porta**.
 - c (Facoltativo) Fare clic sull'icona **Sfoglia** accanto alla casella di testo **Credenziali**.
Selezionare o creare le credenziali che rappresentano il nome utente e la password per il server proxy, se richieste dalla configurazione del proxy.
- 6 (Facoltativo) Aggiungere proprietà personalizzate.
- 7 Fare clic su **OK**.

Dopo la creazione dell'endpoint, vRealize Automation inizia a raccogliere dati dalle regioni di Amazon Web Services.

Passi successivi

vRealize Automation offre diversi tipi di istanze di Amazon Web Services utilizzabili nel corso della creazione di blueprint, ma è comunque possibile importare tipi di istanze proprie. A tale scopo, vedere [Aggiunta di un tipo di istanza Amazon](#).

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 alla console di vRealize Automation come **amministratore IaaS**.

Procedura

1 Fare clic su **Infrastruttura > Amministrazione > Tipi di istanze**.

2 Fare clic su **Nuovo tipo di istanza**.

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** (👍).

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

Passi successivi

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

Creazione di un endpoint OpenStack o PowerVC

L'utente crea un endpoint per consentire a vRealize Automation di comunicare con l'istanza OpenStack o PowerVC.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore IaaS**.
- [Archiviazione delle credenziali utente](#).
- Verificare che i DEM vRealize Automation siano installati in una macchina che soddisfa i requisiti OpenStack o PowerVC. Vedere *Installazione di vRealize Automation 7.1*.
- Verificare che la versione in uso di OpenStack sia attualmente supportata. Vedere *Matrice di supporto di vRealize Automation*.

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 essere nel formato https://FQDN/powervc/openstack/service . Ad esempio: https://openstack.mycompany.com/powervc/openstack/admin .
OpenStack	L'URL deve essere nel formato FQDN:5000 o IP_address:5000 . Non includere il suffisso /v2.0 nell'indirizzo dell'endpoint. Ad esempio: https://openstack.mycompany.com:5000 .

- 5 Fare clic su **Credenziali** e selezionare le credenziali di livello amministrativo archiviate per l'endpoint specificato.

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 (Facoltativo) Aggiungere proprietà personalizzate.
- 8 Fare clic su **OK**.

Passi successivi

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

Importazione di un elenco di endpoint

Importare un file di endpoint in formato CSV può essere più efficace rispetto a aggiungere endpoint uno alla volta tramite la console di vRealize Automation.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore laaS**.
- Memorizzare le credenziali per gli endpoint.
- Preparare un file CSV di endpoint per l'importazione.

Procedura

- 1 Selezionare **Infrastruttura > Endpoint > Endpoint**.
- 2 Fare clic su **Importa endpoint**.
- 3 Fare clic su **Sfoglia**.
- 4 Individuare il file CSV che contiene gli endpoint.
- 5 Fare clic su **Apri**.

Viene aperto un file CSV contenente un elenco di endpoint nel formato seguente:

```
InterfaceType,Address,Credentials,Name,Description
vCloud,https://abxpoint2vco,svc-admin,abxpoint2vco,abxpoint
```

- 6 Fare clic su **Importa**.

È possibile modificare e gestire gli endpoint attraverso la console di vRealize Automation.

Preparazione di un file CSV di endpoint per l'importazione

Per evitare di aggiungere endpoint uno alla volta tramite la console vRealize Automation, è possibile importare in un'unica operazione tutti gli endpoint da aggiungere caricando l'elenco contenuto in un file CSV.

Il file CSV deve contenere una riga di intestazione con i campi previsti. I campi devono rispettare un ordine specifico e per essi viene fatta distinzione tra lettere maiuscole e minuscole. Nello stesso file CSV è possibile caricare endpoint multipli di tipologie differenti. Per vCloud Director vengono importati gli account degli amministratori di sistema anziché gli endpoint degli amministratori di organizzazione.

Tavola 3-3. Campi del file CSV e loro ordine per l'importazione degli endpoint

Campo	Descrizione
InterfaceType	(Obbligatori) In un singolo file è possibile caricare diversi tipi di endpoint. <ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director ■ vRealize Orchestrator ■ vSphere ■ Amazon EC2 ■ OpenStack ■ NetAppOnTap ■ SCVMM ■ KVM
Address	(Obbligatorio per tutti i tipi di interfaccia, eccetto Amazon) URL dell'endpoint. Per informazioni sul formato richiesto per il tipo di piattaforma, vedere la procedura corrispondente per creare un endpoint per la piattaforma.
Credentials	(Obbligatorio) Nome assegnato alle credenziali utente quando le si memorizza in vRealize Automation.
Name	(Obbligatorio) Specificare un nome per l'endpoint. Per OpenStack, l'indirizzo viene utilizzato come nome predefinito.
Description	(Obbligatorio) Inserire una descrizione dell'endpoint.
OpenstackProject	(Obbligatorio solo per OpenStack) Specificare il nome del progetto per l'endpoint.

Risoluzione dei messaggi di errore che attestano l'impossibilità di trovare l'endpoint vSphere collegato

Quando è impossibile completare la raccolta dati per un endpoint vSphere, spesso il motivo è che il nome del proxy e il nome dell'endpoint non coincidono.

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 attesta l'impossibilità di trovare un 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**.

L'agente proxy può comunicare con l'endpoint e la raccolta dati viene completata correttamente.

Risoluzione dei problemi di individuazione dell'URL di gestione di vCloud Air per un Virtual Data Center dell'organizzazione

Per creare un endpoint vCloud Air, è necessario specificare a vRealize Automation la regione di vCloud Air richiesta e l'URL di gestione.

Soluzione

L'URL di gestione di vCloud Air coincide anche con l'URL del server vCloud Director utilizzato per gestire uno specifico Virtual Data Center (vDC). È possibile utilizzare le informazioni della regione e l'URL di gestione per configurare l'endpoint vCloud Air.

Individuare l'URL di gestione per ogni vDC di regione dalla console di vCloud Air.

Procedura

- 1 Accedere alla console di vCloud Air con privilegi amministrativi.
- 2 Dalla dashboard di vCloud Air, selezionare il Virtual Data Center.
- 3 Fare clic sul collegamento per visualizzare un URL relativo al Virtual Data Center da utilizzare nei comandi API.

Ad esempio `https://mycompany.com:443/cloud/org/vCloudAutomation/`.

L'URL di gestione da fornire a vRealize Automation corrisponde alla porzione dell'URL del comando API composta da host e porta, mentre la regione è la porzione dell'URL che segue `cloud/org/`. Nell'esempio precedente, l'URL di gestione è `https://mycompany.com:443` e la regione è `vCloudAutomation`.

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 alla console di vRealize Automation come **amministratore IaaS**.
- Creare almeno un endpoint.

Procedura

- 1 Selezionare **Infrastruttura > Gruppi di strutture**.
- 2 Fare clic su **Nuovo gruppo di strutture**.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 (Facoltativo) Immettere una descrizione nella casella di testo **Descrizione**.
- 5 Immettere il nome di un utente o di un gruppo di utenti nella casella di testo **Amministratori di struttura** e premere Invio.

Ripetere questo passaggio per aggiungere più utenti o gruppi al ruolo.

- 6 Fare clic su 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**.

Gli amministratori di struttura a questo punto possono configurare i prefissi macchina. Vedere [Configurazione dei prefissi macchina](#).

Gli utenti che sono attualmente connessi alla console di vRealize Automation devono disconnettersi e riaccedere alla console di vRealize Automation prima di 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 alla console di vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Fare clic su **Infrastruttura > Amministrazione > Prefissi macchina**.
- 2 Fare clic su **Nuovo**.
- 3 Immettere il prefisso macchina nella casella di testo **Nome**.
- 4 Immettere il numero di cifre del contatore nella casella di testo **Numero di cifre**.
- 5 Immettere il numero iniziale del contatore nella casella di testo **Numero successivo**.
- 6 Fare clic sull'icona **Salva** ()

Gli amministratori tenant possono creare gruppi di business per consentire agli utenti di accedere a vRealize Automation per richiedere macchine.

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 AWS. 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 alla console di 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 sull'icona **Salva** (✓).

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 alla console di 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 alla console di 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**.

Creazione di un profilo di rete

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 per le quali esegue il provisioning.

È possibile creare un profilo di rete per definire un tipo di rete disponibile, compresi profili di reti esterne e modelli per profili di reti NAT (Network Address Translation) su richiesta e instradate che creeranno switch logici NSX e impostazioni di routing appropriate per un nuovo percorso di rete. Quando si aggiungono componenti di rete a un blueprint, sono necessari profili 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 Edge NSX che vengono creati durante il provisioning delle macchine. 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.

Un creatore di blueprint specifica un profilo di rete appropriato durante la definizione dei componenti di rete nel blueprint. È possibile utilizzare un profilo di rete esistente e un profilo di rete NAT o instradata su richiesta durante la definizione delle schede di rete e i bilanciamenti del carico per il provisioning delle macchine.

I profili di rete supportano anche i provider IPAM (IP Address Management) 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 per l'uso con un profilo di rete esterno.

Si possono specificare intervalli di indirizzi IP che possono essere utilizzati 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. I profili di rete possono essere assegnati a percorsi di rete specifici in 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.

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.

Se viene specificato un profilo di rete in una prenotazione e un blueprint, il valore del blueprint ha la precedenza. Ad esempio, se viene specificato un profilo di rete nel blueprint mediante la proprietà personalizzata `VirtualMachine.NetworkN.ProfileName` e in una prenotazione utilizzata dal blueprint, il profilo di rete specificato nel blueprint ha la precedenza. Se, tuttavia, la proprietà personalizzata non viene utilizzata nel blueprint e si seleziona un profilo di rete per una NIC della macchina, vRealize Automation utilizza il percorso di rete della prenotazione per la NIC della macchina per la quale è stato specificato il profilo di rete.

Tavola 3-4. Tipi di reti disponibili per un profilo di rete di vRealize Automation

Tipo di rete	Descrizione
Esterna	<p>Reti esistenti configurate sul server vSphere. Esse 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 anche possibile utilizzare intervalli IP ottenuti dal provider IPAM interno di VMware fornito o la soluzione di un provider IPAM esterno che è stata importata e registrata in vRealize Orchestrator, come ad esempio l'IPAM Infoblox.</p> <p>Un profilo di rete esterna con un intervallo di IP statici è un prerequisito per le reti NAT e instradate.</p>
NAT	<p>Le reti private vengono create durante il provisioning. Sono reti che utilizzano un set di indirizzi IP per la comunicazione esterna e un altro set per le comunicazioni interne. 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>Un profilo di rete NAT definisce una rete locale e una esterna che utilizzano una tabella di traduzione per comunicare tra loro.</p>
Instradato	<p>Le reti private vengono create durante il provisioning. Esse rappresentano uno spazio di indirizzi IP instradabile suddiviso tra subnet collegate tra loro tramite un DLR (Distributed Logical Router). 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>Un profilo di rete instradata definisce uno spazio instradabile e le subnet disponibili.</p> <p>Per ulteriori informazioni sui Distributed Logical Router, vedere la <i>guida di amministrazione di NSX</i>.</p>

Assegnazione di un intervallo di indirizzi IP statici mediante i profili di rete

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.

È possibile utilizzare facoltativamente l'IPAM interno di VMware o un provider di servizi IPAM esterno registrato per ottenere e configurare gli indirizzi IP. Per informazioni sui requisiti per IPAM esterni, vedere [Elenco di controllo per la preparazione del supporto di provider IPAM esterni](#).

Quando si seleziona un endpoint IPAM esterno 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.

Se viene specificato un profilo di rete in una prenotazione e un blueprint, il valore del blueprint ha la precedenza. Ad esempio, se viene specificato un profilo di rete nel blueprint mediante la proprietà personalizzata `VirtualMachine.NetworkN.ProfileName` e in una prenotazione utilizzata dal blueprint, il profilo di rete specificato nel blueprint ha la precedenza. Se, tuttavia, la proprietà personalizzata non viene utilizzata nel blueprint e si seleziona un profilo di rete per una NIC della macchina, vRealize Automation utilizza il percorso di rete della prenotazione per la NIC della macchina per la quale è stato specificato il profilo di rete.

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 inutilizzati potrebbero non essere disponibili immediatamente dopo l'eliminazione delle macchine che li utilizzavano, dato che il processo di recupero degli indirizzi IP statici viene eseguito ogni 30 minuti. Se nel profilo di rete non sono disponibili indirizzi IP, non sarà possibile eseguire il provisioning delle macchine con assegnazione di IP statici sul percorso di rete associato.

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
<code>ip_address</code>	Un indirizzo IP in formato IPv4.
<code>machine_name</code>	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 <code>status</code> non può essere Allocated.
<code>status</code>	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 <code>machine_name</code> non può essere vuoto.
<code>NIC_offset</code>	Un numero intero non negativo.

Di seguito viene riportato l'esempio di una voce che non specifica uno scarto NIC:

```
100.10.100.1,mymachine01,Unallocated
```

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 esterno di fornire gli 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 presente alcuna opzione **Importa da CSV** per i profili di rete che utilizzano un tipo di endpoint IPAM esterno in quanto gli indirizzi IP sono gestiti da un provider IPAM esterno e non da vRealize Automation.

Prerequisiti

- Accedere alla console di 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 esterno](#) 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**. In questo modo, sarà possibile inserire in modo rapido le informazioni di base sui profili di rete nelle prime due schede.
- 5 Facoltativamente, è possibile 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 Fare clic su **Nuovo** per immettere un nuovo nome di intervallo di rete e intervallo di indirizzi IP manualmente o fare clic su **Importa da CSV** per importare le informazioni degli indirizzi IP da un file CSV correttamente formattato.
 - Fare clic su **Aggiungi**.
 - a Immettere un nuovo nome nella casella di testo **Intervallo di rete**.
 - b Immettere una descrizione dell'intervallo di rete.

- c Immettere l'indirizzo IP iniziale dell'intervallo nella casella di testo **Indirizzo IP iniziale**.
- d Immettere l'indirizzo IP finale dell'intervallo nella casella di testo **Indirizzo IP finale**.

■ Fare clic su **Importa da CSV**.

- a Individuare e selezionare il file CSV o trascinarlo e rilasciarlo 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,Unallocated
```

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.

- b Fare clic su **Applica**.

10 Fare clic su **OK**.

Il nome dell'intervallo IP viene visualizzato nell'elenco degli intervalli definiti. Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP caricati vengono visualizzati nella pagina **Indirizzi IP** quando si fa clic su **Applica** o dopo aver salvato e quindi modificato il profilo di rete.

11 Fare clic sulla scheda **Indirizzi IP** per visualizzare i dati dell'indirizzo IP per lo spazio di indirizzi dell'intervallo specificato.

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) Selezionare le informazioni dell'indirizzo IP dal menu a discesa **Intervallo di rete** per filtrare le voci degli indirizzi IP.

È possibile visualizzare informazioni su tutti gli intervalli di rete definiti, sugli intervalli di rete importati da un file CSV o su un intervallo di rete denominato. I dettagli comprendono l'indirizzo IP di inizio, il nome della macchina, la data dell'ultima modifica e il relativo timestamp, nonché lo stato dell'IP.

Passi successivi

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

È possibile creare un profilo di rete esterna per definire le proprietà della rete e un intervallo di indirizzi IP statici da utilizzare nel provisioning delle macchine per una rete esistente.

Facoltativamente, è possibile utilizzare il pacchetto del provider IPAM interno fornito o di un provider IPAM esterno di terze parti, come ad esempio Infoblox, che è stato importato, configurato e registrato in vRealize Orchestrator.

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 esterno](#).

Procedura

1 Definizione delle informazioni sui profili di rete esterna

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 di intervalli di IP per il profilo di rete esterno

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).

Definizione delle informazioni sui profili di rete esterna

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 la preparazione del supporto di provider IPAM esterni](#) e [Creazione di un profilo di rete esterna mediante un provider IPAM esterno](#). Attenersi alla seguente procedura per creare un profilo di rete utilizzando l'endpoint IPAM interno di VMware

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **Esistente** o **Esterno** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.

- 4 (Facoltativo) Accettare l'endpoint IPAM **VMware** interno fornito nel menu a discesa **Endpoint IPAM**.
- 5 Immettere la subnet mask IP nella casella di testo **Subnet mask**.
Ad esempio, immettere 255.255.0.0.
- 6 Immettere un indirizzo di gateway instradato o Edge nella casella di testo **Gateway**.
- 7 Fare clic sulla scheda **DNS**.
- 8 Immettere i valori di DNS e WINS secondo necessità.

I campi DNS e WINS sono facoltativi se si utilizza un endpoint IPAM interno. Se si utilizza un endpoint IPAM esterno, i valori di DNS e WINS vengono forniti dal provider 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 il **suffisso DNS**.
Il suffisso DNS è usato nella registrazione e risoluzione dei nomi DNS.
- d (Facoltativo) Immettere un valore per il **suffisso di ricerca DNS**.
- e (Facoltativo) Immettere un valore del server **WINS preferito**.
- f (Facoltativo) Immettere un valore del server **WINS alternativo**.

Passi successivi

È possibile configurare intervalli di indirizzi IP statici. Vedere [Configurazione di intervalli di IP per il profilo di rete esterno](#).

Configurazione di intervalli di IP per il profilo di rete esterno

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).

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.

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.

Prerequisiti

[Definizione delle informazioni sui profili di rete esterna](#).

Procedura

- 1 Fare clic sulla scheda **Intervalli di rete**.

- 2 Fare clic su **Nuovo** per immettere un nuovo nome di intervallo di rete e intervallo di indirizzi IP manualmente o fare clic su **Importa da CSV** per importare le informazioni degli indirizzi IP da un file CSV correttamente formattato.

■ Fare clic su **Aggiungi**.

- a Immettere un nuovo nome nella casella di testo **Intervallo di rete**.
- b Immettere una descrizione dell'intervallo di rete.
- c Immettere l'indirizzo IP iniziale dell'intervallo nella casella di testo **Indirizzo IP iniziale**.
- d Immettere l'indirizzo IP finale dell'intervallo nella casella di testo **Indirizzo IP finale**.

■ Fare clic su **Importa da CSV**.

- a Individuare e selezionare il file CSV o trascinarlo e rilasciarlo 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,Unallocated
```

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.

- b Fare clic su **Applica**.

- 3 Fare clic su **OK**.

Il nome dell'intervallo IP viene visualizzato nell'elenco degli intervalli definiti. Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP caricati vengono visualizzati nella pagina **Indirizzi IP** quando si fa clic su **Applica** o dopo aver salvato e quindi modificato il profilo di rete.

- 4 Fare clic sulla scheda **Indirizzi IP** per visualizzare i dati dell'indirizzo IP per lo spazio di indirizzi dell'intervallo specificato.

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) Selezionare le informazioni dell'indirizzo IP dal menu a discesa **Intervallo di rete** per filtrare le voci degli indirizzi IP.

È possibile visualizzare informazioni su tutti gli intervalli di rete definiti, sugli intervalli di rete importati da un file CSV o su un intervallo di rete denominato. I dettagli comprendono l'indirizzo IP di inizio, il nome della macchina, la data dell'ultima modifica e il relativo timestamp, nonché lo stato dell'IP.

- 6 (Facoltativo) Selezionare un tipo di stato nel menu a discesa **Stato IP** per filtrare le voci degli indirizzi IP in modo da avere solo quelle con lo stato IP selezionato corrispondente. Lo stato può essere Allocato, Non allocato, Eliminato e Scaduto.

Fare clic su **Recupera** per rendere gli intervalli degli indirizzi IP con stato Scaduto o Eliminato disponibili per l'allocazione. È necessario salvare il profilo affinché il recupero abbia effetto. Gli indirizzi non vengono recuperati immediatamente, per cui la colonna dello stato non cambia subito da Scaduto o Eliminato ad Allocato.

- 7 Fare clic su **OK** per completare il profilo di rete.

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 esterno

È possibile utilizzare una rete esistente per creare un profilo di rete esterna e definire le proprietà della rete e un intervallo di indirizzi IP statici per il provisioning delle macchine. È possibile utilizzare un provider IPAM esterno precedentemente importato, configurato e registrato in vRealize Orchestrator.

È possibile creare un profilo di rete esterna che utilizza l'endpoint di un provider di soluzioni IPAM 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](#).

Procedura

- 1 [Specificare le informazioni del profilo di rete esterno per un endpoint IPAM registrato](#)

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 di IP per i profili di reti esterne per l'endpoint IPAM registrato

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).

Passi successivi

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 tale profilo quando si crea un profilo di rete NAT o instradata su richiesta.

Specificare le informazioni del profilo di rete esterno per un endpoint IPAM registrato

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 la preparazione del supporto di provider IPAM esterni](#).
- [Creazione di un endpoint del provider IPAM esterno](#).
- Configurare vRealize Orchestrator Appliance con il workflow dell'endpoint IPAM registrato come Orchestrator autonomo nel tenant globale (administrator @ vsphere.local).
- Accedere alla console di vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Profili di rete**.
- 2 Fare clic su **Nuovo** e selezionare **Esistente** o **Esterno** dal menu a discesa.
- 3 Immettere un nome e, facoltativamente, una descrizione.
- 4 Se è stato configurato un provider di servizi IPAM esterno, è possibile selezionare il nome dell'endpoint IPAM registrato nel menu a discesa **Endpoint IPAM**.

Quando si seleziona un endpoint IPAM esterno registrato in vRealize Orchestrator, gli indirizzi IP vengono ottenuti dall'endpoint del provider di servizi IPAM specificato. Le opzioni Subnet mask, Gateway e DNS/WINS non sono disponibili perché le loro funzioni sono controllate dall'endpoint IPAM selezionato. I valori selezionati per le opzioni Subnet mask, Gateway e DNS/WINS sono forniti dall'endpoint IPAM selezionato.

Passi successivi

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 di IP per i profili di reti esterne per l'endpoint IPAM registrato

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 di IP utilizzando gli indirizzi IP forniti da un provider IPAM esterno.

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.

Prerequisiti

[Specificare le informazioni del profilo di rete esterno per un endpoint IPAM registrato.](#)

Procedura

- 1 Fare clic sulla scheda **Intervalli di rete** per creare un nuovo intervallo di rete oppure selezionarne uno esistente.

Vengono visualizzati i dettagli sull'intervallo selezionato, comprendenti nome, descrizione, indirizzo IP di inizio e di fine. Vengono inoltre fornite informazioni relative allo stato.

- 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 reti disponibili per lo spazio di indirizzi specificato.
- 4 Fare clic su **OK**.

Il nome dell'intervallo IP viene visualizzato nell'elenco degli intervalli definiti. Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP caricati vengono visualizzati nella pagina **Indirizzi IP** quando si fa clic su **Applica** o dopo aver salvato e quindi modificato il profilo di rete.

- 5 Fare clic su **OK** per completare il profilo di rete.

Passi successivi

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 NAT

È possibile creare un profilo di rete NAT su richiesta per definire una rete NAT e assegnare a essa intervalli di indirizzi IP statici e DHCP.

Procedura

1 Definizione delle informazioni dei profili di rete NAT

Il profilo di rete identifica le proprietà della rete NAT, il relativo profilo di rete esterna sottostante, il tipo di NAT e gli altri valori utilizzati nel provisioning della rete.

2 Configurazione di intervalli di IP per il profilo di rete NAT

È possibile definire uno o più intervalli di indirizzi IP statici da utilizzare nel provisioning di una rete.

Definizione delle informazioni dei profili di rete NAT

Il profilo di rete identifica le proprietà della rete NAT, il relativo profilo di rete esterna sottostante, il tipo di NAT e gli altri valori utilizzati nel provisioning della rete.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore di struttura**.
- Creare un profilo di rete esterna. Vedere [Creazione di un profilo di rete esterna](#) o [Creazione di un profilo di rete esterna mediante un provider IPAM esterno](#).

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 dell'**endpoint IPAM** predefinito per il provider IPAM **VMware** interno fornito oppure selezionare un altro endpoint di provider IPAM, ad esempio Infoblox, importato e registrato in vRealize Orchestrator.

Nota: L'IPAM esterno non è disponibile per le reti instradate e NAT su richiesta.

- 5 Selezionare un profilo di rete 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.
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.

- 7 Immettere la subnet mask IP nella casella di testo **Subnet mask**.

Ad esempio, immettere 255.255.0.0.

- 8 Immettere un indirizzo di gateway instradato o Edge nella casella di testo **Gateway**.

Utilizzare un formato di indirizzo IPv4 standard. Ad esempio, immettere 10.10.110.1.

- 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.

- 10 (Facoltativo) Impostare una durata lease 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.

I campi DNS e WINS sono facoltativi se si utilizza un endpoint IPAM interno. Se si utilizza un endpoint IPAM esterno, i valori di DNS e WINS vengono forniti dal provider 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 il **suffisso DNS**.
Il suffisso DNS è usato nella registrazione e risoluzione dei nomi DNS.
- d (Facoltativo) Immettere un valore per il **suffisso di ricerca DNS**.
- e (Facoltativo) Immettere un valore del server **WINS preferito**.
- f (Facoltativo) Immettere un valore del server **WINS alternativo**.

Passi successivi

[Configurazione di intervalli di IP per il profilo di rete NAT.](#)

Configurazione di intervalli di IP per il profilo di rete NAT

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

[Definizione delle informazioni dei profili di rete NAT.](#)

Procedura

- 1 Fare clic sulla scheda **Intervalli di rete** per creare un nuovo intervallo di rete oppure selezionarne uno esistente.

Vengono visualizzati i dettagli sull'intervallo selezionato, comprendenti nome, descrizione, indirizzo IP di inizio e di fine. Vengono inoltre fornite informazioni relative allo stato.

