

Utilizzo e gestione di vRealize Automation Cloud Assembly

Dicembre 2022

vRealize Automation 8.7

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

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

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

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

Copyright © 2022 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

1 Cos'è Cloud Assembly 8

Come funziona Cloud Assembly 9

2 Tutorial 11

Distribuire una macchina virtuale 13

Configurazione e verifica dell'infrastruttura e delle distribuzioni di vSphere 20

Configurazione e provisioning di un carico di lavoro di produzione 38

Utilizzo dei tag per gestire le risorse di vSphere 46

Aggiunta di un modello cloud al catalogo di Service Broker con un modulo di richiesta personalizzato 56

Onboarding e gestione delle risorse di vSphere 67

Infrastruttura e distribuzioni multi-cloud 77

Parte 1: configurazione dell'infrastruttura di esempio 78

Parte 2: creazione del progetto di esempio 84

Parte 3: progettazione e distribuzione del modello cloud di esempio 85

Configurazione di VMware Cloud on AWS 102

Configurazione di un workflow di VMware Cloud on AWS di base 103

Configurazione di una rete isolata in VMware Cloud on AWS 118

Configurazione dell'integrazione di un provider IPAM esterno per Infoblox 122

Aggiunta degli attributi estendibili obbligatori nell'applicazione Infoblox prima di distribuire il pacchetto di download 124

Download e distribuzione di un pacchetto del provider IPAM esterno 125

Creazione di un ambiente in esecuzione per un punto di integrazione IPAM 127

Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox 128

Configurazione di una rete e di un profilo di rete per l'utilizzo di un IPAM esterno per una rete esistente 132

Definizione e distribuzione di un modello cloud che utilizza un'assegnazione dell'intervallo del provider IPAM esterno 135

Utilizzo delle proprietà specifiche di Infoblox per le integrazioni IPAM nei modelli cloud 138

Controllo della raccolta dei dati di rete mediante filtri Infoblox 142

3 Impostazione di Cloud Assembly per l'organizzazione 144

Che cosa sono i ruoli utente di vRealize Automation 144

Ruoli utente di organizzazione e servizio 146

Ruoli utente personalizzati 174

Casi d'uso: in che modo i ruoli utente possono consentire il controllo dell'accesso 178

Ruolo integrato di Amministratore dell'infrastruttura 198

Aggiunta di account cloud 200

Credenziali necessarie per l'utilizzo di account cloud 201

Creazione di un account cloud di Microsoft Azure	219
Creazione di un account cloud di Amazon Web Services	224
Creazione di un account cloud di Google Cloud Platform	225
Creazione di un account cloud di vCenter	227
Creazione di un account cloud di NSX-V	229
Creazione di un account cloud di NSX-T	230
Creazione di un account cloud di VMware Cloud on AWS	234
Creazione di un account cloud di VMware Cloud Foundation	236
Creazione di un account cloud di VMware Cloud Director in vRealize Automation	237
Integrazione con altre applicazioni	243
Come utilizzare l'integrazione di GitLab e GitHub	244
Come configurare un'integrazione IPAM esterna	250
Come eseguire l'aggiornamento a un pacchetto di integrazione IPAM esterno più recente	252
Configurazione dell'integrazione di My VMware in Cloud Assembly	253
Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly	254
Come si utilizza Kubernetes in Cloud Assembly	259
Che cos'è la gestione della configurazione in Cloud Assembly	286
Creazione di un'integrazione di SaltStack Config	302
Come creare un'integrazione di Active Directory in Cloud Assembly	306
Configurazione di un'integrazione di VMware SDDC Manager	310
Integrazione con vRealize Operations Manager	311
Che cosa sono i piani di onboarding	328
Onboarding delle macchine selezionate come singola distribuzione	330
Configurazione avanzata	334
Come configurare un server proxy Internet	334
Quali operazioni è possibile eseguire con la mappatura di NSX-T a più vCenter	337
Che cosa accade se si rimuove un'associazione di account cloud di NSX	338
Come utilizzare l'SDK IPAM per creare un pacchetto di integrazione IPAM esterno specifico del provider	339
Utilizzo di vRealize Automation con Azure VMware Solution	340
Uso di vRealize Automation con Google Cloud VMware Engine	341
Utilizzo di vRealize Automation con Oracle Cloud VMware Solution	341
Utilizzo di vRealize Automation con VMware Cloud on Dell EMC	342