- 2 Fare clic su **Nuovo** per immettere un nuovo nome di intervallo di rete e intervallo di indirizzi IP manualmente o fare clic su **Importa da CSV** per importare le informazioni degli indirizzi IP da un file CSV correttamente formattato.

■ Fare clic su **Aggiungi**.

- a Immettere un nuovo nome nella casella di testo **Intervallo di rete**.
- b Immettere una descrizione dell'intervallo di rete.
- c Immettere l'indirizzo IP iniziale dell'intervallo nella casella di testo **Indirizzo IP iniziale**.
- d Immettere l'indirizzo IP finale dell'intervallo nella casella di testo **Indirizzo IP finale**.

■ Fare clic su **Importa da CSV**.

- a Individuare e selezionare il file CSV o trascinarlo e rilasciarlo 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,Unallocated
```

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.

- b Fare clic su **Applica**.

- 3 Fare clic su **OK**.

Il nome dell'intervallo IP viene visualizzato nell'elenco degli intervalli definiti. Gli indirizzi IP dell'intervallo vengono visualizzati nell'elenco degli indirizzi IP definiti.

Gli indirizzi IP caricati vengono visualizzati nella pagina **Indirizzi IP** quando si fa clic su **Applica** o dopo aver salvato e quindi modificato il profilo di rete.

- 4 Fare clic sulla scheda **Indirizzi IP** per visualizzare gli indirizzi IP dell'intervallo di rete denominato.

- 5 (Facoltativo) Selezionare le informazioni dell'indirizzo IP dal menu a discesa **Intervallo di rete** per filtrare le voci degli indirizzi IP.

È possibile visualizzare informazioni su tutti gli intervalli di rete definiti, sugli intervalli di rete importati da un file CSV o su un intervallo di rete denominato. I dettagli comprendono l'indirizzo IP di inizio, il nome della macchina, la data dell'ultima modifica e il relativo timestamp, nonché lo stato dell'IP.

- 6 (Facoltativo) Selezionare un tipo di stato nel menu a discesa **Stato IP** per filtrare le voci degli indirizzi IP in modo da avere solo quelle con lo stato IP selezionato corrispondente. Lo stato può essere Allocato, Non allocato, Eliminato e Scaduto.

Fare clic su **Recupera** per rendere gli intervalli degli indirizzi IP con stato Scaduto o Eliminato disponibili per l'allocazione. È necessario salvare il profilo affinché il recupero abbia effetto. Gli indirizzi non vengono recuperati immediatamente, per cui la colonna dello stato non cambia subito da Scaduto o Eliminato ad Allocato.

- 7 Fare clic su **OK**.

Creazione di un profilo di rete instradata

È possibile creare un profilo di rete instradata su richiesta per definire uno spazio IP instradabile e le subnet disponibili per le reti instradate.

Procedura

1 Definizione delle informazioni dei profili di rete instradata

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.

2 Configurazione di intervalli di IP per il profilo di rete instradata

È possibile definire uno o più intervalli di indirizzi IP statici da utilizzare nel provisioning di una rete.

Definizione delle informazioni dei profili di rete instradata

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.

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.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore di struttura**.
- Creare un profilo di rete esterna. Vedere [Creazione di un profilo di rete esterna](#) o [Creazione di un profilo di rete esterna mediante un provider IPAM esterno](#).
- Verificare che il router logico NSX sia configurato nel vSphere Client per utilizzare il profilo di rete instradata. Vedere la *guida di amministrazione di NSX*.

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 Selezionare un profilo di rete esistente dal menu a discesa **Profilo di rete esterno**.

- 5 Accettare il valore dell'**endpoint IPAM** predefinito per il provider IPAM **VMware** interno fornito oppure selezionare un altro endpoint di provider IPAM, ad esempio Infoblox, importato e registrato in vRealize Orchestrator.

Nota: L'IPAM esterno non è disponibile per le reti instradate e NAT su richiesta.

- 6 Immettere la subnet mask nella casella di testo **Subnet mask** associata al profilo di rete esterno.
Ad esempio, immettere 255.255.0.0.
- 7 Immettere un valore nella casella di testo **Subnet mask intervallo** per determinare in che modo gli intervalli vengano generati dall'opzione **Genera intervalli** nella pagina **Intervalli IP**.
Ad esempio, immettere 255.255.255.0.
- 8 Immettere il primo indirizzo IP disponibile nella casella di testo **IP base**. Le impostazioni IP base e della subnet mask dell'intervallo sono utilizzate per generare intervalli.
Ad esempio, immettere 120.120.0.1.
- 9 Fare clic sulla scheda **DNS**.
- 10 Immettere i valori di DNS e WINS secondo necessità.

I campi DNS e WINS sono facoltativi se si utilizza un endpoint IPAM interno. Se si utilizza un endpoint IPAM esterno, i valori di DNS e WINS vengono forniti dal provider 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 il **suffisso DNS**.
Il suffisso DNS è usato nella registrazione e risoluzione dei nomi DNS.
- d (Facoltativo) Immettere un valore per il **suffisso di ricerca DNS**.
- e (Facoltativo) Immettere un valore del server **WINS preferito**.
- f (Facoltativo) Immettere un valore del server **WINS alternativo**.

Passi successivi

[Configurazione di intervalli di IP per il profilo di rete instradata.](#)

Configurazione di intervalli di IP per il profilo di rete instradata

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 il successivo intervallo disponibile e lo utilizza come proprio spazio di indirizzi IP.

Prerequisiti

[Definizione delle informazioni dei profili di rete instradata.](#)

Procedura

- 1 Fare clic sulla scheda **Intervalli di rete** per creare un nuovo intervallo di rete oppure selezionarne uno esistente.

Vengono visualizzati i dettagli sull'intervallo selezionato, comprendenti nome, descrizione, indirizzo IP di inizio e di fine. Vengono inoltre fornite informazioni relative allo stato.

- 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 Range*n*.

- 3 Fare clic su **OK**.

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.

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.

Nota: 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. Lo storage e la memoria 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

- Hyper-V
- KVM
- OpenStack
- SCVMM
- XenServer

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.

Tavola 3-5. 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
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

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.

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.

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.

Creazione di una prenotazione Amazon

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. Vedere .

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 alla console di 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**.
- 3 (Facoltativo) Selezionare una prenotazione esistente dal menu a discesa **Copia da prenotazione esistente**.

Vengono visualizzati i dati provenienti dalla prenotazione selezionata. È possibile apportare le modifiche necessarie per la nuova prenotazione.

- 4 Immettere un nome nella casella di testo **Nome**.
- 5 Selezionare un tenant dal menu a discesa **Tenant**.
- 6 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.

- 7 (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.

- 8 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.

- 9 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

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.

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.

Opzione	Descrizione
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.
- 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.
- 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.

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 uno o più indirizzi email di utenti o nomi di gruppi per ricevere le notifiche degli avvisi.

Premere Invio per separare voci multiple.
- 11 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.
- 12 Specificare una frequenza per i promemoria (giorni).
- 13 Fare clic su **Salva**.

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Passi successivi

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 alla console di 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 (Facoltativo) Selezionare una prenotazione esistente dal menu a discesa **Copia da prenotazione esistente**.

Vengono visualizzati i dati provenienti dalla prenotazione selezionata. È possibile apportare le modifiche necessarie per la nuova prenotazione.

- 4 Immettere un nome nella casella di testo **Nome**.
- 5 Selezionare un tenant dal menu a discesa **Tenant**.
- 6 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.

- 7 (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.

- 8 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.

- 9 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

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 dall'elenco **Percorsi di rete** un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.
- c (Facoltativo) Selezionare un profilo di rete elencato dal menu a discesa **Profilo di rete**.

Questa opzione richiede l'esistenza di uno o più profili di rete.

È possibile selezionare più di un percorso di rete su una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

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 uno o più indirizzi email di utenti o nomi di gruppi per ricevere le notifiche degli avvisi.

Premere Invio per separare voci multiple.
- 11 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.
- 12 Specificare una frequenza per i promemoria (giorni).
- 13 Fare clic su **Salva**.

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Passi successivi

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.

Passi successivi

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 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 alla console di 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 (Facoltativo) Selezionare una prenotazione esistente dal menu a discesa **Copia da prenotazione esistente**.

Vengono visualizzati i dati provenienti dalla prenotazione selezionata. È possibile apportare le modifiche necessarie per la nuova prenotazione.

4 Immettere un nome nella casella di testo **Nome**.

5 Selezionare un tenant dal menu a discesa **Tenant**.

6 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.

7 (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.

8 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.

9 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

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 di vCloud Air e gli endpoint di vCloud Director non supportano l'utilizzo di profili di rete per il provisioning di 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 dall'elenco **Percorsi di rete** un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.
- c (Facoltativo) Selezionare un profilo di rete elencato dal menu a discesa **Profilo di rete**.

Questa opzione richiede l'esistenza di uno o più profili di rete.

È possibile selezionare più di un percorso di rete su una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

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 uno o più indirizzi email di utenti o nomi di gruppi per ricevere le notifiche degli avvisi.
Premere Invio per separare voci multiple.
- 13 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.
- 14 Specificare una frequenza per i promemoria (giorni).
- 15 Fare clic su **Salva**.

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.

Passi successivi

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 alla console di 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 (Facoltativo) Selezionare una prenotazione esistente dal menu a discesa **Copia da prenotazione esistente**.

Vengono visualizzati i dati provenienti dalla prenotazione selezionata. È possibile apportare le modifiche necessarie per la nuova prenotazione.

4 Immettere un nome nella casella di testo **Nome**.

5 Selezionare un tenant dal menu a discesa **Tenant**.

6 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.

7 (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.

8 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.

9 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

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 di vCloud Air e gli endpoint di vCloud Director non supportano l'utilizzo di profili di rete per il provisioning di 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 dall'elenco **Percorsi di rete** un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.
- c (Facoltativo) Selezionare un profilo di rete elencato dal menu a discesa **Profilo di rete**.

Questa opzione richiede l'esistenza di uno o più profili di rete.

È possibile selezionare più di un percorso di rete su una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

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 uno o più indirizzi email di utenti o nomi di gruppi per ricevere le notifiche degli avvisi.
Premere Invio per separare voci multiple.
- 13 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.
- 14 Specificare una frequenza per i promemoria (giorni).
- 15 Fare clic su **Salva**.

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

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 alla console di 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 AWS. Vedere [Scenario: configurazione di 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 AWS 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 AWS 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 AWS di accedere alle risorse di vRealize Automation. È necessario aggiungere proprietà personalizzate alla prenotazione per configurare gli agenti per accedere a dette porte.

Scenario: definizione delle informazioni di prenotazione di Amazon AWS 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.

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 AWS 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 AWS 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.

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 AWS di accedere alle risorse di vRealize Automation. È necessario aggiungere proprietà personalizzate alla prenotazione per configurare gli agenti per accedere a dette porte.

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 AWS e la porta 1443, assegnata per *vRealize_automation_appliance_fqdn* quando è stato invocato il tunnel SSH.

Opzione	Valore
software.ebs.url	<code>https://Private_IP:1443/event-broker-service/api</code>
software.agent.service.url	<code>https://Private_IP:1443/software-service/api</code>
agent.download.url	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

- 4 Fare clic su **Salva**.

È stata creata una prenotazione per allocare risorse di Amazon AWS 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.

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 quella 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 quella posizione che soddisfino tutti gli altri criteri, il provisioning può proseguire su un'altra prenotazione, indipendentemente dalla posizione. Questa è l'opzione predefinita.

- Se il blueprint o la richiesta specificano la proprietà personalizzata *VirtualMachine.Host.TpmEnabled*, è necessario installare hardware attendibile sulla 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 c'è un percorso di storage con capacità sufficiente all'interno del criterio di prenotazione di storage, il provisioning può procedere con un percorso di storage esterno al criterio di prenotazione di 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 virtualizzazione di rete e sicurezza di NSX

È possibile creare una prenotazione di vSphere per assegnare reti esterne e gateway instradati a profili di rete per reti di base, specificare la zona di trasporto e assegnare gruppi di sicurezza a componenti di macchine.

Se è stato configurato VMware NSX e installato il plug-in NSX per vRealize Automation, quando si crea o si modifica un blueprint è possibile specificare le impostazioni di NSX relative a zona di trasporto, criterio di prenotazione Edge e gateway instradato e isolamento app. Queste impostazioni sono disponibili nella scheda **Impostazioni NSX** nelle pagine **Nuovo blueprint** e **Proprietà blueprint**.

Le impostazioni dei componenti rete e sicurezza aggiunte alla tela di progettazione del blueprint derivano dalla configurazione di NSX e richiedono l'installazione preventiva del plug-inNSX e l'esecuzione di una raccolta dei dati per l'inventario di NSX per i cluster vSphere. I componenti rete e sicurezza sono specifici di NSX e sono disponibili solo per l'uso con componenti macchina vSphere. Per informazioni sulla configurazione di NSX, consultare la *guida di amministrazione di NSX*.

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.

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.

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.

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.

Quando si seleziona un gateway Edge o instradato e un profilo di rete in una prenotazione durante la configurazione di reti instradate, selezionare il percorso di rete da utilizzare per collegare le reti instradate e assegnargli il profilo di rete esterno utilizzato per configurare il profilo di rete instradato. 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.

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*.

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 alla console di 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 (Facoltativo) Selezionare una prenotazione esistente dal menu a discesa **Copia da prenotazione esistente**.
Vengono visualizzati i dati provenienti dalla prenotazione selezionata. È possibile apportare le modifiche necessarie per la nuova prenotazione.
- 4 Immettere un nome nella casella di testo **Nome**.
- 5 Selezionare un tenant dal menu a discesa **Tenant**.
- 6 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.
- 7 (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.
- 8 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.
- 9 (Facoltativo) Deselezionare la casella di controllo **Attiva questa prenotazione** se si desidera non attivare la prenotazione.

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.

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 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.

- 6 Se disponibile per la risorsa di elaborazione, selezionare un pool di risorse dal menu a discesa **Pool di risorse**.
- 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 dall'elenco **Percorsi di rete** un percorso di rete per le macchine fornite in provisioning utilizzando questa prenotazione.
- c (Facoltativo) Selezionare un profilo di rete elencato dal menu a discesa **Profilo di rete**.

Questa opzione richiede l'esistenza di uno o più profili di rete.

È possibile selezionare più di un percorso di rete su una prenotazione, ma solo una rete viene utilizzata nel provisioning di una macchina.

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 uno o più indirizzi email di utenti o nomi di gruppi per ricevere le notifiche degli avvisi.

Premere Invio per separare voci multiple.

- 12 Selezionare **Invia avvisi al manager gruppo** per includere i manager di gruppo negli avvisi via email.
- 13 Specificare una frequenza per i promemoria (giorni).
- 14 Fare clic su **Salva**.

La prenotazione è stata salvata e apparirà nell'elenco Prenotazioni.

Passi successivi

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, il valore del blueprint ha la precedenza. Ad esempio, se viene specificato un profilo di rete nel blueprint mediante la proprietà personalizzata `VirtualMachine.NetworkN.ProfileName` e in una prenotazione utilizzata dal blueprint, il profilo di rete specificato nel blueprint ha la precedenza. Se, tuttavia, la proprietà personalizzata non viene utilizzata nel blueprint e si seleziona un profilo di rete per una NIC della macchina, vRealize Automation utilizza il percorso di rete della prenotazione per la NIC della macchina per la quale è stato specificato il profilo di rete.

Nota: Queste informazioni non riguardano i Amazon Web Services.

Prerequisiti

- Accedere alla console di vRealize Automation come **amministratore di struttura**.
- Creare un profilo di rete. Vedere [Creazione di un profilo di rete](#).

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 di vCloud Air e gli endpoint di vCloud Director non supportano l'utilizzo di profili di rete per il provisioning di 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.

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 alla console di vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Criteri di prenotazione**.
- 2 Fare clic su **Aggiungi**.
- 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 **Aggiorna** per salvare il criterio.

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.

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 alla console di vRealize Automation come **amministratore di struttura**.

Procedura

- 1 Selezionare **Infrastruttura > Prenotazioni > Criteri di prenotazione**.
- 2 Fare clic su **Aggiungi**.
- 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 **Aggiorna** per salvare il criterio.

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 sull'icona **Salva** (✓).
- 8 Fare clic su **OK**.
- 9 (Facoltativo) Assegnare datastore aggiuntivi al criterio di prenotazione storage.

Scenario: configurazione di risorse IaaS per Rainpole

Utilizzando una combinazione dei privilegi di amministratore IaaS e amministratore tenant, è possibile creare un prefisso da apporre a macchine vSphere create in vRealize Automation, organizzare le risorse vSphere in un gruppo di strutture e assegnare risorse al gruppo personalizzato di architetti vRealize Automation.



Procedura

- 1 **Scenario: creazione di un componente gruppo di strutture per Rainpole**
Utilizzando i privilegi di amministratore IaaS, si supponga di creare un gruppo di strutture contenente le risorse di elaborazione scoperte durante la creazione dell'endpoint vSphere. Assegnare il gruppo personalizzato di architetti e sviluppatori vRealize Automation al ruolo di amministratore delle strutture a questo gruppo.
- 2 **Scenario: configurazione di prefissi di macchine per Rainpole**
Utilizzando i privilegi di amministratore di strutture, è possibile creare un prefisso configurabile per essere apposto alle macchine delle quali gli architetti e gli sviluppatori vRealize Automation hanno eseguito il provisioning durante lo sviluppo e il test.

3 Scenario: creazione di un gruppo di business per consentire agli architetti Rainpole di sottoporre a test gli elementi del catalogo

Utilizzando i privilegi di amministratore tenant, è possibile creare un gruppo di business per il team IT responsabile della progettazione e del collaudo dei blueprint vRealize Automation.

4 Scenario: creazione di una prenotazione per assegnare risorse agli architetti Rainpole

Utilizzando i privilegi di amministratore delle strutture, si supponga di creare una prenotazione per il gruppo di business Rainpole a cui allocare risorse vSphere.

Scenario: creazione di un componente gruppo di strutture per Rainpole

Utilizzando i privilegi di amministratore IaaS, si supponga di creare un gruppo di strutture contenente le risorse di elaborazione scoperte durante la creazione dell'endpoint vSphere. Assegnare il gruppo personalizzato di architetti e sviluppatori vRealize Automation al ruolo di amministratore delle strutture a questo gruppo.

Non è necessario creare un endpoint vSphere perché ne è già stato creato uno quando si richiede l'elemento del catalogo dei contenuti iniziale.

Procedura

- 1 Selezionare **Infrastruttura > Gruppi di strutture**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere **Rainpole fabric** nella casella di testo Nome.
- 4 Cercare gli **architetti Rainpole** nella casella di ricerca **Amministratori struttura** e selezionare il gruppo personalizzato.
- 5 Selezionare la risorsa di elaborazione dell'ambiente vSphere da includere nel gruppo di strutture.
- 6 Fare clic su **OK**.
- 7 Aggiornare il browser per visualizzare le nuove opzioni di menu disponibili per l'amministratore di strutture.

Passi successivi

Utilizzando i privilegi di amministratore delle strutture, è possibile creare un prefisso macchina che gli architetti Rainpole potranno usare in modo tale da identificare facilmente ogni macchina di cui eseguiranno il provisioning durante lo sviluppo e il test.

Scenario: configurazione di prefissi di macchine per Rainpole

Utilizzando i privilegi di amministratore di strutture, è possibile creare un prefisso configurabile per essere apposto alle macchine delle quali gli architetti e gli sviluppatori vRealize Automation hanno eseguito il provisioning durante lo sviluppo e il test.

Procedura

- 1 Selezionare **Infrastruttura > Amministrazione > Prefissi macchina**.

- 2 Fare clic su **Nuovo**.
- 3 Immettere **Rainpole** nella casella di testo **Prefisso macchina**.
- 4 Immettere **3** nella casella di testo **Numero di cifre**.
- 5 Immettere **1** nella casella di testo **Numero successivo**.
- 6 Fare clic sull'icona **Salva** (✓).

Passi successivi

Utilizzando i privilegi di amministratore tenant, è stato creato un gruppo di business per il team IT responsabile della progettazione e del collaudo dei blueprint vRealize Automation.

Scenario: creazione di un gruppo di business per consentire agli architetti Rainpole di sottoporre a test gli elementi del catalogo

Utilizzando i privilegi di amministratore tenant, è possibile creare un gruppo di business per il team IT responsabile della progettazione e del collaudo dei blueprint vRealize Automation.

Procedura

- 1 Selezionare **Amministrazione > Utenti e gruppi > Gruppi di business**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere **Rainpole business group** nella casella di testo **Nome**.
- 4 Immettere uno o più indirizzi e-mail nella casella di testo **Invia e-mail gestione a**.
Ad esempio, immettere il proprio indirizzo e-mail o l'indirizzo e-mail oppure quello del proprio responsabile IT.
- 5 Aggiungere una proprietà personalizzata per aiutare gli architetti nelle procedure di risoluzione dei problemi relativi ai blueprint.
 - a Fare clic sull'icona **Nuovo** (+).
 - b Immettere **_debug_deployment** nella casella di testo **Nome**.
 - c Immettere **true** nella casella di testo **Valore**.
 - d Selezionare **Richiedi conferma** per consentire agli architetti di attivare o disattivare questa funzionalità quando richiedono un elemento del catalogo.

In genere, se un componente di un elemento del catalogo non riesce a eseguire il provisioning, vRealize Automation esegue il rollback di tutte le risorse dell'intero elemento del catalogo. Questa proprietà personalizzata viene utilizzata per ignorare tale comportamento, in modo tale che gli architetti possano individuare gli errori dei blueprint. Questa proprietà personalizzata va aggiunta al gruppo di business anziché i blueprint per fare in modo che gli architetti possano sempre ignorare tale comportamento, ma tale opzione non viene mai fornita accidentalmente agli utenti.
- 6 Fare clic su **Avanti**.

- 7 Cercare gli **architetti Rainpole** nella casella di ricerca **Ruolo manager di gruppo** e selezionare il gruppo personalizzato.
- 8 Cercare **test_user** nella casella di ricerca **Ruolo utente** e selezionare l'utente locale da impostare come accesso condiviso per testare i blueprint.
- 9 Fare clic su **Avanti**.
- 10 Selezionare **Rainpole** come prefisso della macchina predefinito dal menu a discesa.
- 11 Fare clic su **Fine**.

Passi successivi

Utilizzando i privilegi di amministratore della struttura, assegnare le risorse IaaS al gruppo di business Rainpole creando una prenotazione.

Scenario: creazione di una prenotazione per assegnare risorse agli architetti Rainpole

Utilizzando i privilegi di amministratore delle strutture, si supponga di creare una prenotazione per il gruppo di business Rainpole a cui allocare risorse vSphere.

Nota: Dopo aver creato una prenotazione non è possibile cambiare il gruppo di business o la risorsa di elaborazione.

Procedura

- 1 Selezionare **Infrastrutture > Prenotazioni > Prenotazioni**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Selezionare **vSphere** dal menu a discesa.
- 4 Immettere le informazioni di prenotazione.

Opzione	Input
Nome	Prenotazione Rainpole
Tenant	vsphere.local
Gruppo di business	Gruppo di business Rainpole
Priorità	1

- 5 Selezionare la scheda **Risorse**.
- 6 Immettere le informazioni sulle risorse dall'ambiente di distribuzione.

Opzione	Input
Risorse di elaborazione	Selezionare un cluster di risorse dal menu a discesa.
Quota macchina	Specificare il numero massimo di macchine attive per per la prenotazione in questione.

Opzione	Input
Memoria	Specificare la quantità massima di memoria (in MB) utilizzabile dalla prenotazione in questione.
Storage	Selezionare uno o più percorsi di storage e prenotare spazio (in GB) per la prenotazione in questione. Attribuire priorità ai percorsi di storage, dove 1 è la priorità massima.

- 7 Selezionare la scheda **Rete**.
- 8 Selezionare almeno un percorso di rete vSphere.
- 9 Fare clic su **OK**.

Ora l'infrastruttura vSphere è sotto la gestione di vRealize Automation e le risorse vSphere sono state allocate al team.

Passi successivi

Utilizzando i privilegi di architetto IaaS, si creerà un blueprint di macchina per clonare le macchine CentOS vSphere.

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 alla console di 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.

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 [Scenario: abilitazione degli utenti a selezionare posizioni di datacenter per distribuzioni tra più regioni](#).

Elenco di controllo per il provisioning di una distribuzione di vRealize Automation mediante un provider IPAM esterno

È possibile ottenere indirizzi e intervalli IP per l'uso in un profilo di rete di vRealize Automation esterna ed esistente da un provider di soluzioni IPAM esterno supportato, come 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 di blueprint, si ottiene un indirizzo IP dall'intervallo di indirizzi IP specificato dall'IPAM Infoblox. Dopo la distribuzione della macchina, è possibile scoprire l'indirizzo IP utilizzato interrogando la relativa pagina dei dettagli degli elementi di vRealize Automation.

Tavola 3-6. Preparazione per il provisioning di una distribuzione di vRealize Automation mediante elenco di controllo dell'IPAM Infoblox

Attività	Posizione	Dettagli
<input type="checkbox"/> Ottenere, importare e configurare il plug-in o il pacchetto del provider di soluzioni IPAM esterno.	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 (https://solutionexchange.vmware.com/store/category_groups/cloud-management) non contiene il pacchetto del provider IPAM necessario, è possibile creare il proprio utilizzando l'SDK del provider di soluzioni IPAM e la documentazione di supporto.	Vedere Elenco di controllo per la preparazione del supporto di provider IPAM esterni .
<input type="checkbox"/> Creazione di un endpoint del provider di soluzioni IPAM esterno	Creare un nuovo endpoint IPAM in vRealize Automation.	Vedere Creazione di un endpoint del provider IPAM esterno .
<input type="checkbox"/> Specificare le impostazioni dell'endpoint del provider di soluzioni IPAM esterno 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 esterno .

Tavola 3-6. Preparazione per il provisioning di una distribuzione di vRealize Automation mediante elenco di controllo dell'IPAM Infoblox (Continua)

Attività	Posizione	Dettagli
<input type="checkbox"/> Definire una prenotazione per usare il profilo di rete esterna per un percorso di rete esistente.	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 .
<input type="checkbox"/> Definire un blueprint che utilizzi il profilo di rete esterna.	Creare un blueprint che utilizzi la prenotazione in vRealize Automation.	
<input type="checkbox"/> Autorizzare il blueprint e aggiungerlo al catalogo.	Autorizzare il blueprint e aggiungerlo al catalogo in vRealize Automation.	
<input type="checkbox"/> Richiedere il provisioning della macchina utilizzando l'elemento del catalogo di blueprint.	Utilizzare l'elemento del catalogo di blueprint per richiedere il provisioning della macchina in vRealize Automation	
<input type="checkbox"/> Eseguire una query per stabilire in quale indirizzo IP risiede la distribuzione utilizzando la pagina I miei elementi.	Determinare l'indirizzo IP di rete utilizzato per la distribuzione in vRealize Automation.	

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 alla console 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**.

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.

Passi successivi

- 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 alla console 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> <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.
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 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. b 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> <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.

11 Fare clic su **Fine**.

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, e utilizzare i risultati ottenuti.

Prerequisiti

- Assicurarsi di avere accesso a un host Windows PowerShell. Per ulteriori informazioni su Microsoft Windows PowerShell, vedere la documentazione di Windows PowerShell.
- Accedere alla console vRealize Automation come **amministratore tenant**.

Procedura

- 1 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 e, facoltativamente, una descrizione.
- 6 Fare clic su **Avanti**.
- 7 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**.
- 8 Selezionare il tipo di host PowerShell a cui si deve connettere il plug-in.

Opzione	Azione
WinRM	<ol style="list-style-type: none"> 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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Nota: Se si utilizza il protocollo di trasporto HTTPS, il certificato dell'host PowerShell remoto viene importato nel keystore di vRealize Orchestrator. </div> c Selezionare il tipo di autenticazione dal menu a discesa Autenticazione. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Nota: Per utilizzare l'autenticazione Kerberos, attivarla nel servizio WinRM. Per informazioni sulla configurazione dell'autenticazione Kerberos, vedere <i>Utilizzo del plug-in PowerShell</i>. </div>
SSH	Nessuno.

- 9 Immettere le credenziali per la comunicazione mediante una sessione condivisa con l'host PowerShell nelle caselle di testo **Nome utente** e **Password**.
- 10 Fare clic su **Fine**.

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 alla console 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> <ol 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.

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. 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> <ol style="list-style-type: none"> 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. 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> <ol style="list-style-type: none"> Fornire le credenziali dell'utente. <ol 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. Immettere il nome SPN del servizio Kerberos nella casella di testo SPN servizio Kerberos (Kerberos service SPN).

11 Fare clic su **Fine**.

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 alla console 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**.

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.

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 la preparazione del supporto di provider IPAM esterni](#).

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.

I criteri di Active Directory sono una funzionalità dell'anteprima tecnica in vRealize Automation 7.1 e non devono essere utilizzati in un ambiente di produzione.

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.

I criteri di Active Directory sono una funzionalità dell'anteprima tecnica in vRealize Automation 7.1 e non devono essere utilizzati in un ambiente di produzione.

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 alla console vRealize Automation come **amministratore tenant**.

Procedura

- 1 Selezionare **Amministrazione > Criteri AD**.
- 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**.

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.

Passi successivi

- 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**.

Il blueprint di test include la proprietà personalizzata, ma gli utenti non la vedono nel modulo di richiesta.

Passi successivi

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.

Fornitura di servizi su richiesta agli utenti

4

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:

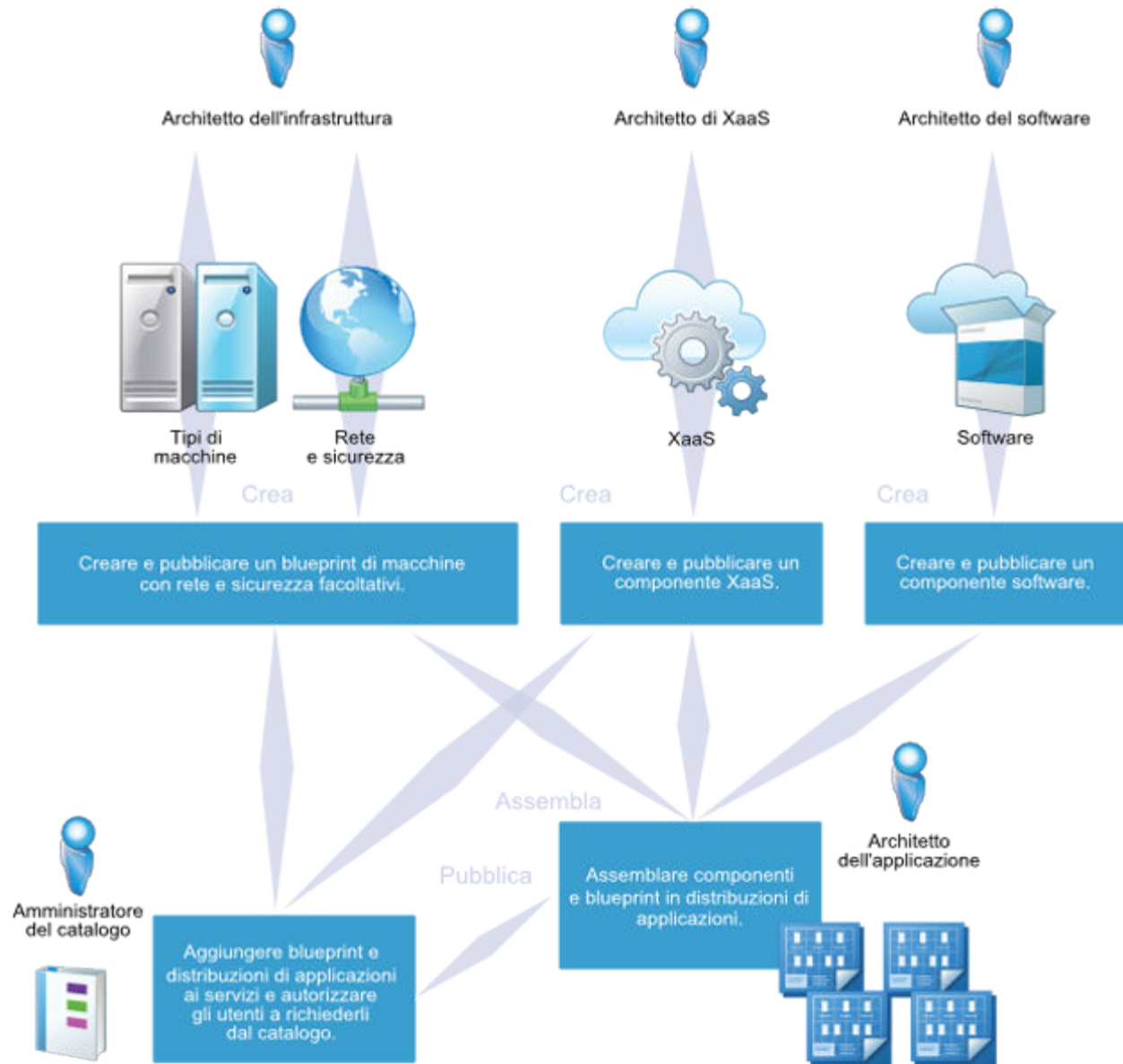
- [Progettazione dei blueprint](#)
- [Esportazione e importazione dei blueprint](#)
- [Creazione di una libreria di progettazione](#)
- [Assemblaggio di blueprint compositi](#)
- [Gestione del catalogo dei servizi](#)

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.

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.

Blueprint delle macchine

È possibile creare e pubblicare semplici blueprint per eseguire il provisioning di macchine singole, oppure è possibile creare blueprint multimacchina che contengono tipi di componenti macchina differenti. È possibile aggiungere anche componenti reti e sicurezza a blueprint di macchine, come i gruppi di sicurezza o i profili di rete.

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.

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.

Esportazione e importazione dei blueprint

È possibile esportare 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 contenuti di vRealize Automation:

- Blueprint di applicazioni e tutti i rispettivi componenti
- Blueprint di macchine IaaS
- Componenti di Software
- Blueprint di XaaS

■ 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>.

Tavola 4-1. Scelta dello strumento di importazione ed esportazione

Strumento	Ulteriori informazioni
vRealize CloudClient	Consultare il sito per gli sviluppatori di VMware all'indirizzo https://developercenter.vmware.com/tool/cloudclient .
API REST di vRealize Automation	Vedere <i>Guida alla programmazione</i> nel Centro informazioni di vRealize Automation all'indirizzo https://www.vmware.com/support/pubs/vcac-pubs.html .

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 esterno](#).
- 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 da vRealize Automation appliance. 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.

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 da vRealize Automation appliance. 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 a vRealize Automation appliance come root utilizzando SSH.

- 2 Scaricare Dukes Bank per l'applicazione campione di vSphere da vRealize Automation appliance in /tmp.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/DukesBankAppForvSphere.zip
```

Non decomprimere il pacchetto.

- 3 Scaricare Cloud Client versione 4.x da <http://developercenter.vmware.com/tool/cloudclient> in /tmp.
- 4 Decomprimere il pacchetto cloudclient-4x-dist.zip.
- 5 Eseguire Cloud Client nella directory /bin.

```
$>./bin/cloudclient.sh
```

- 6 Se richiesto, accettare il contratto di licenza.
- 7 Utilizzando Cloud Client, accedere a vRealize Automation appliance come utente con privilegi di **architetto software** e di **infrastrutture**.

```
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
```

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
```

Quando si accede alla console di vRealize Automation come utente con privilegi di **architetto software** e di **architetto di infrastrutture**, vengono visualizzati i blueprint e i componenti di Dukes Bank 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**.

Il blueprint dell'applicazione campione Dukes Bank è stato configurato per il proprio ambiente e il blueprint completato è stato pubblicato.

Passi successivi

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 di vRealize Automation appliance 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 di vRealize Automation appliance 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 **Richieste** e, dopo il provisioning dell'applicazione, visualizzare i dettagli dell'elemento di catalogo nella scheda **Elementi**.

- 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 Selezionare **Elementi > Distribuzioni**.
 - b Espandere la distribuzione dell'applicazione campione Dukes Bank e selezionare il server di bilanciamento del carico di Apache.
 - c Fare clic su **Visualizza dettagli**.
 - 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**.

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.

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.

Tavola 4-2. 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 di macchine con rete e sicurezza di NSX
Software su macchine	Architetto del software	Creare e pubblicare componenti Software dalla scheda Software , quindi combinarli con i blueprint delle macchine nella scheda Blueprint .	<p>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.</p> <p>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.</p>	Creazione di un componente Software

Tavola 4-2. 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.	Creazione 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"> ■ Architetti dell'applicazione ■ Architetti dell'infrastruttura ■ Architetti 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: 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 Net App FlexClone se si opera in un ambiente vSphere che utilizza storage NFS (Network File System) e 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 di macchine, ma il percorso di storage FlexClone si comporterà come uno storage standard.

L'elenco che segue è una panoramica ad alto livello 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 [Creazione di un endpoint NetApp ONTAP](#).
- 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, l'opzione FlexClone è visualizzata nella colonna dell'endpoint di una pagina di prenotazione. Se c'è un endpoint NetApp ONTAP, la pagina della prenotazione mostra 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.
- 4 Un architetto dell'infrastruttura o un altro utente autorizzato crea un blueprint per il provisioning FlexClone.

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.

Prerequisiti

- Accedere alla console di 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. [Capitolo 2 Configurazione delle impostazioni del tenant](#).
- Configurare le risorse IaaS. [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 Attenersi alle istruzioni presentate nelle diverse schede per configurare i dettagli relativi al provisioning della macchina.
- 8 Fare clic su **Fine**.
- 9 Selezionare il blueprint e fare clic su **Pubblica**.

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.

Passi successivi

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](#).

Impostazioni dei blueprint macchina

Di seguito sono elencate le impostazioni e le opzioni che è possibile configurare quando si creano blueprint di macchine.

Nuovo blueprint e impostazioni delle proprietà del blueprint

Di seguito sono elencate le impostazioni e le opzioni che è possibile configurare nella finestra di dialogo Nuovo blueprint. Dopo aver creato il blueprint, è possibile modificare le impostazioni nella finestra di dialogo Proprietà blueprint.

Scheda Generale

Consente di applicare le impostazioni nell'intero blueprint, inclusi tutti i componenti che si intende aggiungere in un dato momento o successivamente.

Tavola 4-3. 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. Dato che gli identificatori 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 riassume il blueprint a vantaggio di altri architetti. Questa descrizione viene anche visualizzata per gli utenti nel modulo di richiesta.
Giorni di archiviazione	Invece di eliminare le distribuzioni immediatamente alla scadenza del lease, è possibile specificare un periodo di archiviazione temporanea. Specificare 0 (impostazione predefinita) 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.
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.

Scheda Impostazioni NSX

Se è stato configurato VMware NSX e installato il plug-in NSX per vRealize Automation, quando si crea o si modifica un blueprint è possibile specificare le impostazioni di NSX relative a zona di trasporto, criterio di prenotazione Edge e gateway instradato e isolamento app. Queste impostazioni sono disponibili nella scheda **Impostazioni NSX** nelle pagine **Nuovo blueprint** e **Proprietà blueprint**.

Per informazioni sulle impostazioni di NSX, vedere [Nuovo blueprint e impostazione delle proprietà del blueprint con NSX](#).

Scheda **Proprietà**

Le proprietà personalizzate aggiunte al livello del blueprint si applicano all'intero blueprint, inclusi tutti i componenti. Tuttavia queste possono essere sovrascritte da proprietà personalizzate assegnate in una posizione successiva della catena di precedenza. Per ulteriori informazioni sull'ordine di precedenza delle proprietà personalizzate, vedere *Guida di riferimento alle proprietà personalizzate*.

Tavola 4-4. Impostazioni della scheda **Proprietà**

Scheda	Impostazione	Descrizione
Gruppi di proprietà	I gruppi di proprietà sono gruppi riutilizzabili pensati per semplificare l'aggiunta di proprietà personalizzate ai blueprint. Gli amministratori tenant e di struttura possono raggruppare le proprietà che vengono spesso usate insieme in modo da consentire di aggiungere a un blueprint un gruppo di proprietà anziché le singole proprietà personalizzate.	
	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 possibile anche trascinare 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. È possibile visualizzare queste proprietà unite per facilitare l'assegnazione delle priorità ai gruppi di proprietà.
Proprietà personalizzate	È possibile aggiungere singole proprietà personalizzate invece di gruppi di proprietà.	
	Nome	Per un elenco dei nomi e dei comportamenti delle proprietà personalizzate, vedere <i>Guida di riferimento alle proprietà personalizzate</i> .
	Valore	Immettere il valore della proprietà personalizzata.
	Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.

Tavola 4-4. Impostazioni della scheda Proprietà (Continua)

Scheda	Impostazione	Descrizione
	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.

Impostazioni dei componenti macchina di vSphere

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. vSphere è l'unico tipo di componente macchina che può utilizzare le impostazioni dei componenti rete e sicurezza di NSX nella tela di progettazione.

Scheda Generale

Configurare le impostazioni generali di un componente macchina di vSphere.

Tavola 4-5. 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, come vSphere, è possibile configurare la funzionalità delle posizioni per consentire agli utenti di selezionare la posizione di un particolare data center per il provisioning di una macchina richiesta. Per configurare completamente l'opzione, l'amministratore di sistema aggiunge informazioni sulla posizione del data center in un file di posizioni e un amministratore di struttura modifica una risorsa di elaborazione per associarla a una posizione.</p>

Tavola 4-5. Impostazioni della scheda Generale (Continua)

Impostazione	Descrizione
Criterio di prenotazione	<p>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. Creando criteri di prenotazione, gli amministratori di struttura offrono un mezzo utile e facoltativo per controllare come vengono elaborate le richieste di prenotazione, ad esempio per raggruppare le risorse per diversi livelli di servizi oppure per rendere più facilmente disponibile un tipo di risorsa specifica per uno scopo particolare. Se l'amministratore di struttura non ha configurato criteri di prenotazione, questo menu a discesa non conterrà opzioni disponibili.</p>
Prefisso macchina	<p>I prefissi macchina sono creati dagli amministratori di struttura e utilizzati per definire i nomi delle macchine fornite in provisioning. Se si seleziona l'opzione Utilizza impostazione predefinita gruppo, i nomi delle macchine di cui viene eseguito il provisioning dal blueprint vengono definiti in base al prefisso delle macchine configurate come predefinite per il gruppo di business dell'utente. Se non è configurato alcun prefisso macchina, ne viene generato uno in base al nome del gruppo di business. 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 non si desidera fornire agli utenti la scelta, l'immissione dello stesso valore nei campi Minimo e Massimo consente di configurare esattamente il numero di istanze per le quali eseguire il provisioning e disattivare le azioni di scalabilità per il componente macchina in questione.</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 secondo necessità. In alternativa, è possibile disabilitare la scalabilità configurando esattamente 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.

Tavola 4-6. 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> ■ LinkedClone <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> ■ NetAppFlexClone <p>Se gli amministratori di struttura hanno configurato le prenotazioni per utilizzare lo storage NetApp Flexclone, utilizzando questa tecnologia è possibile clonare copie di macchine dalle dimensioni ottimizzate.</p>

Tavola 4-6. 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 Esegue il provisioning di una macchina senza sistema operativo guest. ■ ExternalProvisioningWorkflow Crea una macchina a partire da un'istanza di macchina virtuale o un'immagine basata su cloud. ■ LinuxKickstartWorkflow 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. ■ VirtualSccmProvisioningWorkflow 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. ■ WIMImageWorkflow 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>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>
Clona da	<p>Per la clonazione o NetApp FlexClone, consente di selezionare un modello di macchina da cui eseguire la clonazione.</p> <p>Per cloni collegati, consente di selezionare una macchina dall'elenco delle macchine. 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>

Tavola 4-6. Scheda Informazioni build (Continua)

Impostazione	Descrizione
Clona da snapshot	<p>Per cloni collegati, consente di 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 sul menu a discesa e selezionare lo snapshot specifico dall'elenco.</p> <p>Questa opzione è disponibile 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 il componente macchina di vSphere.

Tavola 4-7. Scheda Risorse macchina

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU di cui è possibile effettuare il provisioning tramite questo componente macchina.
Memoria (MB): Minimo e Massimo	Immettere una quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina.
Storage (GB): Minimo e Massimo	<p>Immettere una quantità minima e massima di storage che può essere utilizzato dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina. Per vSphere, KVM (RHEV), SCVMM, vCloud Air e vCloud Director, lo storage minimo è impostato in base al valore immesso nella scheda Storage.</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>

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.

Tavola 4-8. 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.
Etichetta	Consente di specificare un'etichetta per la lettera di unità e un percorso di montaggio per il volume di storage.
Criterio di prenotazione storage	Consente di specificare il criterio di prenotazione storage da utilizzare con questo volume di storage.
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 del blueprint.

Per informazioni sull'aggiunta e la configurazione di componenti rete e sicurezza di NSX prima di utilizzare le impostazioni della scheda Rete in un componente macchina vSphere, vedere [Configurazione delle impostazioni dei componenti rete e sicurezza](#).

Per informazioni sulla definizione di impostazioni di NSX a livello di blueprint che si applicano a componenti macchina vSphere, vedere [Nuovo blueprint e impostazione delle proprietà del blueprint con NSX](#).

Tavola 4-9. 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 del blueprint.
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 DCHP 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.
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 disabilitare 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 del blueprint.

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 del blueprint.

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](#).

Per informazioni sulla specifica di informazioni NSX a livello di blueprint che si applicano ai componenti macchina vSphere, vedere [Nuovo blueprint e impostazione delle proprietà del blueprint con NSX](#).

Tavola 4-10. 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 del blueprint. 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.

Tavola 4-10. Impostazioni della scheda Sicurezza (Continua)

Impostazione	Descrizione
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

Facoltativamente 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 possibile aggiungere proprietà e gruppi di proprietà personalizzate anche per l'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint dalla pagina **Nuovo blueprint** o **Proprietà blueprint**, rispettivamente.

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.

Tavola 4-11. 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. Ad esempio, immettere il nome della proprietà personalizzata <code>Machine.SSH</code> per specificare se le macchine di cui è stato eseguito il provisioning mediante questo blueprint consentono connessioni SSH. 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 mediante SSH alle macchine di cui è stato eseguito il provisioning mediante il blueprint.
Codificato	Si può scegliere di codificare il valore di una proprietà, ad esempio se il valore è una password.

Tavola 4-11. 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. 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.

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.

Tavola 4-12. 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 elencati 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	Visualizza tutte le proprietà personalizzate nei gruppi di proprietà elencati nell'ordine in cui appaiono nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi di proprietà, il nome della proprietà compare solo una volta nell'elenco in base alla sua prima occorrenza nell'elenco.

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.

Tavola 4-13. 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, come vSphere, è possibile configurare la funzionalità delle posizioni per consentire agli utenti di selezionare la posizione di un particolare data center per il provisioning di una macchina richiesta. Per configurare completamente l'opzione, l'amministratore di sistema aggiunge informazioni sulla posizione del data center in un file di posizioni e un amministratore di struttura modifica una risorsa di elaborazione per associarla a una posizione.</p>
Criterio di prenotazione	<p>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. Creando criteri di prenotazione, gli amministratori di struttura offrono un mezzo utile e facoltativo per controllare come vengono elaborate le richieste di prenotazione, ad esempio per raggruppare le risorse per diversi livelli di servizi oppure per rendere più facilmente disponibile un tipo di risorsa specifica per uno scopo particolare. Se l'amministratore di struttura non ha configurato criteri di prenotazione, questo menu a discesa non conterrà opzioni disponibili.</p>
Prefisso macchina	<p>I prefissi macchina sono creati dagli amministratori di struttura e utilizzati per definire i nomi delle macchine fornite in provisioning. Se si seleziona l'opzione Utilizza impostazione predefinita gruppo, i nomi delle macchine di cui viene eseguito il provisioning dal blueprint vengono definiti in base al prefisso delle macchine configurate come predefinite per il gruppo di business dell'utente. Se non è configurato alcun prefisso macchina, ne viene generato uno in base al nome del gruppo di business.</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 non si desidera fornire agli utenti la scelta, l'immissione dello stesso valore nei campi Minimo e Massimo consente di configurare esattamente il numero di istanze per le quali eseguire il provisioning e disattivare le azioni di scalabilità per il componente macchina in questione.</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 secondo necessità. In alternativa, è possibile disabilitare la scalabilità configurando esattamente 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.

Tavola 4-14. 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>Sono disponibili le seguenti azioni:</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>
Provisioning workflow	<p>Le opzioni visualizzate nel menu a discesa provisioning workflow dipendono dal tipo di macchina selezionato e dall'azione selezionata.</p> <p>Sono disponibili le seguenti azioni:</p> <ul style="list-style-type: none"> ■ CloneWorkflow <p>Crea copie di una macchina virtuale mediante clone, clone collegato o Netapp Flexclone.</p>
Clona da	<p>Per la clonazione o NetApp FlexClone, consente di selezionare un modello di macchina da cui eseguire la clonazione.</p> <p>Per cloni collegati, consente di selezionare una macchina dall'elenco delle macchine. 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.

Tavola 4-15. Scheda Risorse macchina

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU di cui è possibile effettuare il provisioning tramite questo componente macchina.
Memoria (MB): Minimo e Massimo	Immettere una quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina.
Storage (GB): Minimo e Massimo	Immettere una quantità minima e massima di storage che può essere utilizzato dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina. Per vSphere, KVM (RHEV), SCVMM, vCloud Air e vCloud Director, lo storage minimo è impostato in base al valore immesso nella scheda Storage.

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.

Tavola 4-16. 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.
Etichetta	Consente di specificare un'etichetta per la lettera di unità e un percorso di montaggio per il volume di storage.
Criterio di prenotazione storage	Consente di specificare il criterio di prenotazione storage da utilizzare con questo volume di storage.
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 possibile aggiungere proprietà e gruppi di proprietà personalizzate anche per l'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint dalla pagina **Nuovo blueprint** o **Proprietà blueprint**, rispettivamente.

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.

Tavola 4-17. 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. Ad esempio, immettere il nome della proprietà personalizzata <code>Machine.SSH</code> per specificare se le macchine di cui è stato eseguito il provisioning mediante questo blueprint consentono connessioni SSH. 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 mediante SSH alle macchine di cui è stato eseguito il provisioning mediante il blueprint.
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 .

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.

Tavola 4-18. 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 elencati 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	Visualizza tutte le proprietà personalizzate nei gruppi di proprietà elencati nell'ordine in cui appaiono nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi di proprietà, il nome della proprietà compare solo una volta nell'elenco in base alla sua prima occorrenza nell'elenco.

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.

Tavola 4-19. 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, come vSphere, è possibile configurare la funzionalità delle posizioni per consentire agli utenti di selezionare la posizione di un particolare data center per il provisioning di una macchina richiesta. Per configurare completamente l'opzione, l'amministratore di sistema aggiunge informazioni sulla posizione del data center in un file di posizioni e un amministratore di struttura modifica una risorsa di elaborazione per associarla a una posizione.</p>

Tavola 4-19. Impostazioni della scheda Generale (Continua)

Impostazione	Descrizione
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. Creando criteri di prenotazione, gli amministratori di struttura offrono un mezzo utile e facoltativo per controllare come vengono elaborate le richieste di prenotazione, ad esempio per raggruppare le risorse per diversi livelli di servizi oppure per rendere più facilmente disponibile un tipo di risorsa specifica per uno scopo particolare. Se l'amministratore di struttura non ha configurato criteri di prenotazione, questo menu a discesa non conterrà opzioni disponibili.
Prefisso macchina	I prefissi macchina sono creati dagli amministratori di struttura e utilizzati per definire i nomi delle macchine fornite in provisioning. Se si seleziona l'opzione Utilizza impostazione predefinita gruppo , i nomi delle macchine di cui viene eseguito il provisioning dal blueprint vengono definiti in base al prefisso delle macchine configurate come predefinite per il gruppo di business dell'utente. Se non è configurato alcun prefisso macchina, ne viene generato uno in base al nome del gruppo di business. 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.
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 non si desidera fornire agli utenti la scelta, l'immissione dello stesso valore nei campi Minimo e Massimo consente di configurare esattamente il numero di istanze per le quali eseguire il provisioning e disattivare le azioni di scalabilità per il componente macchina in questione.</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 secondo necessità. In alternativa, è possibile disabilitare la scalabilità configurando esattamente 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.

Tavola 4-20. 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> <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.
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>

Tavola 4-20. 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 VPC (Virtual Private Cloud) 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.

Tavola 4-21. Scheda Risorse macchina

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU di cui è possibile effettuare il provisioning tramite questo componente macchina.
Memoria (MB): Minimo e Massimo	Immettere una quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina.
Storage (GB): Minimo e Massimo	Immettere una quantità minima e massima di storage che può essere utilizzato dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina. Per vSphere, KVM (RHEV), SCVMM, vCloud Air e vCloud Director, lo storage minimo è impostato in base al valore immesso nella scheda Storage.
Storage EBS (GB): Minimo e Massimo	<p>Immettere una quantità minima e massima di volume di storage Amazon Elastic Block Store (EBS) utilizzabile dalle risorse macchina di cui è stato effettuato il provisioning tramite questo componente macchina.</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>

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 possibile aggiungere proprietà e gruppi di proprietà personalizzate anche per l'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint dalla pagina **Nuovo blueprint** o **Proprietà blueprint**, rispettivamente.

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.

Tavola 4-22. 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. Ad esempio, immettere il nome della proprietà personalizzata <code>Machine.SSH</code> per specificare se le macchine di cui è stato eseguito il provisioning mediante questo blueprint consentono connessioni SSH. 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 mediante SSH alle macchine di cui è stato eseguito il provisioning mediante il blueprint.
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 .

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.

Tavola 4-23. 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 elencati 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	Visualizza tutte le proprietà personalizzate nei gruppi di proprietà elencati nell'ordine in cui appaiono nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi di proprietà, il nome della proprietà compare solo una volta nell'elenco in base alla sua prima occorrenza nell'elenco.

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.

Tavola 4-24. 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, come vSphere, è possibile configurare la funzionalità delle posizioni per consentire agli utenti di selezionare la posizione di un particolare data center per il provisioning di una macchina richiesta. Per configurare completamente l'opzione, l'amministratore di sistema aggiunge informazioni sulla posizione del data center in un file di posizioni e un amministratore di struttura modifica una risorsa di elaborazione per associarla a una posizione.</p>

Tavola 4-24. Impostazioni della scheda Generale (Continua)

Impostazione	Descrizione
Criterio di prenotazione	<p>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. Creando criteri di prenotazione, gli amministratori di struttura offrono un mezzo utile e facoltativo per controllare come vengono elaborate le richieste di prenotazione, ad esempio per raggruppare le risorse per diversi livelli di servizi oppure per rendere più facilmente disponibile un tipo di risorsa specifica per uno scopo particolare. Se l'amministratore di struttura non ha configurato criteri di prenotazione, questo menu a discesa non conterrà opzioni disponibili.</p>
Prefisso macchina	<p>I prefissi macchina sono creati dagli amministratori di struttura e utilizzati per definire i nomi delle macchine fornite in provisioning. Se si seleziona l'opzione Utilizza impostazione predefinita gruppo, i nomi delle macchine di cui viene eseguito il provisioning dal blueprint vengono definiti in base al prefisso delle macchine configurate come predefinite per il gruppo di business dell'utente. Se non è configurato alcun prefisso macchina, ne viene generato uno in base al nome del gruppo di business. 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 non si desidera fornire agli utenti la scelta, l'immissione dello stesso valore nei campi Minimo e Massimo consente di configurare esattamente il numero di istanze per le quali eseguire il provisioning e disattivare le azioni di scalabilità per il componente macchina in questione.</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 secondo necessità. In alternativa, è possibile disabilitare la scalabilità configurando esattamente 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.

Tavola 4-25. 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 di macchina OpenStack disponibile. Le immagini delle macchine OpenStack sono modelli contenenti una configurazione software, che include un sistema operativo. Le immagini delle macchine sono gestite da account di OpenStack.

Tavola 4-25. 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.

Tavola 4-26. Scheda Risorse macchina

Impostazione	Descrizione
CPU: Minimo e Massimo	Immettere un numero minimo e massimo di CPU di cui è possibile effettuare il provisioning tramite questo componente macchina.
Memoria (MB): Minimo e Massimo	Immettere una quantità minima e massima di memoria che può essere utilizzata dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina.
Storage (GB): Minimo e Massimo	<p>Immettere una quantità minima e massima di storage che può essere utilizzato dalle macchine di cui è stato effettuato il provisioning tramite questo componente macchina. Per vSphere, KVM (RHEV), SCVMM, vCloud Air e vCloud Director, lo storage minimo è impostato in base al valore immesso nella scheda Storage.</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>

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 possibile aggiungere proprietà e gruppi di proprietà personalizzate anche per l'intero blueprint utilizzando la scheda **Proprietà** quando si crea o si modifica un blueprint dalla pagina **Nuovo blueprint** o **Proprietà blueprint**, rispettivamente.

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.

Tavola 4-27. 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. Ad esempio, immettere il nome della proprietà personalizzata <code>Machine.SSH</code> per specificare se le macchine di cui è stato eseguito il provisioning mediante questo blueprint consentono connessioni SSH. 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 mediante SSH alle macchine di cui è stato eseguito il provisioning mediante il blueprint.
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 .

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.

Tavola 4-28. 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 elencati in ordine decrescente. Un gruppo di proprietà elencato prima ha la precedenza sui gruppi di proprietà elencati dopo e così via.

Tavola 4-28. Impostazioni della scheda Proprietà > Gruppi di proprietà (Continua)

Impostazione	Descrizione
Visualizza proprietà	Visualizza le proprietà personalizzate nel gruppo di proprietà selezionato.
Visualizza proprietà unite	Visualizza tutte le proprietà personalizzate nei gruppi di proprietà elencati nell'ordine in cui appaiono nell'elenco dei gruppi di proprietà. Quando la stessa proprietà è presente in più gruppi di proprietà, il nome della proprietà compare solo una volta nell'elenco in base alla sua prima occorrenza nell'elenco.

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.

Causa

Le cause possibili dei problemi più frequenti ai blueprint di cloni e cloni collegati sono molteplici.

Tavola 4-29. 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.
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).

Tavola 4-29. Cause dei problemi più frequenti ai blueprint di cloni e cloni collegati (Continua)

Problema	Causa	Soluzione
Il provisioning del clone collegato non riesce quando si utilizza SDRS	Quando si utilizza il provisioning del clone collegato e SDRS, la nuova macchina deve trovarsi nello stesso cluster. Se i dischi della macchina di origine si trovano in un cluster e si chiede di eseguire il provisioning di una macchina in un cluster diverso, si verifica un errore di provisioning.	Quando si utilizza SDRS e il provisioning del clone collegato, effettuare il provisioning delle macchine nello stesso cluster dell'origine del clone collegato. Non effettuare il provisioning in un cluster diverso.
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.

Aggiunta di proprietà di rete e sicurezza a un componente macchina

I componenti macchina non vSphere non hanno una scheda Rete e sicurezza. Per aggiungere opzioni di rete e sicurezza a componenti macchina non vSphere nella tela di progettazione del blueprint, utilizzare le proprietà personalizzate.

I componenti **Rete e sicurezza** sono disponibili solo per l'uso con componenti macchina vSphere.

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 del blueprint. Le proprietà del 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*.

Scenario: creazione di un blueprint CentOS di vSphere per la clonazione in Rainpole

Utilizzando i privilegi di architetto di IaaS, creare e pubblicare un blueprint di base per la clonazione di macchine CentOS di vSphere.



Dopo aver pubblicato il blueprint, altri architetti possono riutilizzarlo come componente in nuovi blueprint. Nessuno potrà vedere o richiedere il blueprint dal catalogo finché non si utilizzeranno i propri privilegi di amministratore tenant per renderlo disponibile alle richieste.

Procedura

1 Scenario: creazione di un blueprint per il componente macchina Rainpole

Utilizzando i propri privilegi di architetto IaaS, creare un blueprint e configurare il nome e la descrizione per il blueprint di macchine CentOS di vSphere. Al blueprint viene assegnato un identificatore univoco, in modo da poter interagire con i blueprint tramite programma o creare binding di proprietà, se necessario. Per concedere agli utenti un certo grado di flessibilità con i lease dei loro blueprint, è possibile configurare il blueprint per permettere agli utenti di scegliere la durata del lease fino a un massimo di un mese.

2 Scenario: configurazione dei dettagli generali per il componente macchina Rainpole

Utilizzando i propri privilegi di architetto di IaaS, trascinare un componente macchina vSphere sulla tela di progettazione e configurare i dettagli generali per le macchine con provisioning eseguito utilizzando il blueprint.

3 Scenario: definizione delle informazioni build per il componente macchina Rainpole

Utilizzando i privilegi di architetto di IaaS, configurare il blueprint per clonare macchine dal modello di CentOS creato in vSphere.

4 Scenario: configurazione delle risorse per le macchine Rainpole

Utilizzando i privilegi di architetto IaaS, è possibile attribuire agli utenti parametri minimi e massimi per la memoria e il numero di CPU consentite. In questo modo vengono conservate risorse e soddisfatte le esigenze degli utenti.

Scenario: creazione di un blueprint per il componente macchina Rainpole

Utilizzando i propri privilegi di architetto IaaS, creare un blueprint e configurare il nome e la descrizione per il blueprint di macchine CentOS di vSphere. Al blueprint viene assegnato un identificatore univoco, in modo da poter interagire con i blueprint tramite programma o creare binding di proprietà, se necessario. Per concedere agli utenti un certo grado di flessibilità con i lease dei loro blueprint, è possibile configurare il blueprint per permettere agli utenti di scegliere la durata del lease fino a un massimo di un mese.

Procedura

1 Scegliere **Progettazione > Blueprint**.

2 Fare clic sull'icona **Nuovo** (+).

3 Immettere **Centos on vSphere** nella casella di testo **Nome**.

4 Rivedere l'identificatore univoco generato.

È possibile modificare il campo, ma dopo aver salvato il blueprint il campo non potrà più essere modificato. Dato che gli identificatori sono permanenti e unici all'interno del tenant, è possibile utilizzarli per interagire con i blueprint tramite programmazione e per creare binding di proprietà.

Il campo dell'identificatore viene compilato automaticamente in base al nome immesso.

5 Immettere **Configurazione macchina Golden Standard CentOS** nella casella di testo **Descrizione**.

6 Configurare un intervallo di lease da cui possono scegliere gli utenti immettendo **1** nella casella di testo **Minimo** e **30** nella casella di testo **Massimo**.

7 Fare clic su **OK**.

Passi successivi

Trascinare un componente macchina vSphere sulla tela e configurarlo per clonare il modello CentOS creato in vSphere.

Scenario: configurazione dei dettagli generali per il componente macchina Rainpole

Utilizzando i propri privilegi di architetto di IaaS, trascinare un componente macchina vSphere sulla tela di progettazione e configurare i dettagli generali per le macchine con provisioning eseguito utilizzando il blueprint.

La configurazione dei componenti macchina è permessa ai soli architetti di IaaS. Gli architetti di applicazioni e Software possono utilizzare i componenti macchina solo riutilizzando i blueprint delle macchine pubblicate creati.

Procedura

1 Fare clic sulla categoria **Tipi di macchine** nel riquadro di navigazione a sinistra.

Nel pannello inferiore vengono mostrati i tipi di componenti macchina.

2 Trascinare e rilasciare un componente macchina vSphere sulla tela.

3 Immettere **Macchina CentOS golden standard** nella casella di testo **Descrizione**.

4 Selezionare **Utilizza impostazione predefinita gruppo** dal menu a discesa **Prefisso macchina**.

Se si intende importare questi blueprint in altri ambienti, selezionando il prefisso predefinito del gruppo invece del prefisso di Rainpole specifico consente di evitare la configurazione del blueprint affinché funzioni con un prefisso macchina che potrebbe non essere disponibile.

Passi successivi

Configurare i componenti macchina per clonare macchine dal modello CentOS creato.

Scenario: definizione delle informazioni build per il componente macchina Rainpole

Utilizzando i privilegi di architetto di IaaS, configurare il blueprint per clonare macchine dal modello di CentOS creato in vSphere.

Configurare i componenti macchina per l'esecuzione dell'azione di clonazione e selezionare il modello creato come oggetto dal quale eseguire la clonazione. Immettere la specifica di personalizzazione, creata per evitare eventuali conflitti causati dalla distribuzione di più macchine virtuali con impostazioni identiche.

Procedura

- 1 Fare clic sulla scheda **Informazioni build**.
- 2 Dal menu a discesa **Tipo di blueprint** selezionare la classificazione Desktop o Server delle macchine di cui viene eseguito il provisioning da questo blueprint.
Queste informazioni hanno solo finalità di conservazione registri e gestione licenze.
- 3 Selezionare **Clona** dal menu a discesa **Azione**.
- 4 Selezionare **CloneWorkflow** dal menu a discesa **Provisioning workflow**.
- 5 Fare clic sull'icona **Sfoglia** accanto alla casella di testo **Clone da**.
- 6 Selezionare **Rainpole_centos_63_x86** per clonare macchine dal modello creato in vSphere.
- 7 Fare clic su **OK**.
- 8 Immettere **Linux** nella casella di testo **Specifica personalizzazione** per utilizzare la specifica di personalizzazione creata in vSphere.

Nota: Per questo valore viene fatta distinzione tra lettere maiuscole e minuscole.

Passi successivi

Configurare le impostazioni di CPU, memoria e storage per le macchine con provisioning eseguito utilizzando il blueprint.

Scenario: configurazione delle risorse per le macchine Rainpole

Utilizzando i privilegi di architetto IaaS, è possibile attribuire agli utenti parametri minimi e massimi per la memoria e il numero di CPU consentite. In questo modo vengono conservate risorse e soddisfatte le esigenze degli utenti.

Gli architetti del software e gli architetti delle applicazioni non possono configurare i componenti delle macchine, ma possono riutilizzare blueprint contenenti componenti delle macchine. Una volta terminato di modificare il componente della macchina, sarà necessario pubblicare il blueprint in modo che altri architetti possano riutilizzare il blueprint della macchina per progettare i loro elementi del catalogo. Il blueprint pubblicato è anche disponibile per gli amministratori del catalogo e gli amministratori tenant per l'inclusione nel catalogo dei servizi.

Procedura

- 1 Fare clic sulla scheda **Risorse macchina**.

2 Specificare le impostazioni della CPU per le macchine fornite in provisioning.

- a Immettere **1** nella casella di testo **Minimo**.
- b Immettere **4** nella casella di testo **Massimo**.

3 Specificare le impostazioni di memoria per le macchine fornite in provisioning.

- a Immettere **1024** nella casella di testo **Minimo**.

Questo campo viene compilato automaticamente in base alla memoria del modello.

- b Immettere **4096** nella casella di testo **Massimo**.

4 Specificare le impostazioni di storage per le macchine fornite in provisioning.

Alcuni dati relativi allo storage vengono compilati in base alla configurazione del modello, ma è possibile aggiungere ulteriore storage.

- a Fare clic sull'icona **Nuovo** (+).
- b Immettere **10** nella casella di testo **Capacità**.
- c Fare clic su **OK**.

5 Fare clic su **Fine**.

6 Selezionare la riga contenente CentOS on vSphere e fare clic su **Pubblica**.

È stato creato un blueprint pronto per il catalogo per offrire macchine vSphere CentOS clonate agli utenti e da riutilizzare in altri blueprint come standard per le macchine CentOS.

Passi successivi

Utilizzando i privilegi di amministratore tenant, creare un servizio di catalogo con cui gli architetti potranno convalidare i loro blueprint. Pubblicare CentOS su blueprint di macchine vSphere come elemento del catalogo e richiedere che verifichi il lavoro.

Scenario: conversione di una macchina Rainpole in una base per la fornitura di componenti Software

Utilizzando i privilegi di architetto di IaaS, creare un blueprint che supporti componenti Software utilizzando uno snapshot della macchina con provisioning eseguito come macchina di riferimento da cui clonare. Per supportare componenti Software, installare l'agente guest e l'agente di avvio automatico sulla macchina con provisioning eseguito prima di creare lo snapshot.



Procedura

1 Scenario: installazione dell'agente guest e dell'agente di avvio automatico di Software sulla macchina Rainpole

Utilizzando i privilegi di manager del gruppo di business, accedere alla macchina Rainpole001 di cui è stato eseguito il provisioning come utente di test. Installare l'agente guest e l'agente di avvio automatico di Software sulla macchina da preparare per il provisioning del Software. Terminata l'operazione, creare uno snapshot della macchina da utilizzare come base per clonare macchine da utilizzare con componenti Software.

2 Scenario: creazione di un blueprint clone collegato basato su uno snapshot di Rainpole

Utilizzando i privilegi di architetto IaaS, si desidera fornire agli architetti software copie con ottimizzazione dello spazio della macchina CentOS con provisioning preparata.

Scenario: installazione dell'agente guest e dell'agente di avvio automatico di Software sulla macchina Rainpole

Utilizzando i privilegi di manager del gruppo di business, accedere alla macchina Rainpole001 di cui è stato eseguito il provisioning come utente di test. Installare l'agente guest e l'agente di avvio automatico di Software sulla macchina da preparare per il provisioning del Software. Terminata l'operazione, creare uno snapshot della macchina da utilizzare come base per clonare macchine da utilizzare con componenti Software.

Procedura

- 1 Selezionare **Elementi > Macchine**.
- 2 Fare clic su CentOS sull'elemento vSphere per visualizzare i dettagli dell'elemento.
- 3 Fare clic su **Connetti a console remota** dal menu Azioni a destra.
- 4 Accedere alla macchina come utente root.
- 5 Scaricare lo script d'installazione da vRealize Automation appliance.