4 Creazione dell'infrastruttura delle risorse 343

Come aggiungere zone cloud	343
Ulteriori informazioni sulle zone cloud	344
Come aggiungere mappature delle caratteristiche	347
Ulteriori informazioni sulle mappature delle caratteristiche	348
Come aggiungere mappature dell'immagine	348
Ulteriori informazioni sulle mappature dell'immagine	349

Come aggiungere profili di rete	355
Ulteriori informazioni sui profili di rete	355
Utilizzo delle impostazioni di rete	362
Utilizzo delle impostazioni dei gruppi di sicurezza	367
Utilizzo delle impostazioni di bilanciamento del carico	368
Come configurare un profilo di rete per supportare una rete su richiesta per un'integrazione IPAM esterna	369
Come configurare un profilo di rete per supportare una rete esistente per un'integrazione IPAM esterna	373
Come aggiungere profili di storage	373
Ulteriori informazioni sui profili di storage	373
Come utilizzare le schede dei prezzi	377
Come creare le schede dei prezzi per vSphere e VMC	379
Come utilizzare i tag	384
Creazione di una strategia di assegnazione dei tag	387
Utilizzo di tag di funzionalità in Cloud Assembly	388
Utilizzo dei tag di vincolo in Cloud Assembly	390
Tag standard	392
In che modo Cloud Assembly elabora i tag	393
Come configurare una struttura di tag semplice	393
Come utilizzare le risorse	395
Risorse di elaborazione	395
Risorse di rete	396
Risorse di sicurezza	399
Risorse di storage	401
Ulteriori informazioni sulle risorse	402
Configurazione delle risorse tenant multi-provider con vRealize Automation	424
Come creare una zona privata virtuale per vRealize Automation	424
Gestione delle zone private virtuali per i tenant di vRealize Automation	428
Creazione di mappature delle immagini e caratteristiche per i tenant di vRealize Automation	430
Configurazione delle mappature di immagini e caratteristiche specifiche del tenant per vRealize Automation	433
Creazione di sottoscrizioni di estendibilità per provider o tenant	434
Utilizzo delle zone private virtuali legacy nelle versioni più recenti di vRealize Automation	436

5 Aggiunta e gestione di progetti 437

Come aggiungere un progetto per il team di sviluppo	437
Ulteriori informazioni sui progetti	440
Utilizzo dei tag di progetto e delle proprietà personalizzate	440
Utilizzo dei criteri di posizionamento a livello di progetto	442
Costi del progetto	447