```
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
```

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

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

7 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.

8 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.

9 Tornare alla console di vRealize Automation e creare lo snapshot.

- a Fare clic su **Crea snapshot** dal menu Azioni a destra e seguire le istruzioni visualizzate.
- b Fare clic sulla scheda **Snapshot** per monitorare il processo.

Sono stati installati l'agente di avvio automatico software e l'agente guest, in modo da poter utilizzare lo snapshot come base di clonazione nei blueprint che contengono componenti software.

Scenario: creazione di un blueprint clone collegato basato su uno snapshot di Rainpole

Utilizzando i privilegi di architetto IaaS, si desidera fornire agli architetti software copie con ottimizzazione dello spazio della macchina CentOS con provisioning preparata.

Si procede innanzitutto alla copia del blueprint vSphere CentOS, quindi si modifica la copia per creare copie clone collegate dello snapshot preparato. I cloni collegati utilizzano una catena di dischi delta per tenere traccia delle differenze rispetto a una macchina padre. Vengono sottoposti a provisioning rapidamente, riducono i costi di storage e sono ideali quando le prestazioni non sono considerate prioritarie.

Procedura

1 Scegliere **Progettazione > Blueprint**.

2 Selezionare la riga contenente CentOS su vSphere e fare clic su **Copia**.

È stata creata una copia indipendente del blueprint della macchina CentOS su vSphere.

3 Immettere il nome **CentOS per il test del software** nella casella di testo **Nome**.

4 Immettere il nome **vSphere CentOS spazialmente efficiente per il test del software** nella casella di testo **Descrizione**.

5 Fare clic su **OK**.

6 Selezionare il componente macchina sulla tela per modificarne i dettagli.

7 Fare clic sulla scheda **Informazioni build**.

8 Selezionare **Clone collegato** dal menu a discesa **Azione**.

9 Fare clic sull'icona **Sfoglia** accanto alla casella di testo **Clone da**.

- 10 Selezionare la macchina sottoposta a provisioning **Rainpole001** su cui si installano gli agenti di avvio automatico software e guest.
- 11 Selezionare lo snapshot dal menu a discesa **Clona da snapshot**.
- 12 Fare clic su **Fine**.
- 13 Selezionare la riga contenente CentOS per il test del software e fare clic su **Pubblica**.

È possibile creare un blueprint clone collegato utilizzabile, anche con gli architetti, per fornire software su macchine CentOS.

Passi successivi

Usare i privilegi di architetto software per creare un componente Software per installare MySQL.

Aggiunta del supporto delle connessioni RDP ai blueprint di macchine Windows

Per consentire agli amministratori del catalogo di autorizzare utenti all'azione Connessione con RDP per i blueprint Windows, è necessario aggiungere le proprietà personalizzate RDP al blueprint della macchina e fare riferimento al file RDP personalizzato preparato dall'amministratore di 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 alla console di 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 Selezionare **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
(Obbligatorio)RDP.File.Name	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.
(Obbligatorio) VirtualMachine.Rdp.SettingN	Configura impostazioni di RDP specifiche. <i>N</i> è un numero unico utilizzato per distinguere un'impostazione RDP da un'altra. Ad esempio, per specificare il livello di autenticazione 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> . Utilizzare per aprire un collegamento RDP per specificare le impostazioni. Per conoscere l'elenco delle impostazioni disponibili e la sintassi corretta, consultare la documentazione di RDP di Microsoft Windows.
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 contenente il blueprint e fare clic su **Pubblica**.

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.

Scenario: aggiunta della pulitura 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 CentOS di vSphere esistente per configurare il plug-in Cleanup 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
- Disabilitare 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 alla console di 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, disabilitare, 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 [Scenario: creazione di un blueprint CentOS di vSphere per la clonazione in Rainpole](#).

Procedura

- 1 Selezionare **Progettazione > Blueprint**.
- 2 Puntare sul blueprint **Centos on vSphere** 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 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, disabilitare, 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**.

L'ambiente Active Directory verrà aggiornato ogni volta che macchine con provisioning eseguito dal blueprint saranno eliminate dall'hypervisor.

Scenario: 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. Per far ciò, l'architetto dovrà modificare il blueprint vSphere di CentOS 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 alla console di vRealize Automation come **architetto dell'infrastruttura**.
- Creare un blueprint macchina. Vedere [Scenario: creazione di un blueprint CentOS di vSphere per la clonazione in Rainpole](#).

Procedura

- 1 Selezionare **Progettazione > Blueprint**.
- 2 Puntare sul blueprint **Centos on vSphere** 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**.

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.

Scenario: 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 Londra, dovrà modificare il blueprint CentOS di vSphere 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 alla console di 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 [Scenario: creazione di un blueprint CentOS di vSphere per la clonazione in Rainpole](#).

Procedura

- 1 Selezionare **Progettazione > Blueprint**.
- 2 Puntare sul blueprint **Centos on vSphere** 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 Individuare il blueprint **CentOS su vSphere** e fare clic su **Pubblica**.

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.

Progettazione di blueprint di macchine con rete e sicurezza di NSX

Se si dispone di un'istanza di NSX integrata con vRealize Automation, è possibile configurare i blueprint di vSphere per sfruttare NSX per la virtualizzazione di rete e sicurezza.

Se è stata configurata l'integrazione di vRealize Automation con NSX, è possibile utilizzare i componenti rete, sicurezza e bilanciamento del carico nella tela di progettazione per configurare il blueprint per il provisioning delle macchine. È anche possibile aggiungere le seguenti impostazioni di rete e sicurezza di NSX al blueprint complessivo quando si crea un nuovo blueprint o si modifica un blueprint esistente.

- Zona di trasporto: contiene le reti utilizzate per la distribuzione delle macchine fornite in provisioning
- Criterio di prenotazione Edge e gateway instradato: gestisce le comunicazioni di rete per la distribuzione delle macchine con provisioning
- Isolamento app: consente solo il traffico interno tra le macchine utilizzate nella distribuzione delle macchine fornite in provisioning

Le impostazioni di NSX sono applicabili solo ai tipi di componente macchina vSphere.

Nuovo blueprint e impostazione delle proprietà del blueprint con NSX

È possibile specificare le impostazioni da applicare all'intero blueprint. Dopo aver creato il blueprint, è possibile modificare le impostazioni nella finestra di dialogo Proprietà blueprint.

Scheda **Generale**

Consente di applicare le impostazioni nell'intero blueprint, inclusi tutti i componenti che si intende aggiungere in un dato momento o successivamente.

Tavola 4-30. 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. Dato che gli identificatori 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 riassume il blueprint a vantaggio di altri architetti. Questa descrizione viene anche visualizzata per gli utenti nel modulo di richiesta.
Giorni di archiviazione	Invece di eliminare le distribuzioni immediatamente alla scadenza del lease, è possibile specificare un periodo di archiviazione temporanea. Specificare 0 (impostazione predefinita) per eliminare le distribuzioni 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.
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.

Scheda Impostazioni NSX

Se è stato configurato VMware NSX e installato il plug-in NSX per vRealize Automation, quando si crea o si modifica un blueprint è possibile specificare le impostazioni di NSX relative a zona di trasporto, criterio di prenotazione Edge e gateway instradato e isolamento app. Queste impostazioni sono disponibili nella scheda **Impostazioni NSX** nelle pagine **Nuovo blueprint** e **Proprietà blueprint**.

Per informazioni sulla configurazione di NSX, consultare la *guida di amministrazione di NSX*.

Tavola 4-31. 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.</p> <p>Una zona di trasporto è obbligatoria solo per i blueprint che presentano una rete su richiesta. Per gruppi di sicurezza, tag di sicurezza e bilanciamenti del carico, la zona di trasporto è facoltativa. Se non si specifica una zona di trasporto, l'endpoint viene determinato dalla posizione del gruppo di sicurezza, del tag di sicurezza o della rete a cui si connette il bilanciamento del carico.</p>
Criterio di prenotazione Edge e gateway instradato	<p>Selezionare un criterio di prenotazione Edge o gateway instradato NSX. Questo criterio di prenotazione si applica ai gateway instradati e a tutti gli edge distribuiti come parte del provisioning. Per ogni distribuzione viene eseguito il provisioning di un solo edge.</p> <p>Per le reti instradate, non viene eseguito il provisioning degli edge, ma è possibile utilizzare un criterio di prenotazione per selezionare una prenotazione con i gateway instradati da utilizzare per il provisioning della rete instradata.</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 gateway instradato è una macchina di gestione che consuma risorse di elaborazione, come le altre macchine virtuali, ma gestisce le comunicazioni di rete di tutte le macchine presenti 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>
Isolamento app	<p>Selezionare la casella di controllo Isolamento app per utilizzare il criterio di protezione isolamento app configurato in NSX. Il criterio di isolamento app viene applicato a tutti i componenti macchina vSphere nel blueprint.</p> <p>Facoltativamente è possibile aggiungere gruppi e tag di sicurezza NSX per consentire a vRealize Orchestrator di aprire la configurazione di rete isolata al fine di consentire percorsi di ingresso e uscita aggiuntivi dell'isolamento app.</p>

Scheda Proprietà

Le proprietà personalizzate aggiunte al livello del blueprint si applicano all'intero blueprint, inclusi tutti i componenti. Tuttavia queste possono essere sovrascritte da proprietà personalizzate assegnate in una posizione successiva della catena di precedenza. Per ulteriori informazioni sull'ordine di precedenza delle proprietà personalizzate, vedere *Guida di riferimento alle proprietà personalizzate*.

Tavola 4-32. Impostazioni della scheda Proprietà

Scheda	Impostazione	Descrizione
Gruppi di proprietà		I gruppi di proprietà sono gruppi riutilizzabili pensati per semplificare l'aggiunta di proprietà personalizzate ai blueprint. Gli amministratori tenant e di struttura possono raggruppare le proprietà che vengono spesso usate insieme in modo da consentire di aggiungere a un blueprint un gruppo di proprietà anziché le singole proprietà personalizzate.
	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 possibile anche trascinare 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. È possibile visualizzare queste proprietà unite per facilitare l'assegnazione delle priorità ai gruppi di proprietà.
Proprietà personalizzate		È possibile aggiungere singole proprietà personalizzate invece di gruppi di proprietà.
	Nome	Per un elenco dei nomi e dei comportamenti delle proprietà personalizzate, vedere <i>Guida di riferimento alle proprietà personalizzate</i> .
	Valore	Immettere il valore 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.

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.

Se il blueprint contiene una rete su richiesta, è necessario specificare la zona di trasporto di NSX che contiene le reti usate dalla distribuzione delle macchine con provisioning. Nella prenotazione deve essere specificata la stessa zona di trasporto.

Applicazione di un criterio di prenotazione di gateway instradato o Edge di NSX a un blueprint

È possibile specificare un criterio di prenotazione per gestire le comunicazioni di rete per le macchine di cui viene eseguito il provisioning dal 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. Il criterio di prenotazione di gateway instradato è anche definito "criterio di prenotazione Edge".

In ogni prenotazione sono contenute informazioni di networking. Quando viene eseguito il provisioning delle macchine, viene allocato un gateway Edge o instradato come router di rete per gestire le comunicazioni di rete per le macchine oggetto del provisioning nella distribuzione. È possibile aggiungere o modificare proprietà a livello di blueprint utilizzando la pagina delle proprietà del blueprint.

Un criterio di prenotazione del gateway instradato è facoltativo. Controlla quale prenotazione o prenotazioni è possibile utilizzare per il provisioning dell'Edge di NSX associato ai componenti di servizi di rete su richiesta e bilanciamento del carico su richiesta specificati nel blueprint.

Si utilizzano criteri di prenotazione per controllare la selezione delle prenotazioni. Si seleziona un criterio di prenotazioni nella definizione delle macchine virtuali nel blueprint e quindi si assegna tale criterio alle prenotazioni utilizzate dalle macchina virtuale.

Non è possibile condividere prenotazioni tra più gruppi aziendali.

vRealize Automation esegue il provisioning di un gateway instradato, ad esempio un gateway di servizi Edge (ESG), per reti NAT e per bilanciamenti del carico. Per le reti instradate, vRealize Automation utilizza i router distribuiti esistenti.

Un profilo di rete NAT e un bilanciamento del carico consentono a vRealize Automation di distribuire un gateway di servizi Edge di NSX. Un profilo di rete instradato utilizza un router distribuito logico (DLR, Logical Distributed Router) di NSX. 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 DLR per eseguire il provisioning delle macchine virtuali.

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, nonché gli indirizzi IP virtuali del bilanciamento del carico.

Quando si utilizza il blueprint per eseguire il provisioning di una distribuzione di macchine, vRealize Automation tenta di utilizzare solo le prenotazioni associate al criterio di prenotazione specificato per eseguire il provisioning dell'Edge o del gateway instradato.

Applicazione di un criterio di protezione di isolamento app di NSX a un 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.

È possibile applicare l'isolamento app al livello di blueprint utilizzando la finestra di dialogo **Nuovo blueprint** o **Proprietà blueprint**.

Quando si utilizza un criterio di isolamento app di NSX, 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. Viene creato un criterio di protezione di isolamento app in NSX e poi 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. Per informazioni correlate, vedere [Creazione di un endpoint vSphere con integrazione di rete e sicurezza](#).

Nota: quando si esegue il provisioning con un blueprint che utilizza sia un bilanciamento del carico NSX Edge che un criterio di protezione di isolamento app di NSX, 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, 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. 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 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.

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.

Per informazioni sulle funzionalità di sicurezza che possono essere applicate a un componente macchina in un blueprint, vedere [Utilizzo dei componenti sicurezza nella tela del blueprint](#).

Configurazione delle impostazioni dei componenti rete e sicurezza

vRealize Automation supporta le reti virtualizzate basate sulle piattaforme vCloud Networking and Security e NSX.

La virtualizzazione di rete e sicurezza consente alle macchine virtuali di comunicare tra loro su reti fisiche e virtuali in maniera sicura ed efficiente.

Per integrare rete e sicurezza con vRealize Automation, è necessario che un amministratore di IaaS installi i plug-in NSX in vRealize Orchestrator e crei gli endpoint vRealize Orchestrator e vSphere.

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 nelle tele dei blueprint. I profili di rete esterna definiscono le reti fisiche esistenti. I profili NAT e instradati sono modelli che creano switch logici NSX e impostazioni di routing appropriate per un nuovo percorso di rete e configurano interfacce di rete per la connessione al percorso di rete quando si esegue il provisioning di macchine virtuali e si configurano dispositivi NSX Edge.

Le impostazioni dei componenti rete e sicurezza aggiunte alla tela di progettazione del blueprint derivano dalla configurazione di NSX e richiedono l'installazione preventiva del plug-in NSX e l'esecuzione di una raccolta dei dati per l'inventario di NSX per i cluster vSphere. I componenti rete e sicurezza sono specifici di NSX e sono disponibili solo per l'uso con componenti macchina vSphere. Per informazioni sulla configurazione di NSX, consultare la *guida di amministrazione di NSX*.

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 del blueprint. Le proprietà del bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Se viene specificato un profilo di rete in una prenotazione e un blueprint, il valore del blueprint ha la precedenza. Ad esempio, se viene specificato un profilo di rete nel blueprint mediante la proprietà personalizzata `VirtualMachine.NetworkN.ProfileName` e in una prenotazione utilizzata dal blueprint, il profilo di rete specificato nel blueprint ha la precedenza. Se, tuttavia, la proprietà personalizzata non viene utilizzata nel blueprint e si seleziona un profilo di rete per una NIC della macchina, vRealize Automation utilizza il percorso di rete della prenotazione per la NIC della macchina per la quale è stato specificato il profilo di rete.

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. Vedere la *guida di amministrazione di NSX*.

Utilizzo dei componenti sicurezza nella tela del blueprint

È possibile aggiungere componenti sicurezza di NSX alla tela 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 rete e sicurezza aggiunte alla tela di progettazione del blueprint derivano dalla configurazione di NSX e richiedono l'installazione preventiva del plug-in NSX e l'esecuzione di una raccolta dei dati per l'inventario di NSX per i cluster vSphere. I componenti rete e sicurezza sono specifici di NSX e sono disponibili solo per l'uso con componenti macchina vSphere. Per informazioni sulla configurazione di NSX, consultare la *guida di amministrazione di NSX*.

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.

Gruppo di sicurezza

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 a un blueprint, in aggiunta ai gruppi di sicurezza specificati nella prenotazione.

I gruppi di sicurezza sono gestiti nella risorsa di origine. Per informazioni sulla gestione dei gruppi di sicurezza per le varie tipologie di risorse, vedere la documentazione del vendor.

È possibile aggiungere un gruppo di sicurezza NSX esistente o su richiesta alla tela del blueprint.

Tag di sicurezza

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.

È possibile aggiungere un tag di sicurezza alla tela del blueprint.

Criterio di protezione

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 per una risorsa di elaborazione.

Isolamento app

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.

Aggiunta di un componente gruppo di sicurezza esistente

È possibile aggiungere un componente gruppo di sicurezza esistente alla tela di progettazione in preparazione per associare le sue impostazioni a uno o più componenti macchina o ad altri tipi di componenti disponibili 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.

È possibile aggiungere più componenti rete e sicurezza alla tela di progettazione del blueprint.

Prerequisiti

- Creare e configurare un gruppo di sicurezza in NSX. Vedere *Configurazione di vRealize Automation e la guida di amministrazione di NSX*.
- Verificare che il plug-in NSX per vRealize Automation sia installato e che l'inventario di NSX sia stato correttamente eseguito per il proprio cluster.

Per utilizzare configurazioni di NSX in vRealize Automation, è necessario installare il plug-in di NSX ed eseguire la raccolta dati.

- Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Fare clic su **Rete e sicurezza** nella sezione Categorie per visualizzare l'elenco dei componenti rete e sicurezza disponibili.
- 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 Fare clic su **Fine** per salvare il blueprint come bozza o continuare la configurazione del blueprint.

Per configurare ulteriormente le impostazioni di sicurezza, è possibile aggiungere componenti sicurezza aggiuntivi e selezionare le impostazioni nella scheda **Sicurezza** di un componente macchina vSphere nella tela del blueprint.

Aggiunta di un componente gruppo di sicurezza su richiesta

È possibile aggiungere un componente gruppo di sicurezza 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.

Prerequisiti

- Creare e configurare un criterio di sicurezza in NSX. Vedere la *guida di amministrazione di NSX*.

- Verificare che il plug-in NSX per vRealize Automation sia installato e che l'inventario di NSX sia stato correttamente eseguito per il proprio cluster.

Per utilizzare configurazioni di NSX in vRealize Automation, è necessario installare il plug-in di NSX ed eseguire la raccolta dati.

- Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Fare clic su **Rete e sicurezza** nella sezione Categorie per visualizzare l'elenco dei componenti rete e sicurezza disponibili.
- 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 tra i criteri di protezione disponibili.
- 5 Fare clic su **OK**.
- 6 Fare clic su **Fine** per salvare il blueprint come bozza o continuare la configurazione del blueprint.

Per configurare ulteriormente le impostazioni di sicurezza, è possibile aggiungere componenti sicurezza aggiuntivi e selezionare le impostazioni nella scheda **Sicurezza** di un componente macchina vSphere nella tela del blueprint.

Aggiunta di un componente tag di sicurezza esistente

È possibile aggiungere un componente tag di sicurezza alla tela di progettazione del blueprint in preparazione per associare le sue impostazioni a uno o più componenti macchina nel blueprint.

È possibile utilizzare un componente tag di sicurezza per aggiungere un tag di sicurezza di NSX 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.

È possibile aggiungere più componenti rete e sicurezza alla tela di progettazione del blueprint.

Prerequisiti

- Creare e configurare tag di sicurezza in NSX. Vedere *Configurazione di vRealize Automation e la guida di amministrazione di NSX*.
- Verificare che il plug-in NSX per vRealize Automation sia installato e che l'inventario di NSX sia stato correttamente eseguito per il proprio cluster.

Per utilizzare configurazioni di NSX in vRealize Automation, è necessario installare il plug-in di NSX ed eseguire la raccolta dati.

- Verificare che il plug-in NSX per vRealize Automation sia installato e che l'inventario di NSX sia stato correttamente eseguito per il proprio cluster.

Per utilizzare configurazioni di NSX in vRealize Automation, è necessario installare il plug-in di NSX ed eseguire la raccolta dati.

- Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Fare clic su **Rete e sicurezza** nella sezione Categorie per visualizzare l'elenco dei componenti rete e sicurezza disponibili.
- 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 Fare clic su **Fine** per salvare il blueprint come bozza o continuare la configurazione del blueprint.

Per configurare ulteriormente le impostazioni di sicurezza, è possibile aggiungere componenti sicurezza aggiuntivi e selezionare le impostazioni nella scheda **Sicurezza** di un componente macchina vSphere nella tela del blueprint.

Utilizzo di componenti di rete nella tela del blueprint

È possibile aggiungere uno o più componenti rete NSX alla tela di progettazione e configurare le loro impostazioni per i componenti macchina vSphere nel blueprint.

È possibile aggiungere componenti rete alla tela per rendere le sue impostazioni configurate disponibili per uno o più componenti macchina nel blueprint.

Le impostazioni dei componenti rete e sicurezza aggiunte alla tela di progettazione del blueprint derivano dalla configurazione di NSX e richiedono l'installazione preventiva del plug-in NSX e l'esecuzione di una raccolta dei dati per l'inventario di NSX per i cluster vSphere. I componenti rete e sicurezza sono specifici di NSX e sono disponibili solo per l'uso con componenti macchina vSphere. Per informazioni sulla configurazione di NSX, consultare la *guida di amministrazione di NSX*.

Aggiunta di un componente rete esistente

È possibile aggiungere un componente rete di NSX 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 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 rete e sicurezza alla tela di progettazione del blueprint.

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 del blueprint. Le proprietà del bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Prerequisiti

- Creare e configurare le impostazioni di rete per NSX. Vedere *Configurazione di vRealize Automation* e la *guida di amministrazione di NSX*.
- Verificare che il plug-in NSX per vRealize Automation sia installato e che l'inventario di NSX sia stato correttamente eseguito per il proprio cluster.

Per utilizzare configurazioni di NSX in vRealize Automation, è necessario installare il plug-in di NSX ed eseguire la raccolta dati.

- Creare un profilo di rete.
- Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Fare clic su **Rete e sicurezza** nella sezione Categorie per visualizzare l'elenco dei componenti rete e sicurezza disponibili.
- 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 o confermare 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 Fare clic su **Fine** per salvare il blueprint come bozza o continuare la configurazione del blueprint.

Passi successivi

Per configurare ulteriormente le impostazioni di rete, è possibile aggiungere componenti rete aggiuntivi e selezionare le impostazioni nella scheda **Rete** di un componente macchina vSphere nella tela del blueprint.

Aggiunta di un componente rete instradata o NAT su richiesta

È possibile aggiungere un componente di rete NAT su richiesta NSX o un componente di rete instradata su richiesta NSX 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 rete e sicurezza alla tela di progettazione del blueprint.

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 del blueprint. Le proprietà del bilanciamento del carico di NSX sono applicabili solo alle macchine vSphere.

Prerequisiti

- Creare e configurare le impostazioni di rete per NSX. Vedere *Configurazione di vRealize Automation* e la *guida di amministrazione di NSX*.
- Verificare che il plug-in NSX per vRealize Automation sia installato e che l'inventario di NSX sia stato correttamente eseguito per il proprio cluster.

Per utilizzare configurazioni di NSX in vRealize Automation, è necessario installare il plug-in di NSX ed eseguire la raccolta dati.

- Creare un profilo di rete.

Ad esempio, se si sta aggiungendo un componente della rete NAT su richiesta, creare un profilo di rete per NAT.

- Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.

Procedura

- 1 Fare clic su **Rete e sicurezza** nella sezione Categorie per visualizzare l'elenco dei componenti rete e sicurezza disponibili.
- 2 Trascinare uno dei componenti rete su richiesta nella tela di progettazione, a seconda che si desideri configurare un componente NAT o instradato su richiesta.
- 3 Immettere un nome e, facoltativamente, una descrizione.

- 4 Selezionare un profilo di rete appropriato dal menu a discesa **Profilo di rete**.

Ad esempio, se si sta aggiungendo un componente della **rete NAT su richiesta**, selezionare un profilo di rete NAT.

Selezionando il profilo di rete vengono popolate automaticamente le seguenti impostazioni di rete. Eventuali modifiche a questi valori devono essere apportate nel profilo di rete:

- Nome del profilo di rete esterna
- Tipo di NAT (rete NAT su richiesta)
- Subnet mask
- Subnet mask dell'intervallo (rete instradata su richiesta)
- Subnet mask dell'intervallo (rete instradata su richiesta)
- Indirizzo IP di base (rete instradata su richiesta)

- 5 (Facoltativo) Fare clic sulla scheda **DNS/WINS**.

- 6 (Facoltativo) Specificare o confermare 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.

- 7 (Facoltativo) Nel caso di un componente di rete NAT su richiesta, fare clic sulla scheda **DHCP** per specificare i valori per l'intervallo di indirizzi IP e la durata del lease.

È possibile specificare i valori degli indirizzi IP iniziale e finale dell'intervallo DHCP. Quando viene eseguito il provisioning della macchina virtuale con DHCP, la scheda di rete assegna alla macchina un indirizzo IP appartenente all'intervallo. Per impostazione predefinita, si tratta di una scheda di rete statica. Gli indirizzi IP non possono coincidere con gli indirizzi della rete o di broadcast utilizzati nella subnet associata. Non è possibile sovrapporre intervalli IP statici.

DHCP è disponibile solo per i componenti di rete NAT One-to-Many su richiesta.

- 8 (Facoltativo) Immettere l'indirizzo IP iniziale nella casella di testo **Inizio intervallo IP**.

- 9 (Facoltativo) Immettere l'indirizzo IP finale nella casella di testo **Fine intervallo IP**.

- 10 Specificare la durata del lease di DHCP, espressa in secondi, nella casella di testo **Durata lease (secondi)** o lasciare vuoto il campo per specificare una durata di lease infinita.

- 11 (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.

12 Fare clic su **Fine** per salvare il blueprint come bozza o continuare la configurazione del blueprint.

Passi successivi

Per configurare ulteriormente le impostazioni di rete, è possibile aggiungere componenti rete aggiuntivi e selezionare le impostazioni nella scheda **Rete** di un componente macchina vSphere nella tela del blueprint.

Utilizzo di componenti bilanciamento del carico nella tela del blueprint

È possibile aggiungere uno o più componenti bilanciamento del carico di NSX su richiesta alla tela di progettazione per configurare le impostazioni dei componenti macchina vSphere nel blueprint.

Le impostazioni dei componenti rete e sicurezza aggiunte alla tela di progettazione del blueprint derivano dalla configurazione di NSX e richiedono l'installazione preventiva del plug-in NSX e l'esecuzione di una raccolta dei dati per l'inventario di NSX per i cluster vSphere. I componenti rete e sicurezza sono specifici di NSX e sono disponibili solo per l'uso con componenti macchina vSphere. Per informazioni sulla configurazione di NSX, consultare la *guida di amministrazione di NSX*.

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 lo stesso profilo di rete NAT nello stesso 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.

Viene anche creata una risorsa NSX Edge e vengono registrati come proprietà della risorsa Edge i dettagli del bilanciamento del carico quali VIP, livello con carico bilanciato e servizi configurati.

Aggiunta di un componente bilanciamento del carico su richiesta

È possibile utilizzare un componente bilanciamento del carico su richiesta per aggiungere un bilanciamento del carico 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.

Le impostazioni del bilanciamento del carico configurano la distribuzione dell'elaborazione delle attività tra le macchine fornite in provisioning di una rete.

Per le informazioni correlate in merito alla creazione dei profili dell'applicazione NSX per definire il comportamento di un tipo particolare di traffico di rete, vedere la *guida di amministrazione di NSX*.

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 il plug-in NSX per vRealize Automation sia installato e che l'inventario di NSX sia stato correttamente eseguito per il proprio cluster.

Per utilizzare configurazioni di NSX in vRealize Automation, è necessario installare il plug-in di NSX ed eseguire la raccolta dati.

- Creare un profilo di rete.
- Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.
- Aprire un blueprint nuovo o già esistente nella tela di progettazione utilizzando la scheda **Progettazione**.
- Accertarsi che nella tela di progettazione del blueprint sia presente almeno un componente macchina vSphere.

Procedura

- 1 Fare clic su **Rete e sicurezza** nella sezione Categorie per visualizzare l'elenco dei componenti rete e sicurezza disponibili.
- 2 Trascinare un componente **Bilanciamento del carico su richiesta** nella tela di progettazione.
- 3 Immettere un nome nella casella di testo **Nome**.
- 4 Selezionare il nome di una macchina dal menu a discesa **Macchina**.
L'elenco contiene solo componenti macchina vSphere nel blueprint attivo.
- 5 Selezionare una scheda di rete dal menu a discesa **NIC**.
L'elenco mostra le NIC definite nel componente macchina vSphere selezionato.
- 6 Selezionare una rete VIP dal menu a discesa **Rete VIP**.
- 7 (Facoltativo) Specificare l'indirizzo VIP della NIC mostrato in **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, per la VIP viene allocato il successivo indirizzo IP disponibile dal profilo di rete. Quando si crea una VIP su una rete NAT è possibile specificare un solo indirizzo IP.
- 8 Selezionare la casella di controllo relativa a ogni servizio da includere nel bilanciamento del carico.
Le opzioni dei servizi sono HTTP, HTTPS e TCP.
- 9 (Facoltativo) Accettare o modificare la porta e le impostazioni relative al controllo di stato per ciascun servizio selezionato.
- 10 Specificare l'indirizzo per il servizio selezionato nella casella di testo **URL per servizio HTTP**.
È disponibile un solo URL per il controllo del servizio HTTP per ogni bilanciamento del carico.
L'URL immesso viene usato per i controlli di stato del servizio.

Inserire l'URL dell'indirizzo per il quale reindirizzare il traffico HTTP. Ad esempio, è possibile reindirizzare il traffico da `http://myweb.com` a `https://myweb.com`. Il valore immesso deve corrispondere al valore specificato nell'impostazione **URL reindirizzamento HTTP** nell'applicazione NSX.

11 Fare clic su **Fine** per salvare il blueprint come bozza o continuare la configurazione del blueprint.

Le impostazioni configurate sono disponibili nella scheda **Rete** del componente macchina vSphere associato.

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 rete o sicurezza NSX in una tela e una volta definite le rispettive impostazioni disponibili, è possibile aprire le schede rete e sicurezza di un componente macchina vSphere nella tela e configurarne le impostazioni.

Le impostazioni dei componenti rete e sicurezza aggiunte alla tela di progettazione del blueprint derivano dalla configurazione di NSX e richiedono l'installazione preventiva del plug-in NSX e l'esecuzione di una raccolta dei dati per l'inventario di NSX per i cluster vSphere. I componenti rete e sicurezza sono specifici di NSX e sono disponibili solo per l'uso con componenti macchina vSphere. Per informazioni sulla configurazione di NSX, consultare la *guida di amministrazione di NSX*.

Ad esempio è possibile trascinare un componente rete NAT su richiesta nella tela di progettazione del blueprint per renderlo disponibile per un componente macchina vSphere già presente nella tela.

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.

Tavola 4-33. 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.

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 sull'API REST di vRealize Automation, vedere *Guida alla programmazione e Riferimento API di vRealize Automation*.
- 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.

Tavola 4-34. Esempi di script per l'opzione di proprietà Elaborate

Proprietà stringa campione	Sintassi script	Uso del campione
my_unique_id = ""	Bash - \$my_unique_id	export my_unique_id="0123456789"
	Windows CMD - %my_unique_id%	set my_unique_id=0123456789
	Windows PowerShell - \$my_unique_id	\$my_unique_id = "0123456789"

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 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, usare la scheda **Proprietà** nella tela del blueprint 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_N% 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 %
	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.

Tavola 4-35. 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.

Tavola 4-36. 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"

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 alla console di vRealize Automation come **architetto 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.

Tavola 4-37. 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**.

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.

Passi successivi

Aggiungere il componente Software pubblicato a un blueprint di applicazioni. Vedere [Assemblaggio di blueprint compositi](#).

Scenario: creazione di un componente Software MySQL per Rainpole

Utilizzando i privilegi di architetto software, creare un componente Software MySQL su macchine vSphere CentOS. Quando si progetta il componente software Software MySQL per una macchina virtuale CentOS, si configurano i parametri di installazione, configurazione e avvio e gli script per i sistemi operativi Linux.

Procedura

- 1 Selezionare **Progettazione > Componenti software**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere **MySQL for Linux Virtual Machines** nella casella di testo **Nome**.
- 4 Verificare che l'identificatore venga compilato in base al nome fornito.

Ad esempio, Software.MySQLforLinuxVirtualMachines

- 5 Immettere **MySQL installation and configuration** nella casella di testo **Descrizione**.
- 6 Selezionare **Macchina** dal menu a discesa **Contenitore**.

Poiché si intende consentire solo l'installazione di MySQL direttamente su una macchina, è necessario impedire agli architetti di rilasciare il componente Software MySQL su altri componenti Software.

7 Fare clic su **Avanti**.

8 Fare clic su **Nuovo**, quindi aggiungere e configurare ciascuna delle proprietà seguenti per lo script di installazione.

Fare clic su **OK** per salvare ciascuna proprietà.

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.

Nome	Descrizione	Tipo	Valore	Codificato	Consenti sovrascrittura	Obbligatorio	Valore elaborato
db_root_username	Nome utente root del database	Stringa	root	No	Sì	Sì	No
JAVA_HOME	Directory in cui è installato JRE 1.8 o versione successiva	Stringa	/opt/vmware-jre	No	Sì	Sì	No
global_ftp_proxy	Eventuale URL del proxy FTP. Non obbligatorio.	Stringa		No	Sì	No	No
db_port	Porta del database MySQL	Stringa		No	Sì	Sì	No
db_root_password	Password dell'utente root del database	Stringa	password	Sì	Sì	Sì	No
global_http_proxy	Eventuale URL del proxy HTTP. Non obbligatorio.	Stringa		No	Sì	No	No

Nome	Descrizione	Tipo	Valore	Codificato	Consenti sovrascrittura	Obbligatorio	Valore elaborato
global_https_proxy	Eventuale URL del proxy HTTPS. Non obbligatorio.	Stringa		No	Sì	No	No
max_allowed_packet_size	Dimensione massima del pacchetto consentita per il server	Integer	1024	No	Sì	No	No

9 Fare clic su **Avanti**.

10 Configurare l'azione di installazione.

- a Selezionare **Bash** dal menu a discesa **Tipo di script**.
- b Fare clic su **Fare clic qui per modificare**.

c Incollare il seguente script.

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
[ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail #"
    echo "#####"
```

```

    echo ""
fi

export PATH=$PATH:$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
set -e

# Tested on CentOS
if [ -x /usr/sbin/selinuxenabled ] && /usr/sbin/selinuxenabled; then
    # SELinux can be disabled by setting "/usr/sbin/setenforce Permissive"
    echo 'SELinux is enabled on this VM template. This service requires SELinux to be
disabled to install successfully'
    exit 1
fi

if [ "x$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
    # Fix the linux-firmware package
    export DEBIAN_FRONTEND=noninteractive
    apt-get install -y linux-firmware < /dev/console > /dev/console
    # Install MySQL package
    apt-get install -y mysql-server
else
    yum --nogpgcheck --noplugins -y install -x MySQL-server-community mysql-server
fi

# Set Install Path to the default install path (For monitoring)
Install_Path=/usr
echo Install_Path is set to $Install_Path, please modify this script if the install path is
not correct.