Come funzionano i progetti al momento della distribuzione 447

6 Progettazione delle distribuzioni 449

Introduzione alle progettazioni 451

Supporto per la compilazione del codice 454

Binding e dipendenze 456

Controllo delle versioni del modello 458

Input dell'utente nelle richieste 460

Azioni di vRealize Orchestrator come input 466

Gruppi di proprietà 470

Gruppi di proprietà di input 471

Gruppi di proprietà costanti 482

Ulteriori informazioni sui gruppi di proprietà 485

Contrassegni di risorsa per le richieste 486

Espressioni 489

Sintassi dell'espressione 493

Proprietà segrete 500

Accesso remoto 501

Posizionamento del disco SCSI 504

Inizializzazione della macchina 508

Specifiche di personalizzazione di vSphere 508

Comandi di configurazione 509

Indirizzi IP statici di vSphere 512

Distribuzione ritardata 518

Personalizzazione guest di Windows 519

Cluster di macchine e dischi 522

Denominazione personalizzata per le risorse distribuite 525

Risorsa SaltStack Config 528

Configurazioni Terraform 535

Preparazione di un ambiente di runtime di Terraform 535

Preparazione delle configurazioni Terraform 542

Progettazione di configurazioni di Terraform 544

Ulteriori informazioni sulle configurazioni Terraform 549

Tipi di risorse personalizzate 552

Come creare un modello cloud per aggiungere utenti ad Active Directory 556

Come creare un modello cloud che includa SSH 561

Preparazione per il giorno 2 565

Come utilizzare gli input del modello cloud per gli aggiornamenti giorno 2 566

Come creare un'azione risorsa in una macchina virtuale vMotion 567

Altri esempi di codice 576

Modello cloud revisionabile 577

Esempi di risorse di vSphere	584
Core per socket e conteggio CPU	587
Reti, risorse di sicurezza e bilanciamenti del carico	588
Modello cloud abilitato per Puppet con accesso tramite nome utente e password	617
Schema delle proprietà delle risorse	627
Proprietà speciali	627
Altri modi per creare modelli	627
Estensione e automazione dei cicli di vita delle applicazioni	628
Sottoscrizioni dell'azione di estendibilità	629
Sottoscrizioni ai workflow di estendibilità	657
Ulteriori informazioni sulle sottoscrizioni di estendibilità	664

7 Gestione di distribuzioni e risorse 679

Gestione delle distribuzioni	679
Come monitorare le distribuzioni	683
Che cosa è possibile fare se una distribuzione Cloud Assembly non riesce	685
Come gestire il ciclo di vita di una distribuzione completata	688
Quali azioni è possibile eseguire sulle distribuzioni	693
Gestione delle risorse	713
Utilizzo delle singole risorse	717
Utilizzo delle macchine rilevate	719