```

d Fare clic su **OK**.

11 Specificare l'azione di configurazione.

- a Selezionare **Bash** dal menu a discesa **Tipo di script**.
- b Fare clic su **Fare clic qui per modificare**.

c Incollare il seguente script.

```
#!/bin/bash

#Setting proxies
export ftp_proxy=${ftp_proxy:-$global_ftp_proxy}
echo "Setting ftp_proxy to $ftp_proxy"

export http_proxy=${http_proxy:-$global_http_proxy}
echo "Setting http_proxy to $http_proxy"

export https_proxy=${https_proxy:-$global_https_proxy}
echo "Setting https_proxy to $https_proxy"

#
# Determine operating system and version
#
export OS=
export OS_VERSION=

if [ -f /etc/redhat-release ]; then
    # For CentOS the result will be 'CentOS'
    # For RHEL the result will be 'Red'
    OS=$(cat /etc/redhat-release | awk '{print $1}')

    if [ -n $OS ] && [ $OS = 'CentOS' ]; then
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $3}')
    else
        # RHEL
        OS_VERSION=$(cat /etc/redhat-release | awk '{print $7}')
    fi

elif [ -f /etc/SuSE-release ]; then
    OS=SuSE

    MAJOR_VERSION=$(cat /etc/SuSE-release | grep VERSION | awk '{print $3}')
    PATCHLEVEL=$(cat /etc/SuSE-release | grep PATCHLEVEL | awk '{print $3}')

    OS_VERSION="$MAJOR_VERSION.$PATCHLEVEL"

elif [ -f /usr/bin/lsb_release ]; then
    # For Ubuntu the result is 'Ubuntu'
    OS=$(lsb_release -a 2> /dev/null | grep Distributor | awk '{print $3}')
    OS_VERSION=$(lsb_release -a 2> /dev/null | grep Release | awk '{print $2}')

fi

echo "Using operating system '$OS' and version '$OS_VERSION'"

if [ "x${global_http_proxy}" == "x" ] || [ "x${global_https_proxy}" == "x" ] ||
[ "x${global_ftp_proxy}" == "x" ]; then
    echo ""
    echo "#####"
    echo "# One or more PROXY(s) not set. Network downloads may fail #"
    echo "#####"
```

```

    echo ""
fi

export PATH=$PATH:$JAVA_HOME/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
set -e

# Locate the my.cnf file
my_cnf_file=
if [ -f /etc/my.cnf ]; then
    my_cnf_file=/etc/my.cnf
elif [ -f /etc/mysql/my.cnf ]; then
    my_cnf_file=/etc/mysql/my.cnf
fi

if [ "x$my_cnf_file" = "x" ]; then
    echo "Neither /etc/my.cnf nor /etc/mysql/my.cnf can be found, stopping configuration"
    exit 1
fi

# update mysql configuration to handle big packets
sed -ie "s/\[mysqld\]/\[mysqld\]\n\
max_allowed_packet=$max_allowed_packet/g" $my_cnf_file
# update listening port
sed -ie "s/\[mysqld\]/\[mysqld\]\n\
port=$db_port/g" $my_cnf_file

sed -i "s/port.*.*[0-9]*/port=$db_port/g" $my_cnf_file

if [ "x$OS" != "x" ] && [ "$OS" = 'Ubuntu' ]; then
    # Make sure that MySQL is started
    service mysql restart
else
    # set up auto-start on booting
    chkconfig mysqld on
    # restart mysqld service
    service mysqld start
fi

# this will assign a password for mysql admin user 'root'
mysqladmin -u $db_root_username password $db_root_password

```

d Fare clic su **OK**.

12 Configurare l'azione di avvio.

- a Selezionare **Bash** dal menu a discesa **Tipo di script**.
- b Fare clic su **Fare clic qui per modificare**.

- c Incollare il seguente script.

```
#!/bin/sh

echo "The maximum allowed packet size is: "
```

- d Posizionare il cursore tra i due punti e la virgoletta.
- e Selezionare **max_allowed_packet_size** dal menu a discesa **Selezionare una proprietà da inserire**.

Lo script contiene ora la proprietà.

```
#!/bin/sh

echo "The maximum allowed packet size is: $max_allowed_packet_size"
```

- f Fare clic su **OK**.

13 Fare clic su **Avanti**.

14 Fare clic su **Fine**.

15 Selezionare la riga contenente MySQL for Linux Virtual Machines e fare clic su **Pubblica**.

Il componente Software MySQL è disponibile per gli altri architetti nella pagina di progettazione del blueprint, ma non è possibile renderle disponibili componenti Software fino a quando non li si è combinati a una macchina.

Passi successivi

Utilizzando i privilegi di architetto software, architetto applicazione o architetto IaaS, combinare il componente MySQL con il blueprint della macchina CentOS for Software.

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.

Tavola 4-38. 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 riassume 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.

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.

Tavola 4-39. 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.

Tavola 4-39. Nuove proprietà di Software (Continua)

Impostazione	Descrizione
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.
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.

Tavola 4-40. 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

Creazione 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 di cui viene eseguito il provisioning.

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 nei gruppi o script 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.

Utilizzo di blueprint XaaS nelle tele di progettazione di blueprint

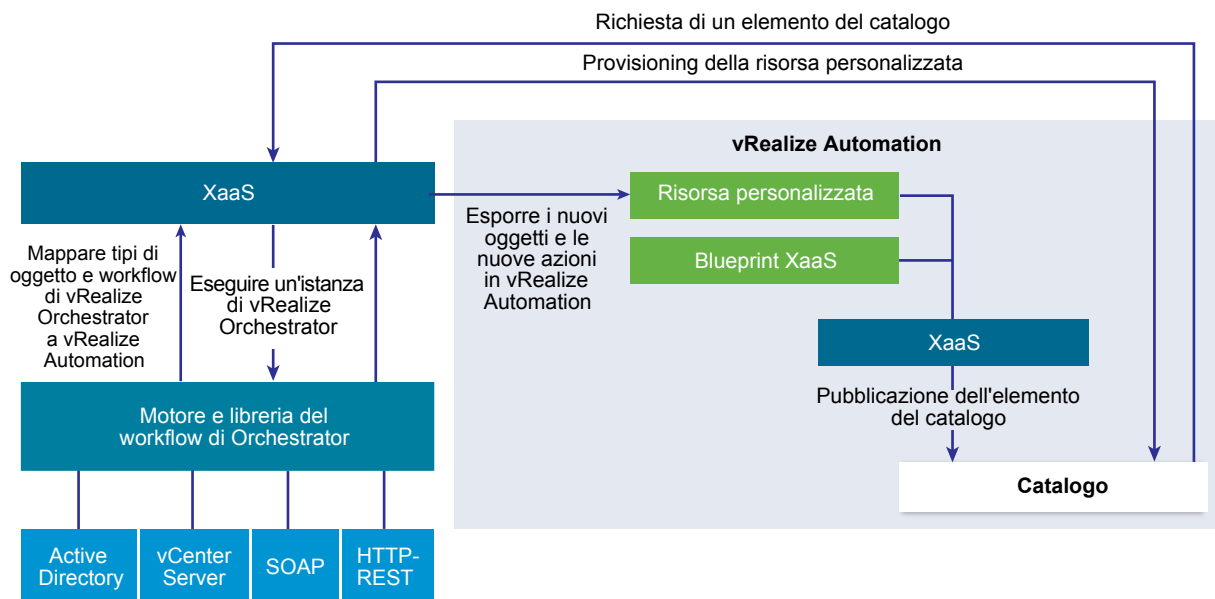
Se si utilizza un blueprint XaaS nelle tele di progettazione come componente blueprint della macchina, il blueprint XaaS viene escluso dalle azioni di scalabilità verticale e orizzontale che vengono eseguite nella propria distribuzione. Le modifiche apportate al componente XaaS in una distribuzione non sono riconosciute dalle azioni di scalabilità. Se si desidera allineare il componente XaaS con le modifiche alla scalabilità apportate alla distribuzione, è necessario eseguire tali azioni separatamente nel componente XaaS utilizzando le azioni risorsa XaaS.

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.

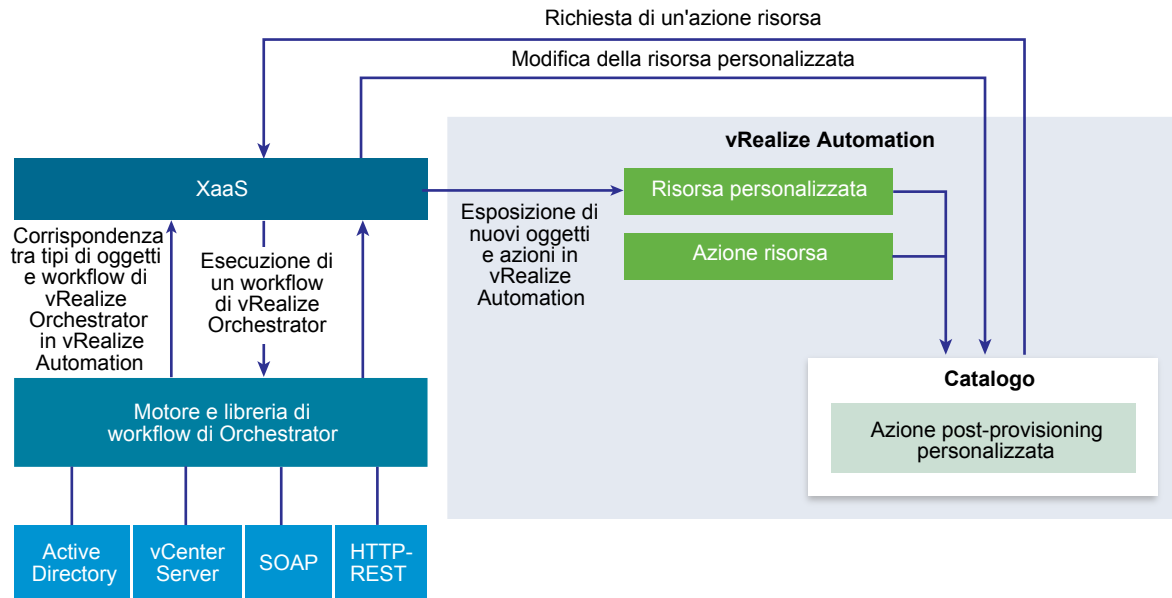
Figura 4-1. Creazione e richiesta di elementi di catalogo inclusi in un XaaS per il provisioning di una risorsa personalizzata



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 4-2. 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:

Tavola 4-41. 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.

Tavola 4-41. Parametri globali di XaaS (Continua)

Parametro	Descrizione
__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 VMware 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.

Tavola 4-42. 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.
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.

Tavola 4-42. Plug-in inclusi per impostazione predefinita in vRealize Orchestrator (Continua)

Plug-in	Scopo
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 (solo nell'istanza incorporata in 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 risorse personalizzate

Quando si crea una risorsa personalizzata, un tipo di oggetto vRealize Orchestrator viene mappato come risorsa di XaaS in modo da consentire la creazione di blueprint e azioni risorsa.

Ad esempio, se si crea una risorsa personalizzata basata su VC:VirtualMachine, è possibile creare blueprint per eseguire il provisioning di macchine virtuali vCenter Server e aggiungere azioni risorsa da eseguire sulle macchine.

Aggiunta di una risorsa personalizzata

La creazione di una risorsa personalizzata consente di definire l'elemento XaaS da fornire in provisioning.

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 creazione di una risorsa personalizzata consente di definire il parametro di output di un blueprint di XaaS per il provisioning e un parametro di input per un'azione risorsa.

Durante il processo di creazione di una risorsa personalizzata, nella pagina Modulo dettagli si possono specificare i campi del modulo di sola lettura per la risorsa, utilizzato per presentare le informazioni nella visualizzazione Dettagli di un elemento di cui è stato eseguito il provisioning. Vedere [Progettazione di un modulo risorsa personalizzata](#).

Prerequisiti

Accedere alla console di vRealize Automation come **architetto XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Risorse personalizzate**.
- 2 Fare clic sull'icona **Nuovo** (+).

- 3 Specificare il tipo di oggetto vRealize Orchestrator nella casella di testo **Tipo di orchestrator** e premere Invio.

Ad esempio, immettere **v** per vedere tutti i tipi che contengono la lettera v. Per visualizzare tutti i tipi, immettere uno spazio e fare clic su **Cerca**.

- 4 Immettere un nome e, facoltativamente, una descrizione.






- 5 Specificare la versione.

Per la versione sono supportati solo numeri interi. Il formato supportato ha l'estensione major.minor.micro-revisione.

- 6 Fare clic su **Avanti**.

- 7 Modificare il modulo della risorsa personalizzata.

È possibile modificare il modulo della risorsa personalizzata 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	Descrizione
Aggiungi un modulo	Fare clic sull'icona Nuovo modulo () accanto al nome del modulo, fornire le informazioni richieste e fare clic su Invia .
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 .
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 . Gli elementi disponibili sono specifici per il tipo di oggetto di vRealize Orchestrator.
Modificare un elemento	Fare clic sull'icona Modifica () accanto all'elemento da modificare, apportare le modifiche necessarie e fare clic su Invia .
Eliminare un elemento	Fare clic sull'icona Elimina () accanto all'elemento da eliminare, quindi scegliere OK nella finestra di dialogo di conferma.
Elimina un modulo	Fare clic sull'icona Elimina () accanto al nome del modulo, quindi scegliere OK nella finestra di dialogo di conferma.

- 8 Fare clic su **Fine**.

È stata creata una risorsa personalizzata che verrà elencata nella pagina Risorse personalizzate.

Passi successivi

Creare un blueprint di XaaS. Vedere [Creazione di un blueprint XaaS](#).

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. Quindi è possibile utilizzare un'azione risorsa per modificare il requisito di cambiamento password da parte dell'utente.

Creazione di un blueprint XaaS come elemento di catalogo

Un blueprint XaaS è un blueprint per il provisioning. Alcuni dei workflow di provisioning forniti includono la creazione di macchine virtuali, l'aggiunta di utenti ad Active Directory o la creazione di snapshot di macchine virtuali.

Prerequisiti

- Accedere alla console di vRealize Automation come **architetto XaaS**.
- Creazione di una risorsa personalizzata per il tipo di risorsa target. Vedere [Aggiunta di una risorsa personalizzata](#).

Procedura

1 Creazione di un blueprint XaaS

Un blueprint XaaS è una specifica completa per il provisioning. Il blueprint può contenere parametri di input, moduli di invio e di sola lettura, sequenze di azioni e provisioning.

2 Pubblicazione di un blueprint XaaS come elemento di catalogo

Dopo averlo creato, un blueprint XaaS è nello stato bozza ed è possibile pubblicarlo come elemento di catalogo.

3 Aggiunta di un blueprint XaaS a un blueprint di applicazione

Per aggiungere un blueprint XaaS a un blueprint di applicazione, procedere in modo analogo all'aggiunta di altri blueprint nelle tele di progettazione.

Creazione di un blueprint XaaS

Un blueprint XaaS è una specifica completa per il provisioning. Il blueprint può contenere parametri di input, moduli di invio e di sola lettura, sequenze di azioni e provisioning.

È possibile creare blueprint di servizi per eseguire il provisioning di risorse personalizzate create in precedenza. Quando i clienti richiedono tali elementi del catalogo, gli elementi di cui viene eseguito il provisioning sono disponibili nella scheda **Elementi** ed è possibile definire operazioni da eseguire dopo il provisioning per tale tipo di risorse di cui è stato eseguito il provisioning.

Se si crea un blueprint del servizio per il provisioning senza specificare il parametro di output, quando i clienti richiedono questo elemento del catalogo, il blueprint esegue il provisioning ma gli elementi di cui viene eseguito il provisioning non vengono aggiunti alla scheda **Elementi**. Non è possibile eseguire operazioni post-provisioning su questo tipo di risorse di cui viene eseguito il provisioning.

Inoltre, è possibile creare blueprint di servizi per richieste che non dispongono di parametri di output e non danno luogo ad alcun provisioning. Ad esempio, è possibile creare il blueprint di un servizio per l'invio di notifiche.

Creando il blueprint di un servizio, si pubblica un workflow vRealize Orchestrator come elemento di catalogo. Durante questa procedura è possibile modificare i moduli predefiniti generati. Vedere [Progettazione di un modulo blueprint di XaaS](#).

Prerequisiti

- Accedere alla console di vRealize Automation come **architetto XaaS**.
- Per il provisioning degli elementi, creare una risorsa personalizzata corrispondente al parametro di output del blueprint del servizio. Vedere [Aggiunta di una risorsa personalizzata](#).

Procedura

1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.

2 Fare clic sull'icona **Nuovo** (+).

3 Sfogliare la libreria di workflow di vRealize Orchestrator e selezionare un workflow.

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 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.

6 (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**.

7 Specificare la versione.

Per la versione sono supportati solo numeri interi. Il formato supportato ha l'estensione major.minor.micro-revisione.

8 Fare clic su **Avanti**.

9 (Facoltativo) Modificare il modulo del blueprint del servizio dalla pagina Modulo blueprint.

Per impostazione predefinita, il modulo del blueprint del servizio è mappato alla presentazione del workflow vRealize Orchestrator. È possibile modificare il modulo del blueprint 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 .

Opzione	Azione
Rigenera la presentazione del workflow	Fare clic sull'icona Rigenera (🔄) accanto al nome del modulo e scegliere OK .
Elimina un modulo	Fare clic sull'icona Elimina (✖) 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 (✎) 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 (✖) 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 (✎) accanto all'elemento da modificare, apportare le modifiche necessarie e fare clic su Invia .
Eliminare un elemento	Fare clic sull'icona Elimina (✖) accanto all'elemento da eliminare, quindi scegliere OK nella finestra di dialogo di conferma.

10 Fare clic su **Avanti**.

11 Selezionare un parametro di output dal menu a discesa.

Opzione	Descrizione
Risorsa personalizzata creata in precedenza	Quando gli utenti richiedono questo elemento del catalogo, gli elementi di cui è stato eseguito il provisioning vengono aggiunti alla scheda Elementi .
Nessun provisioning	Il blueprint del servizio non aggiunge i nuovi elementi alla scheda Elementi .

12 Fare clic su **Fine**.

È stato creato un blueprint di servizio, visibile nella pagina dei blueprint XaaS.

Passi successivi

Pubblicare il blueprint come elemento di catalogo. Vedere [Pubblicazione di un blueprint XaaS come elemento di catalogo](#).

Pubblicazione di un blueprint XaaS come elemento di catalogo

Dopo averlo creato, un blueprint XaaS è nello stato bozza ed è possibile pubblicarlo come elemento di catalogo.

Prerequisiti

Accedere alla console di vRealize Automation come **architetto XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Selezionare la riga del blueprint XaaS da pubblicare e fare clic su **Pubblica**.

Lo stato del blueprint XaaS cambia in Pubblicato. Selezionando **Amministrazione > Gestione catalogo > Elementi del catalogo** è possibile verificare che il blueprint sia pubblicato come elemento di catalogo.

Passi successivi

- Per rendere il blueprint XaaS disponibile nel catalogo dei servizi, è necessario aggiungere l'elemento in un servizio. Vedere [Creazione di un servizio](#).
- Se si utilizza il blueprint XaaS in un blueprint di applicazione, aggiungerlo alla tela di progettazione. Vedere [Aggiunta di un blueprint XaaS a un blueprint di applicazione](#).
- È possibile creare un'azione risorsa che verrà eseguita in fase di provisioning degli elementi. Vedere [Creazione di un'azione risorsa](#).

Aggiunta di un blueprint XaaS a un blueprint di applicazione

Per aggiungere un blueprint XaaS a un blueprint di applicazione, procedere in modo analogo all'aggiunta di altri blueprint nelle tele di progettazione.

Utilizzare questo metodo per aggiungere un XaaS a un blueprint di applicazione che contiene altri blueprint. 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 di applicazione.

Se si esegue un'azione di scalabilità verticale o scalabilità orizzontale su un blueprint di applicazione distribuito, il blueprint XaaS non viene scalato.

Prerequisiti

- Creazione e pubblicazione di un blueprint XaaS. Vedere [Creazione di un blueprint XaaS come elemento di catalogo](#).
- Revisione della modalità di personalizzazione dei moduli di blueprint XaaS. Vedere [Progettazione di moduli per blueprint e azioni di XaaS](#).
- Accedere alla console di vRealize Automation come **architetto dell'infrastruttura**.

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 Nell'elenco Categorie fare clic su **XaaS**.
- 4 Trascinare il blueprint nella tela.
- 5 Configurare i valori predefiniti per le opzioni dell'infrastruttura e i parametri generali.
Questi valori predefiniti vengono visualizzati nel modulo del catalogo dei servizi quando un utente richiede l'elemento.
- 6 Fare clic su **Fine**.

Ora il blueprint XaaS fa parte del blueprint di applicazione.

Passi successivi

Verificare che il blueprint di applicazione venga aggiunto a un servizio e permesso agli utenti. Vedere [Gestione del catalogo dei servizi](#).

Creazione di un'azione risorsa XaaS come elemento di catalogo

È possibile creare un'azione risorsa in modo da poter gestire gli elementi con provisioning utilizzando i workflow di vRealize Orchestrator.

Prerequisiti

- Accedere alla console di vRealize Automation come **architetto XaaS**.
- Assicurarsi di disporre di una risorsa personalizzata che supporti l'azione. Vedere [Aggiunta di una risorsa 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

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 alla console di vRealize Automation come **architetto 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 Sfogliare la libreria di workflow di vRealize Orchestrator e selezionare un workflow.

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.

Per la versione sono supportati solo numeri interi. 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 Elementi . 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 Elementi 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.

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**.

È stata creata un'azione risorsa, che verrà elencata nelle pagina Azioni risorsa.

Passi successivi

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 alla console di vRealize Automation come **architetto XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.

- 2 Selezionare la riga dell'azione risorsa da pubblicare e fare clic su **Pubblica**.

Anche lo stato dell'azione risorsa cambia in Pubblicato.

Passi successivi

Assegnare un'icona all'azione risorsa. Vedere [Assegnazione di un'icona a un'azione risorsa](#). 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

Dopo aver creato e pubblicato un'azione risorsa, è possibile modificarla per assegnarle un'icona.

Prerequisiti

Accedere alla console di vRealize Automation come **architetto 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**.

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 alla console di vRealize Automation come **architetto 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.

Per la versione sono supportati solo numeri interi. 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.

Tavola 4-43. 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**.

Tavola 4-44. 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
Email	Campo in cui i clienti immettono un indirizzo di email
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

Tavola 4-44. Nuovi campi nel modulo dell'azione risorsa o di un blueprint di XaaS (Continua)

Campo	Descrizione
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 specificati nel workflow di vRealize Orchestrator.

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. Utilizzando le condizioni è possibile creare clausole ed espressioni varie e applicarle allo stato o ai vincoli dell'elemento.
Esterno	Selezionare un'azione di script di vRealize Orchestrator per definire il valore.

Tavola 4-45. Vincoli in designer modulo

Vincolo	Descrizione
Obbligatorio	Indica se l'elemento è obbligatorio.
Sola lettura	Indica se il campo è di sola lettura.

Tavola 4-45. Vincoli in designer modulo (Continua)

Vincolo	Descrizione
Valore	Consente di impostare un valore per l'elemento.
Visibile	Indica se l'elemento sarà visibile dal cliente.
Lunghezza minima	Consente di impostare un numero minimo di caratteri per l'elemento di input stringa.
Lunghezza massima	Consente di impostare il numero massimo consentito di caratteri per l'elemento di input stringa.
Valore minimo	Consente di impostare un valore minimo per l'elemento di input numero.
Valore massimo	Consente di impostare un valore massimo per l'elemento di input numero.
Incremento	Consente di impostare un incremento per elementi quali i campi 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	Consente di impostare un numero minimo di voci selezionabili per l'elemento. 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.
Conteggio massimo	Consente di impostare un numero massimo di voci selezionabili per l'elemento. 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.

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.

Tavola 4-46. 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.
Valore	Consente di definire valori personalizzati statici mediante etichette.
Valori esterni	Selezionare un'azione di script di vRealize Orchestrator per definire 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.

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 esplorando una struttura.

Create cluster - Modifica blueprint

Workflow Generale **Modulo blueprint** Risorsa di provisioning

Modulo: Modulo di richiesta

Nuovi campi

- ABC Campo testo
- ABC Area testo
- http:// Collegamento
- Email
- Campo URL immagine
- **** Campo password
- 123 Campo numero intero
- 0.0 Campo decimale
- Data e ora

Pagina modulo: Passaggio

vCloud Distributed Storage

Seleziona
Nessuna selezione di VC:HostFolder

Name of the new cluster

Enable VMware HA No

Enable VMware DRS No

< Indietro Avanti > Fine Annulla

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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- **Aggiunta di una risorsa 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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa 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**.

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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa 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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa 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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Aggiunta di una risorsa 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**.

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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione 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 Richiesta .

- 7 Fare clic su **Invia**.

Passi successivi

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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione 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	Selezionare valori da un elenco di oggetti correlati dall'inventario di vRealize Orchestrator. <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	Definire valori personalizzati con etichette. <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	Selezionare un'azione di script di vRealize Orchestrator per definire il valore con informazioni non direttamente esposte tramite il workflow. <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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione 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**.

Passi successivi

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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione 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 alla console di vRealize Automation come **amministratore tenant** o **architetto di XaaS**.
- [Creazione 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 risistemandolo 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 alla console di 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 Richiesta .

- 7 Fare clic su **Invia**.

Passi successivi

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 alla console di 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**.**Passi successivi**

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 alla console di 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 alla console di 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 alla console di 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 anche possibile associare una nuova operazione di post-provisioning all'utente con provisioning eseguito, che ad esempio consenta ai clienti di cambiare la password utente.

Un architetto di XaaS può creare una nuova risorsa personalizzata, un blueprint di XaaS e pubblicare un elemento di 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

Dopo aver creato la risorsa personalizzata, è possibile creare il blueprint di XaaS per pubblicare il workflow Crea utente in un gruppo come elemento di catalogo.

3 Pubblicazione del blueprint Crea utente di prova come elemento di catalogo

Dopo aver creato il blueprint di XaaS Crea utente di prova, è possibile pubblicarlo come elemento di catalogo.

4 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.

5 Pubblicazione dell'azione risorsa per il cambiamento della password

Per utilizzare l'azione risorsa Cambia password dell'utente di prova come operazione successiva al provisioning, è necessario pubblicarla.

6 Creazione di un servizio del catalogo per la creazione di un utente di prova

È possibile creare un servizio per visualizzare l'elemento di catalogo di creazione utente nel catalogo servizi e permettere ai clienti di individuare facilmente gli elementi di catalogo correlati alla creazione dell'utente di prova.

7 Associazione dell'elemento di catalogo al servizio Crea utente di prova

Per poter includere un elemento di catalogo Crea utente di prova nel servizio Crea utente di prova, è necessario associarlo al servizio.

8 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, in modo tale che essi possano visualizzare il servizio nel proprio catalogo e richiedere l'elemento di 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 alla console di vRealize Automation come **architetto 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 una descrizione per la 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 il modulo invariato.

- 9 Fare clic su **Fine**.

È stata creata la risorsa personalizzata Utente di prova che verrà elencata nella pagina Risorse personalizzate.

Passi successivi

Creare un blueprint di XaaS.

Creazione di un blueprint di XaaS per la creazione di un utente

Dopo aver creato la risorsa personalizzata, è possibile creare il blueprint di XaaS per pubblicare il workflow Crea utente in un gruppo come elemento di catalogo.

Prerequisiti

Accedere alla console di vRealize Automation come **architetto XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.
- 2 Fare clic su **Aggiungi** (+).
- 3 Passare a **Orchestrator > Libreria > Microsoft > Active Directory > Utente** nella libreria dei workflow di vRealize Orchestrator e selezionare il workflow **Crea utente in un gruppo**.
- 4 Fare clic su **Avanti**.
- 5 Cambiare il nome del blueprint in **Crea utente di prova** e lasciare invariata la descrizione.
- 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**.

Il nome del dominio viene impostato su un valore costante.

- d Fare clic sulla fare clic su **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 **Fine**.

È stato creato un blueprint per la creazione di un utente di prova che verrà elencato nelle pagina dei blueprint di XaaS.

Passi successivi

Pubblicare il blueprint Crea utente di prova per renderlo un elemento di catalogo attivo.

Pubblicazione del blueprint Crea utente di prova come elemento di catalogo

Dopo aver creato il blueprint di XaaS Crea utente di prova, è possibile pubblicarlo come elemento di catalogo.

Prerequisiti

Accedere alla console di vRealize Automation come **architetto XaaS**.

Procedura

1 Selezionare **Progettazione > XaaS > Blueprint XaaS**.

2 Selezionare la riga del blueprint Crea utente di prova e fare clic sul pulsante **Pubblica**.

Lo stato del blueprint Crea utente di prova cambia in Pubblicato. È possibile passare a **Amministrazione > Gestione catalogo > Elementi del catalogo** e verificare che il blueprint Crea utente di prova sia pubblicato come elemento di catalogo.

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 alla console di vRealize Automation come **architetto XaaS**.

Procedura

1 Selezionare **Progettazione > XaaS > Azioni risorsa**.

2 Fare clic su **Aggiungi** (+).

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**.
Questa è la 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 **Aggiungi**.

È stata creata un'azione risorsa per cambiare la password di un utente, che verrà elencata nelle pagina Azioni risorsa.

Passi successivi

Pubblicare l'azione risorsa Cambia password dell'utente di prova.

Pubblicazione dell'azione risorsa per il cambiamento della password

Per utilizzare l'azione risorsa Cambia password dell'utente di prova come operazione successiva al provisioning, è necessario pubblicarla.

Prerequisiti

Accedere alla console di vRealize Automation come **architetto XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Selezionare la riga dell'azione Cambia password dell'utente di prova e fare clic sul pulsante **Pubblica**.

Lo stato dell'azione risorsa Cambia password dell'utente di prova cambia in Pubblicato.

Passi successivi

Assegnare un'icona all'azione risorsa. A questo punto è possibile utilizzare l'azione quando si crea un permesso. Per ulteriori informazioni sull'assegnazione di un'icona a un'azione risorsa, vedere [Assegnazione di un'icona a un'azione risorsa](#).

Creazione di un servizio del catalogo per la creazione di un utente di prova

È possibile creare un servizio per visualizzare l'elemento di catalogo di creazione utente nel catalogo servizi e permettere ai clienti di individuare facilmente gli elementi di catalogo correlati alla creazione dell'utente di prova.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Specificare **Crea utente 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**.

È stata creato il servizio Crea utente di prova che verrà elencato nelle pagina Servizi.

Passi successivi

Modificare l'elemento di catalogo Crea utente di prova per includerlo nel servizio.

Associazione dell'elemento di catalogo al servizio Crea utente di prova

Per poter includere un elemento di catalogo Crea utente di prova nel servizio Crea utente di prova, è necessario associarlo al servizio.

Prerequisiti

Accedere alla console di vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Elementi del catalogo**.
- 2 Individuare l'elemento di catalogo Crea utente di prova e fare clic sul suo nome.
- 3 (Facoltativo) Fare clic su **Scegli file** per cambiare l'icona dell'elemento di catalogo.
- 4 Selezionare il servizio **Crea utente di prova** dal menu a discesa **Servizio**.
- 5 Fare clic su **Fine**.

L'elemento di catalogo Crea utente di prova è stato associato al servizio Crea utente di prova.

Passi successivi

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.

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, in modo tale che essi possano visualizzare il servizio nel proprio catalogo e richiedere l'elemento di 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 alla console di vRealize Automation come **amministratore tenant** o **manager del gruppo di business**.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere **Crea utente** 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**.
- 7 Immettere un nome utente nella casella di testo **Utenti e gruppi** e premere Invio.
La persona selezionata vedrà nel catalogo il servizio e gli elementi di catalogo inclusi nel servizio.
- 8 Fare clic su **Avanti**.
- 9 Immettere **Crea utente 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 **Aggiungi**.

È stata creata un'autorizzazione attiva ed esposto il servizio nel catalogo dei clienti.

Una volta effettuato l'accesso alle proprie console vRealize Automation, i clienti del servizio vedranno il servizio creato Crea utente di prova nella scheda **Catalogo**. Essi possono richiedere l'elemento di catalogo creato e incluso nel servizio, Crea utente in un gruppo. Dopo aver creato l'utente, i clienti possono cambiarne la password.

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 alla console di vRealize Automation come **architetto 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**.

È stata creata un'azione risorsa per la migrazione di una macchina virtuale che verrà elencata nella pagina Azioni risorsa.

Passi successivi

[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**.

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](#).

Passi successivi

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 alla console di vRealize Automation come **architetto 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**.

Passi successivi

[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** (✖) 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**.

È stata modificata la presentazione del workflow Migrazione macchina virtuale con vMotion.

Passi successivi

[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** (✎) 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**.

È stata creata un'azione risorsa per migrare una macchina virtuale con vMotion, che verrà elencata nelle pagina Azioni risorsa.

Passi successivi

[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**.

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](#).

Inoltre è stata modificata la presentazione del workflow e definito l'aspetto dell'azione.

Passi successivi

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 alla console di vRealize Automation come **architetto 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**.

È stata creata un'azione risorsa per la creazione di uno snapshot di una macchina virtuale che verrà elencata nella pagina Azioni risorsa.

Passi successivi

[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**.

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](#).

Passi successivi

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 alla console di vRealize Automation come **architetto 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**.

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.

Passi successivi

[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 alla console di vRealize Automation come **architetto 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**.

È stata creata un'azione risorsa per l'avvio di macchine virtuali Amazon che verrà elencata nella pagina Azioni risorsa.

Passi successivi

[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 alla console di vRealize Automation come **architetto XaaS**.

Procedura

- 1 Selezionare **Progettazione > XaaS > Azioni risorsa**.
- 2 Selezionare la riga dell'azione risorsa Start Instances e fare clic su **Pubblica**.

Anche lo stato dell'azione risorsa Start Instances cambia in Pubblicato.