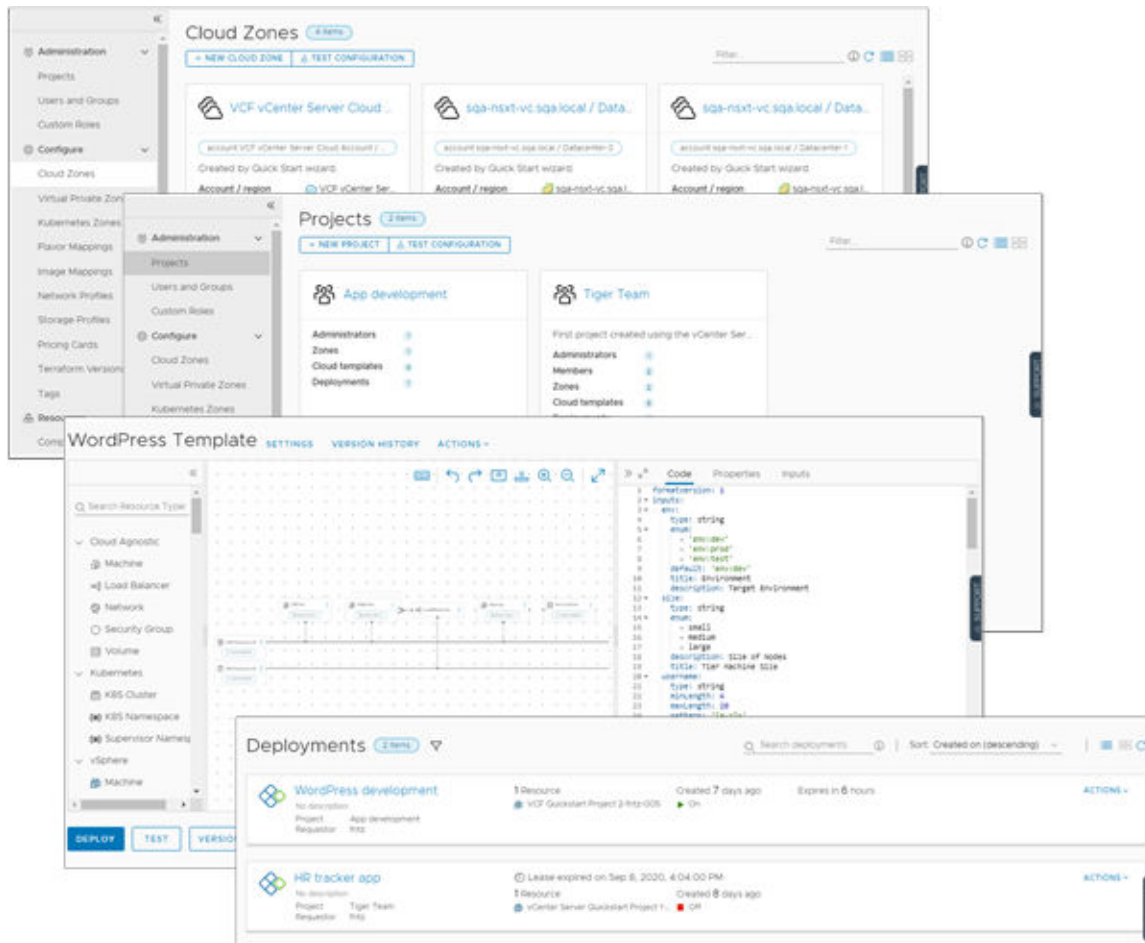
Cos'è Cloud Assembly

1

vRealize Automation Cloud Assembly viene utilizzato per connettersi ai fornitori di soluzioni di cloud pubblico e privato in modo da poter distribuire macchine, applicazioni e servizi creati alle proprie risorse. Insieme al proprio team, è possibile sviluppare modelli cloud come codici in un ambiente che supporti un workflow iterativo, dallo sviluppo al test e alla produzione. Al momento del provisioning, è possibile eseguire la distribuzione per una serie di fornitori di soluzioni cloud. Il servizio è un framework di VMware gestito basato su SaaS e NaaS.

Una panoramica di Cloud Assembly include le seguenti funzioni di base.

- La scheda Risorse mostra lo stato corrente delle risorse rilevate, di cui è stato eseguito il provisioning, l'onboarding e altre risorse. È possibile accedere ai dettagli e alle azioni giorno 2 delle risorse utilizzate per gestire le risorse.
- La scheda Progettazione è il centro di sviluppo. Tramite la tela e l'editor YAML è possibile sviluppare e quindi distribuire le macchine e le applicazioni.
- La scheda Infrastruttura consente di aggiungere e organizzare le risorse e gli utenti del fornitore di soluzioni cloud. Questa scheda fornisce inoltre informazioni sui modelli cloud distribuiti.
- Nella scheda Estendibilità è possibile estendere e automatizzare i cicli di vita delle applicazioni. È possibile sottoscrivere eventi utilizzati per attivare le azioni di estensibilità o i workflow di vRealize Orchestrator.
- Una scheda Avvisi fornisce notifiche relative a capacità, prestazioni e disponibilità per le risorse dell'infrastruttura. Per visualizzare e utilizzare gli avvisi, è necessario disporre di un'integrazione configurata con vRealize Operations Manager.
- La scheda Gestione tenant mostra i diversi tenant configurati se si è provider di servizi e consente di allocare le zone private virtuali o annullarne l'allocazione.



Questo capitolo include i seguenti argomenti:

- [Come funziona Cloud Assembly](#)

Come funziona Cloud Assembly

Cloud Assembly è un servizio di sviluppo e distribuzione di modelli cloud. L'utente e i suoi team utilizzano il servizio per distribuire macchine, applicazioni e servizi alle risorse del fornitore di soluzioni cloud.

L'amministratore di Cloud Assembly, in genere denominato amministratore del cloud, può configurare l'infrastruttura di provisioning e creare i progetti che raggruppano utenti e risorse.