Passi successivi

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 disabilitata.

```
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 alla console di 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**.

Il blueprint viene pubblicato come elemento di catalogo, ma è necessario prima autorizzarlo per renderlo disponibile agli utenti nel catalogo dei servizi.

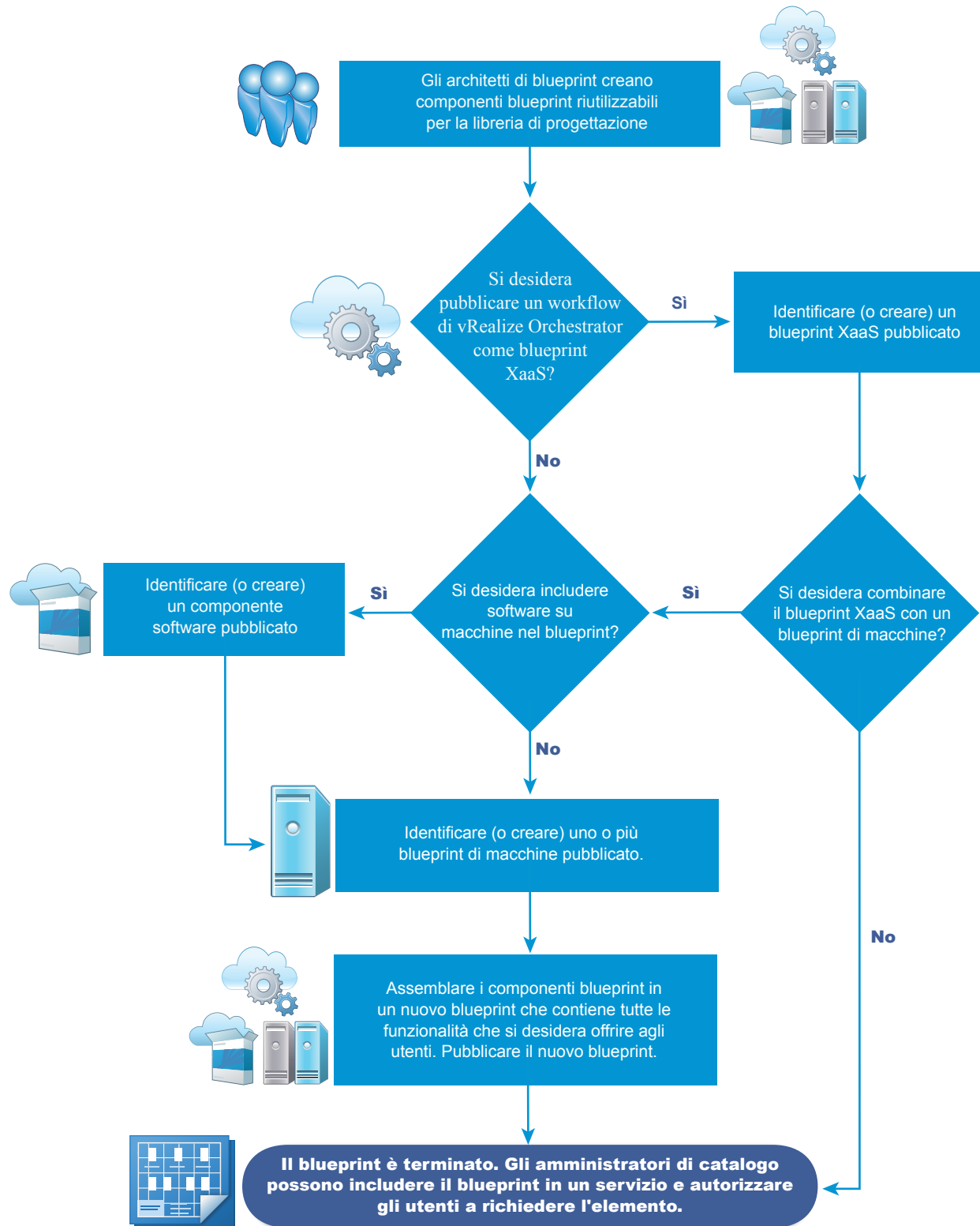
Passi successivi

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.

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.

Figura 4-3. 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.

- **Selezione di un componente della macchina che supporta i componenti di Software**

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 esplicite 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 sempre aggiornamenti dipendenti durante un'operazione di scalabilità verticale o scalabilità orizzontale.

- **Scenario: assemblaggio e test di un blueprint per la fornitura di macchine di cloni collegati MySQL su Rainpole**

Utilizzando privilegi di architetto di applicazioni, architetto software o architetto di IaaS, creare un blueprint per combinare il componente MySQL con il blueprint di cloni collegati CentOS di vSphere creato.

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 all'utilizzo del blueprint principale, tale autorizzazione si estende a tutti gli aspetti del blueprint, inclusi i 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.
- 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.

Regole e considerazioni dei servizi di rete e sicurezza per i blueprint nidificati

- Tutti i componenti di rete e sicurezza nei blueprint esterni possono essere associati alle macchine definite 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.

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.

Selezione di un componente della macchina che supporta i componenti di Software

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 di Software non supportano Internet Protocol versione 6 (IPv6), verificare che i blueprint delle macchine, le prenotazioni e i componenti di rete e sicurezza in uso siano configurati

per l'utilizzo di IPv4 e non di IPv6. 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.

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. 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.

Tavola 4-47. Metodi di provisioning che supportano Software

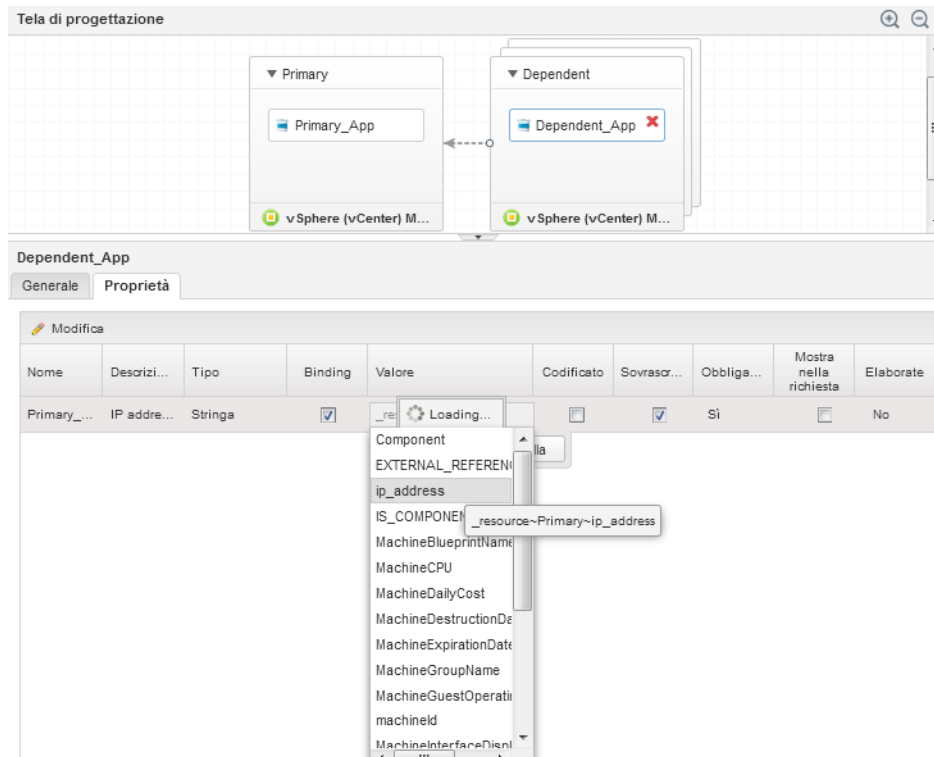
Tipo di macchina	Metodo di provisioning
vSphere	Clona
vSphere	Clone collegato
vCloud Director	Clona
vCloud Air	Clona
Amazon AWS	Immagine macchina Amazon

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`.

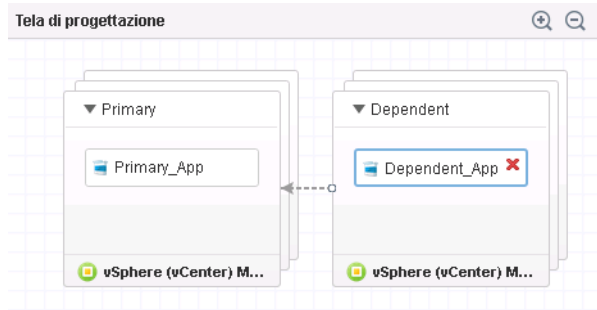
Figura 4-4. Binding di una proprietà software all'indirizzo IP di una macchina

Creazione di dipendenze esplicite 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 sempre aggiornamenti dipendenti durante un'operazione di scalabilità verticale o scalabilità orizzontale.

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.

Per mappare una dipendenza nelle tele dei blueprint, 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 4-5. 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.

Scenario: assemblaggio e test di un blueprint per la fornitura di macchine di cloni collegati MySQL su Rainpole

Utilizzando privilegi di architetto di applicazioni, architetto software o architetto di IaaS, creare un blueprint per combinare il componente MySQL con il blueprint di cloni collegati CentOS di vSphere creato.



Prerequisiti

- Creare un componente Software per installare MySQL su macchine Linux. Vedere [Scenario: creazione di un componente Software MySQL per Rainpole](#).
- Accedere alla console di vRealize Automation come membro del gruppo personalizzato di architetti di Rainpole. Vedere [Scenario: creazione di un gruppo personalizzato per gli architetti Rainpole](#).

Procedura

1 [Scenario: creazione di un contenitore per il blueprint Rainpole MySQL su CentOS](#)

Utilizzando i propri privilegi di architetto IaaS, software o applicazione, creare un contenitore di blueprint e configurare il nome, la descrizione e l'identificatore univoco per il blueprint vSphere MySQL su CentOS.

2 Scenario: aggiunta di software e di una macchina al blueprint MySQL su CentOS per Rainpole

Utilizzando i propri privilegi di architetto IaaS, software o applicazione, trascinare il blueprint della macchina di CentOS per test software pubblicata nella tela per riutilizzare il blueprint come macchina. Il componente software pubblicato viene trascinato sulla macchina virtuale e vengono configurate le proprietà Software specificate nel componente Software.

3 Scenario: aggiunta dell'elemento di catalogo CentOS con MySQL al servizio di Rainpole

Utilizzando i propri privilegi di amministratore tenant, aggiungere il nuovo blueprint al servizio di catalogo di Rainpole in modo da poter verificare il lavoro.

4 Scenario: provisioning di CentOS con la voce di catalogo MySQL per Rainpole

Utilizzando l'account di utente di test, richiedere l'elemento del catalogo di servizi per eseguire il provisioning di una macchina CentOS con MySQL.

Scenario: creazione di un contenitore per il blueprint Rainpole MySQL su CentOS

Utilizzando i propri privilegi di architetto IaaS, software o applicazione, creare un contenitore di blueprint e configurare il nome, la descrizione e l'identificatore univoco per il blueprint vSphere MySQL su CentOS.

Procedura

1 Scegliere **Progettazione > Blueprint**.

2 Fare clic sull'icona **Nuovo** (+).

3 Immettere **MySQL su CentOS** nella casella di testo **Nome**.

4 Rivedere l'identificatore univoco generato.

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. Dato che gli identificatori sono permanenti e unici all'interno del tenant, è possibile utilizzarli per interagire con i blueprint tramite programmazione e per creare binding di proprietà.

5 Immettere **Software MySQL su macchina CentOS vSphere** nella casella di testo **Descrizione**.

6 Configurare un intervallo di lease da cui possono scegliere gli utenti immettendo **1** nella casella di testo **Minimo** e **7** nella casella di testo **Massimo**.

Gli utenti possono scegliere di impostare il lease delle macchine richieste fino a 7 giorni prima di rinnovare i lease o lasciare che le proprie macchine vengano eliminate.

7 Fare clic su **OK**.

Passi successivi

Trascinare sulla tela il componente MySQL e il blueprint della macchina CentOS per software pubblicata.

Scenario: aggiunta di software e di una macchina al blueprint MySQL su CentOS per Rainpole

Utilizzando i propri privilegi di architetto IaaS, software o applicazione, trascinare il blueprint della macchina di CentOS per test software pubblicata nella tela per riutilizzare il blueprint come macchina. Il componente software pubblicato viene trascinato sulla macchina virtuale e vengono configurate le proprietà Software specificate nel componente Software.

Procedura

- 1 Fare clic su **Blueprint** nell'elenco **Categorie**.
- 2 Trascinare **CentOS per il test del software** sulla tela.
- 3 Fare clic su **Componenti software** nell'elenco **Categorie**.
- 4 Trascinare **MySQL per le macchine virtuali Linux** sulla macchina vSphere.
- 5 Fare clic sulla scheda **Proprietà**.
- 6 Aggiornare la proprietà `db_port` di questo blueprint.
 - a Selezionare la proprietà `db_port` e fare clic su **Modifica**.
 - b Immettere **3308** nella casella di testo **Valore**.
Quando un utente del catalogo dei servizi richiede l'elemento, utilizzare il valore predefinito 3308.
 - c Fare clic su **OK**.
- 7 Fare clic su **Fine**.
- 8 Selezionare la riga contenente CentOS con MySQL e fare clic su **Pubblica**.

È stato pubblicato un blueprint che include la macchina CentOS e il componente software MySQL.

Scenario: aggiunta dell'elemento di catalogo CentOS con MySQL al servizio di Rainpole

Utilizzando i propri privilegi di amministratore tenant, aggiungere il nuovo blueprint al servizio di catalogo di Rainpole in modo da poter verificare il lavoro.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.
- 2 Selezionare la riga relativa al servizio di catalogo di Rainpole 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**.

L'elemento di catalogo CentOS con MySQL è pronto per essere richiesto. Non è necessario autorizzare il nuovo elemento di catalogo perché il gruppo di business di Rainpole è stato autorizzato per l'intero servizio di Rainpole.

Passi successivi

Richiedere l'elemento di catalogo CentOS con MySQL per verificare il lavoro.

Scenario: provisioning di CentOS con la voce di catalogo MySQL per Rainpole

Utilizzando l'account di utente di test, richiedere l'elemento del catalogo di servizi per eseguire il provisioning di una macchina CentOS con MySQL.

Procedura

- 1 Disconnettersi dalla console di vRealize Automation.
- 2 Accedere nuovamente utilizzando il nome utente **test_user** e la password **VMware1!**.
- 3 Fare clic sulla scheda **Catalogo**.
- 4 Fare clic sul pulsante **Richiesta** per richiedere un elemento di catalogo.
- 5 Immettere il testo **verifying functionality** nella casella di testo **Descrizione**.
- 6 Fare clic su **Invia** per richiedere l'elemento del catalogo.
- 7 Fare clic sulla scheda **Richiesta** per monitorare lo stato della richiesta.

Terminato il provisioning della macchina, viene visualizzato il messaggio di stato **Completato**.

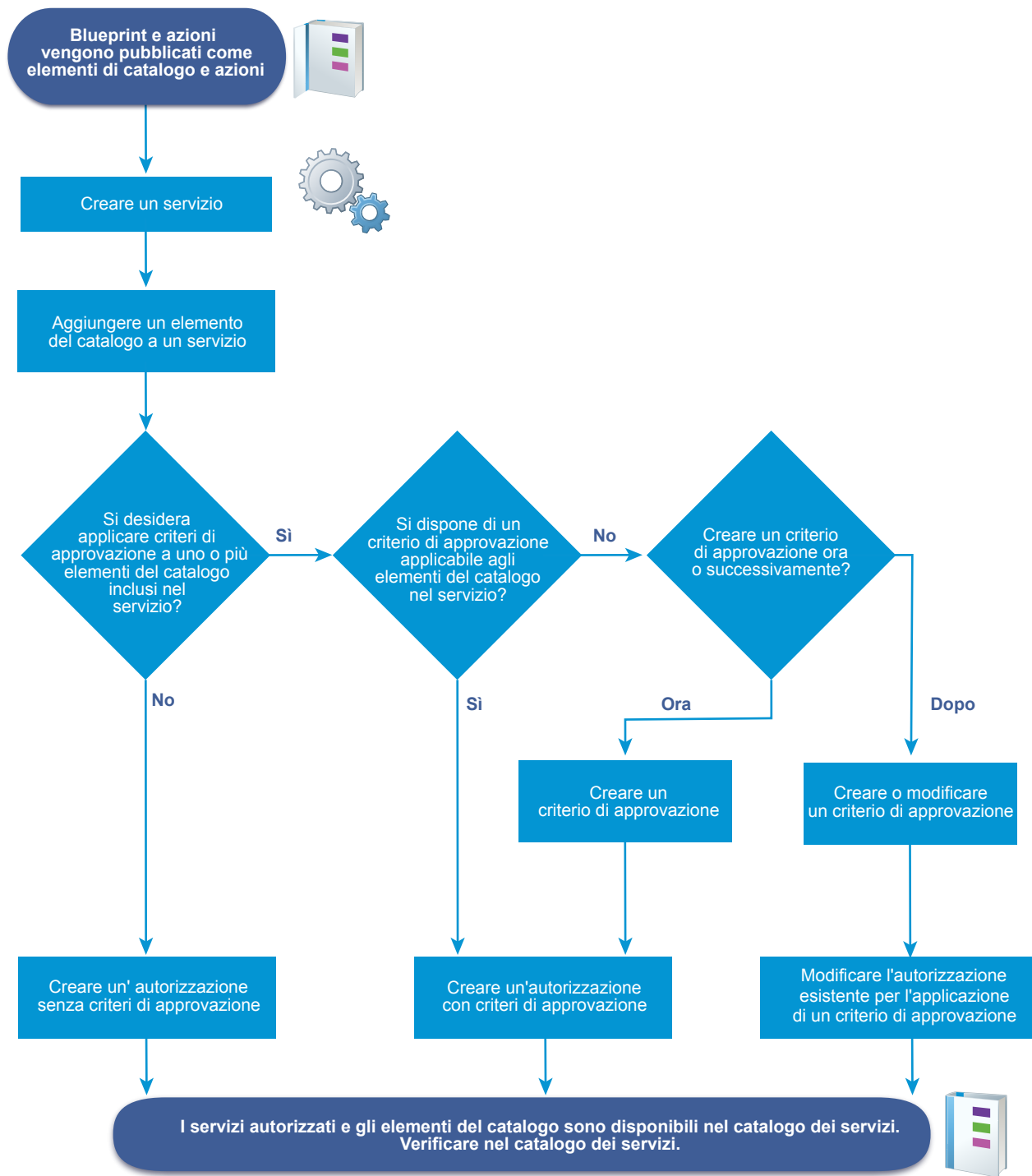
Passi successivi

- Pianificare l'installazione di un ambiente di produzione. Vedere *Architettura di riferimento*.
- Studiare le altre opzioni per la configurazione di vRealize Automation, progettazione ed esportazione di blueprint e la gestione del catalogo dei servizi. Vedere *Configurazione di vRealize Automation*.

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.

Tavola 4-48. 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 alla console di 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**.

Passi successivi

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 alla console di 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**.

Passi successivi

- 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, disabilitarlo 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 autorizzate agli utenti. Se applicabili all'elemento e al suo stato corrente, le azioni vengono rese disponibili per l'elemento fornito in provisioning nella scheda **Elementi** dell'utente del catalogo dei servizi.

È possibile aggiungere un'icona personalizzata all'azione mostrata nella scheda **Elementi**.

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 alla console di 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	I possibili valori sono Attivo , Inattivo e Gestione temporanea . <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.
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.
Nuovo e degno di nota	L'elemento del catalogo è presente nell'area Nuovo e degno di nota della pagina Home.

- 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**.

Passi successivi

- 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 **Elementi** compare l'icona di azione predefinita.

Prerequisiti

- Accedere alla console di 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**.
- 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 **Aggiorna**.

Passi successivi

[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 Elementi. 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 Elementi 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 Elementi. 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 Elementi. 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 autorizzano gli utenti e i gruppi identificati nel permesso a 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 **Elementi** 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 viene creato un permesso, è necessario selezionare un gruppo di business e specificare singoli utenti e gruppi del gruppo di business per tale permesso.

Per sapere come creare un permesso in modo da poter utilizzare le interazioni di servizi, elementi di catalogo e azioni con approvazioni per fornire gli elementi corretti nel catalogo dei servizi, vedere [Creazione di permessi](#).

Prerequisiti

- Accedere alla console di 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 approvazioni a uno o più servizi, elementi di catalogo e azioni.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Configurare le opzioni di 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 Bozza, Attivo, Inattivo.</p> <ul style="list-style-type: none"> ■ Bozza. Gli elementi non sono disponibili nel catalogo dei servizi e non sono stati mai attivi. Una volta attivato un permesso, non è più possibile riportarlo allo stato Bozza. ■ 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, ma il permesso era attivo. Il permesso è stato disattivato dalla data di scadenza o da un utente.

Opzione	Descrizione
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 che un permesso sia disponibile a tutti gli utenti, è necessario avere un gruppo di business. Tutti gli utenti e un gruppo di utenti personalizzato che includa tutti gli utenti, oppure è necessario 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>Aggiungere uno o più utenti o gruppi. Gli utenti o i gruppi disponibili sono limitati ai membri del gruppo di business selezionato.</p> <p>Se lo stato è Bozza, non è necessario specificare gli utenti o i gruppi. Per attivare un permesso, è necessario specificare almeno un utente o 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 un elemento viene aggiunto al servizio in una data successiva, viene aggiunto al catalogo dei servizi per gli utenti autorizzati. I permessi possono includere sia servizi che singoli elementi del 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 di 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>

Opzione	Descrizione
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 autorizzate non vengono visualizzate nel catalogo dei servizi. Vengono bensì visualizzate nella scheda Elementi di 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 l'opzione viene selezionata, i membri del gruppo di business sono autorizzati a eseguire le azioni per gli elementi applicabili in questo permesso. È consigliabile utilizzare questo metodo di autorizzazione delle azioni perché consente di specificare le azioni per i singoli elementi.</p> <p>Se l'opzione non è selezionata, le azioni sono autorizzate agli utenti specificati nel permesso per tutti gli elementi di catalogo applicabili, inclusi o meno nel permesso in oggetto. 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.

Se lo stato del permesso è attivo, il servizio e gli elementi vengono aggiunti al catalogo dei servizi.

Passi successivi

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.

Facciamo l'esempio della creazione di 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 Connie, un membro dei quel gruppo.

Tavola 4-49. Permessi di esempio

Permesso 1	Permesso 2
Gruppo di business: Finanze	Gruppo di business: Finanze
Utenti e gruppi: gruppo Contabilità	Utenti e gruppi: Connie
Elemento di catalogo 1: Criterio A	Elemento di catalogo 1: Criterio C

Connie richiede l'Elemento di catalogo 1 nel catalogo dei servizi. Alla richiesta di Connie viene applicato un criterio differente a seconda dell'ordine di priorità dei permessi del gruppo di business Finanze.


Tavola 4-50. 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. Connie è membro del gruppo di utenti Contabilità. La ricerca di Connie come utente autorizzato si interrompe al Permesso 1 e viene applicato il criterio di approvazione.	Viene applicato il Criterio C. La ricerca di Connie come utente autorizzato si interrompe al Permesso 2 e viene applicato il criterio di approvazione.

Prerequisiti

Accedere alla console di 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** della pagina **Approvazioni**. L'utente richiedente può tenere traccia dello stato di approvazione di una specifica richiesta dalla propria scheda **Richieste**.

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.

Tavola 4-51. 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 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 e 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 e dell'infrastruttura virtuale approvano la richiesta, la macchina viene rilasciata all'utente.

Tavola 4-51. 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 costi, è possibile aggiungere due livelli di pre-approvazione, uno per le risorse della macchina e l'altro per il costo 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 scegliere 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.
			Livello 2 Selezionare Necessaria in base alle condizioni. Configurare la condizione Costo > 15,00 al giorno.	Selezionare Gruppi e utenti specifici. Selezionare il gruppo di utenti personalizzati delle finanze. Selezionare Chiunque può approvare.		

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

Tavola 4-52. Configurazioni dei permessi

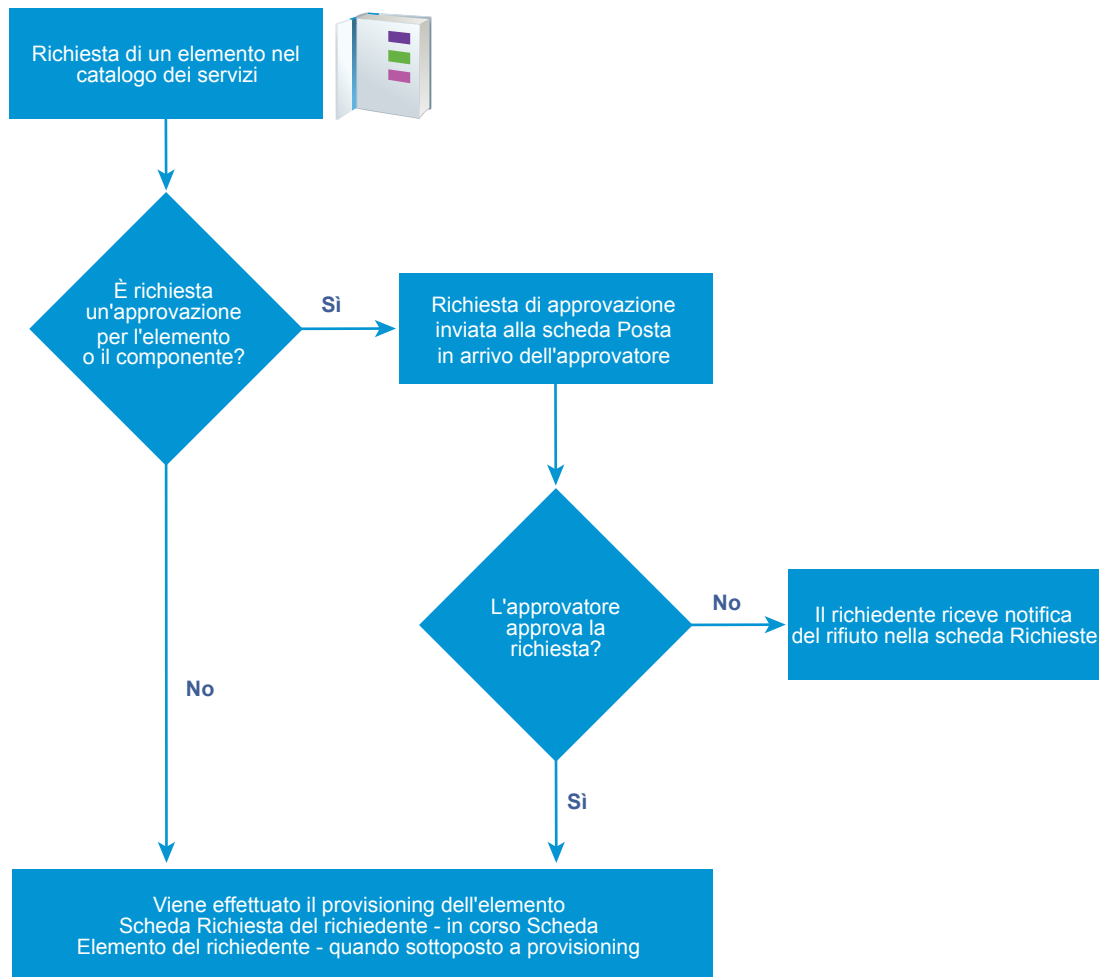
Nome permesso	Gruppo di business	Servizio autorizzato	Elemento autorizzato
Permesso 1	QE	Testing	Richiesta di elemento del catalogo - Macchina virtuale applicata al componente Macchina virtuale
Permesso 2	QE	Training	

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 alla console di 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, lease 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 alla console di 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.

Passi successivi

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](#).

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	La richiesta di approvazione viene inviata agli utenti in base alla condizione specificata.
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	Per poter essere elaborata, è sufficiente che la richiesta venga approvata da uno solo degli approvatori. 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.
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**.

Passi successivi

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, lease 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 alla console di 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.****Passi successivi**

- 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**.

Tavola 4-53. 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**.

Tavola 4-54. 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.

Tavola 4-54. Opzioni dei criteri di approvazione (Continua)

Opzione	Descrizione
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	<p>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.</p>
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.

Tavola 4-55. Opzioni per le informazioni sul livello

Opzione	Descrizione
Nome	Immettere un nome. Il nome del livello viene visualizzato durante la revisione delle richieste con criteri di approvazione.
Descrizione	Immettere una descrizione del livello. Esempio: CPU>4 a VI Admin.
Quando è richiesta l'approvazione?	Selezionare quando deve essere attivato il criterio di approvazione.
Sempre necessaria	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.

Tavola 4-55. Opzioni per le informazioni sul livello (Continua)

Opzione	Descrizione
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>
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>

Tavola 4-55. Opzioni per le informazioni sul livello (Continua)

Opzione	Descrizione
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**.

Tavola 4-56. 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**.

Tavola 4-57. 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 alla console di 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**.

È stato creato un nuovo criterio di approvazione basato su un criterio di approvazione esistente.

Passi successivi

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 alla console di 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**.

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.

Passi successivi

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 alla console di 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**.

Il criterio di approvazione viene eliminato.

Scenario: configurazione del catalogo per consentire agli architetti di Rainpole di testare i blueprint

Utilizzando i propri privilegi di amministratore tenant, creare un servizio di catalogo speciale che contiene pochissima governance, dove gli architetti di Rainpole possono testare efficacemente il proprio lavoro prima di esportare i blueprint nell'ambiente di produzione. L'utente crea un servizio di testing dei blueprint, aggiunge il blueprint vSphere CentOS al servizio e autorizza gli architetti di Rainpole per tutti gli elementi del catalogo e per qualsiasi azione associata al servizio in modo che gli architetti possano verificare il proprio lavoro eseguendo il provisioning degli elementi di catalogo.



Procedura

1 Scenario: creazione di un servizio di catalogo per il test di blueprint Rainpole.

Utilizzando i privilegi di amministratore tenant, creare un catalogo del servizio denominato Servizio Rainpole. Assegnare sé stessi come proprietario e contatto di supporto per questo servizio, in modo che gli architetti Rainpole dispongano delle informazioni di contatto per il supporto in caso di problemi.

2 Scenario: aggiunta dell'elemento del catalogo CentOS vSphere al servizio Rainpole

Utilizzando i privilegi di amministratore tenant, è possibile aggiungere il blueprint della macchina CentOS vSphere pubblicato al servizio Rainpole.

3 Scenario: autorizzazione degli architetti di Rainpole a richiedere elementi di catalogo

Utilizzando i propri privilegi di amministratore tenant, autorizzare gli architetti di Rainpole per tutte le azioni e gli elementi che appartengono al servizio Rainpole.

Scenario: creazione di un servizio di catalogo per il test di blueprint Rainpole.

Utilizzando i privilegi di amministratore tenant, creare un catalogo del servizio denominato Servizio Rainpole. Assegnare sé stessi come proprietario e contatto di supporto per questo servizio, in modo che gli architetti Rainpole dispongano delle informazioni di contatto per il supporto in caso di problemi.

Procedura

1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.

- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Immettere il nome **Rainpole service**.
- 4 Nel menu a discesa Stato selezionare **Attivo**.
- 5 In qualità di amministratore tenant che sta creando il servizio, utilizzare l'opzione di ricerca per aggiungere il proprio nome come Proprietario e Team di supporto.
- 6 Fare clic su **OK**.

Passi successivi

Utilizzando i privilegi di amministratore tenant, aggiungere il blueprint della macchina CentOS vSphere pubblicato al servizio Rainpole.

Scenario: aggiunta dell'elemento del catalogo CentOS vSphere al servizio Rainpole

Utilizzando i privilegi di amministratore tenant, è possibile aggiungere il blueprint della macchina CentOS vSphere pubblicato al servizio Rainpole.

Tutti i blueprint pubblicati per i quali si intende effettuare il provisioning devono far parte di un servizio come elementi del catalogo, ma ogni blueprint può essere un elemento del catalogo in un servizio per volta. Se è necessario pubblicare più servizi di catalogo contemporaneamente, creare copie del blueprint.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Servizi**.
- 2 Nell'elenco dei servizi, selezionare la riga relativa al test del blueprint e scegliere **Gestisci elementi del catalogo**.
- 3 Fare clic sull'icona **Nuovo** (+).
- 4 Selezionare la casella di controllo **CentOS on vSphere**.
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**.

Passi successivi

Utilizzando i privilegi di amministratore tenant, autorizzare gli architetti Rainpole a richiedere elementi del catalogo dal servizio Rainpole.

Scenario: autorizzazione degli architetti di Rainpole a richiedere elementi di catalogo

Utilizzando i propri privilegi di amministratore tenant, autorizzare gli architetti di Rainpole per tutte le azioni e gli elementi che appartengono al servizio Rainpole.

Autorizzando gli architetti di Rainpole a tutte le azioni e gli elementi nel servizio, si rende loro più semplice l'aggiunta di nuovi elementi di catalogo nel servizio a scopo di test. In un ambiente di produzione è possibile utilizzare i permessi in modo differente e configurare una governance stretta. Si può voler gestire quali elementi di catalogo possono essere richiesti da ciascun utente e quali azioni questi possono eseguire su specifici elementi di catalogo di loro proprietà.

Procedura

- 1 Selezionare **Amministrazione > Gestione catalogo > Permessi**.
- 2 Fare clic sull'icona **Nuovo** (+).
- 3 Configurare i dettagli.
 - a Immettere il nome del **permesso dell'architetto di Rainpole**
 - b Selezionare **Attivo** dal menu a discesa **Stato**.
 - c Selezionare il gruppo di business di Rainpole dal menu a discesa **Gruppo di business**.
 - d Aggiungere gli architetti di Rainpole utilizzando la casella di ricerca **Utenti e gruppi**.
 - e Fare clic su **Avanti**.
- 4 Autorizzare il servizio del catalogo di Rainpole.
 - a Fare clic sull'icona **Aggiungi servizi** (+) accanto all'intestazione Servizi autorizzati.
 - b Selezionare **Servizio Rainpole**.
 - c Fare clic su **OK**.

Tutti gli utenti inclusi nell'autorizzazione sono ora autorizzati per tutti gli elementi del catalogo del servizio Rainpole.
- 5 Autorizzare tutte le azioni utente.
 - a Fare clic sull'icona **Aggiungi azioni** (+) accanto all'intestazione Azioni autorizzate.
 - b Selezionare la casella di controllo nell'intestazione della colonna per autorizzare tutte le azioni.
 - c Selezionare la casella di controllo **Le azioni si applicano solo agli elementi definiti in questa autorizzazione** in modo da poter applicare successivamente una governance più restrittiva a questi utenti in altri servizi di catalogo.
 - d Fare clic su **OK**.

Gli architetti sono autorizzati ad eseguire qualsiasi azione applicabile sugli elementi del catalogo di cui effettuano il provisioning dal servizio Rainpole. Non sono autorizzati ad eseguire queste azioni sugli elementi di cui effettuano il provisioning da un altro servizio o attraverso un'autorizzazione diversa.
- 6 Fare clic su **Fine**.

Tutti gli architetti possono ora vedere e richiedere il blueprint della macchina CentOS di vSphere e tutti i nuovi elementi di catalogo aggiunti al loro servizio.

Passi successivi

Utilizzando l'account utente di test locale impostato, richiedere l'esecuzione del provisioning dell'elemento di catalogo CentOS di vSphere per testare il blueprint e la configurazione del catalogo.

Scenario: test della macchina CentOS di Rainpole

Utilizzando l'account utente di test locale creato, richiedere il provisioning della macchina CentOS di vSphere. Accedere alla macchina con provisioning e verificare che funzioni come previsto.



Procedura

1 Scenario: richiesta della macchina virtuale Rainpole

Utilizzando l'account utente di test, richiedere l'elemento del catalogo dei servizi per eseguire il provisioning di una macchina virtuale CentOS su vSphere.

2 Scenario: accesso alla macchina Rainpole con provisioning eseguito

Utilizzando l'account utente di test, accedere alla macchina CentOS di vSphere con provisioning eseguito correttamente.

Scenario: richiesta della macchina virtuale Rainpole

Utilizzando l'account utente di test, richiedere l'elemento del catalogo dei servizi per eseguire il provisioning di una macchina virtuale CentOS su vSphere.

Procedura

- 1 Disconnettersi dalla console di vRealize Automation.
- 2 Accedere nuovamente utilizzando il nome utente **test_user** e la password **VMware1!**.
- 3 Fare clic sulla scheda **Catalogo**.
- 4 Fare clic sul pulsante **Richiesta** per richiedere un elemento di catalogo.
- 5 Immettere il testo **verifying functionality** nella casella di testo **Descrizione**.
- 6 Fare clic su **Invia** per richiedere l'elemento del catalogo.
- 7 Fare clic sulla scheda **Richiesta** per monitorare lo stato della richiesta.

Terminato il provisioning della macchina, viene visualizzato il messaggio di stato **Completato**.

Passi successivi

Accedere alla macchina con provisioning eseguito.

Scenario: accesso alla macchina Rainpole con provisioning eseguito

Utilizzando l'account utente di test, accedere alla macchina CentOS di vSphere con provisioning eseguito correttamente.

Procedura

- 1 Selezionare **Elementi > Macchine**.
- 2 Selezionare la freccia accanto all'elemento CentOS su vSphere.
Sotto l'elemento espanso viene visualizzata la macchina con provisioning eseguito.
- 3 Fare clic sulla macchina con provisioning eseguito.
- 4 Fare clic su **Accesso da remoto alla macchina** sul pannello di destra.
- 5 Accedere alla macchina.

Si è installato vRealize Automation in una distribuzione minima, impostato un prototipo e configurato l'ambiente per lo sviluppo continuato di blueprint.

Passi successivi

- Se è stata acquistata una licenza enterprise di vRealize Automation, è possibile continuare a leggere per apprendere nozioni sul provisioning di macchine con componenti software.
- Pianificare l'installazione di un ambiente di produzione. Vedere *Architettura di riferimento*.
- Studiare le altre opzioni per la configurazione di vRealize Automation, progettazione ed esportazione di blueprint e la gestione del catalogo dei servizi. Vedere *Configurazione di vRealize Automation*.

Scenario: rendere il blueprint dell'applicazione CentOS con MySQL disponibile nel catalogo dei servizi

In qualità di amministratore tenant, è stato richiesto agli architetti dei blueprint di creare un elemento del catalogo per integrare MySQL sulle macchine virtuali CentOS e consentire al proprio gruppo di ingegneri addetti alla distribuzione e alla qualità di 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 alla console di vRealize Automation come **amministratore tenant** o **amministratore del catalogo**.
- Pubblicare un blueprint per integrare MySQL sulle macchine virtuali vSphere CentOS. Vedere [Scenario: assemblaggio e test di un blueprint per la fornitura di macchine di cloni collegati MySQL su Rainpole](#).

- Se si creano blueprint in un ambiente di sviluppo, importare il blueprint nell'ambiente di produzione. Vedere [Esportazione e importazione dei blueprint](#).
- 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**.

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**.

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**.

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.

Passi successivi

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](#).

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 il blueprint dell'applicazione CentOS con MySQL disponibile nel catalogo dei servizi](#).

Procedura

1 [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.

2 [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.

3 [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.

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**.

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**.

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**.

Questo permesso consente di richiedere diverse approvazioni su componenti blueprint differenti.

Passi successivi

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.