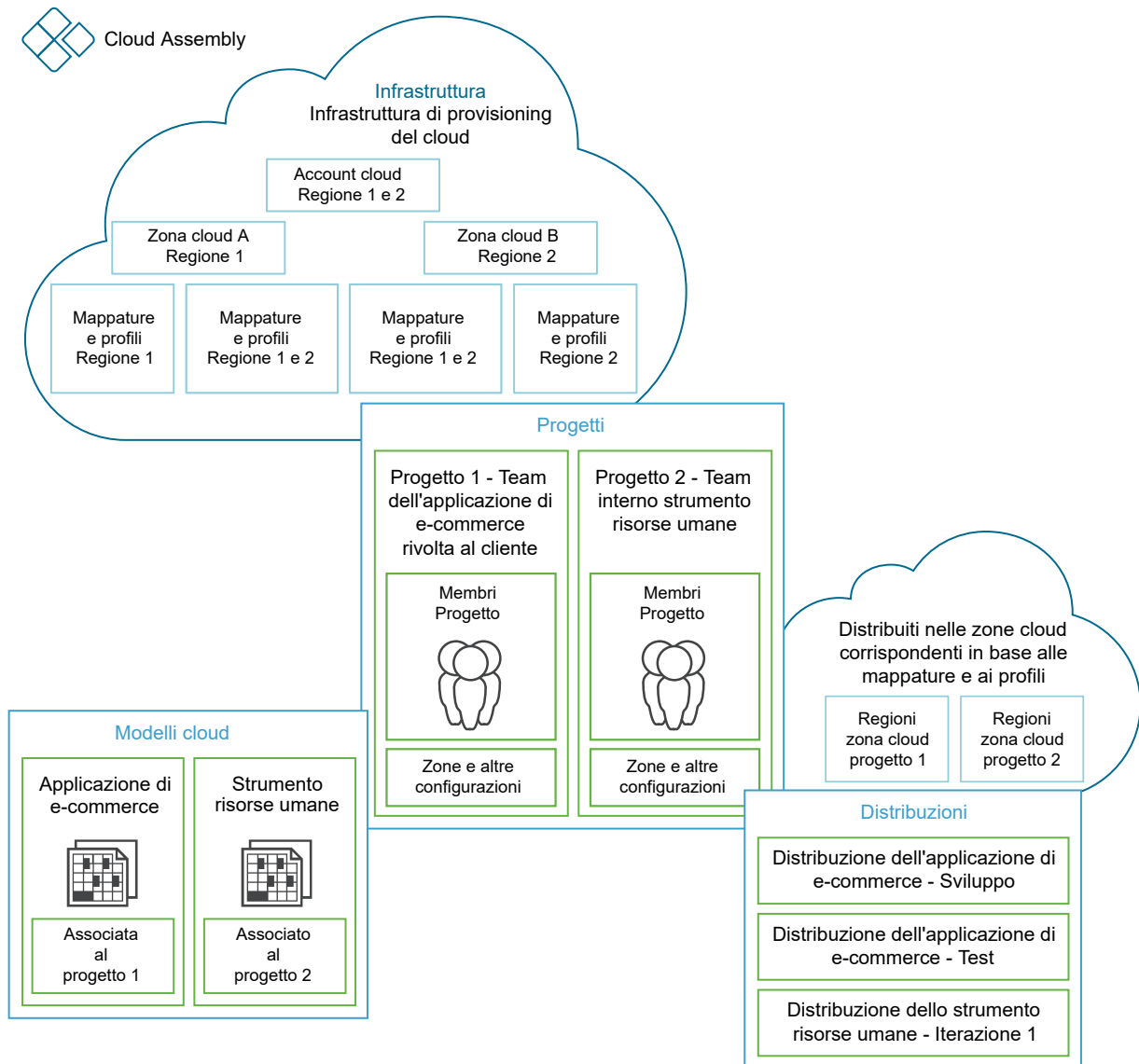
- Aggiungere gli account del fornitore di soluzioni cloud. Vedere [Aggiunta di account cloud a Cloud Assembly](#).
- Determinare quali regioni o datastore sono le zone cloud in cui si desidera che gli sviluppatori eseguano la distribuzione. Vedere [Ulteriori informazioni sulle zone cloud di Cloud Assembly](#).
- Creare criteri che definiscono le zone cloud. Vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).

- Creare progetti che raggruppino gli sviluppatori con le zone cloud. Vedere [Utilizzo dei tag di progetto e delle proprietà personalizzate di Cloud Assembly](#).

Lo sviluppatore di modelli cloud è membro di uno o più progetti. Può creare e distribuire modelli nelle zone cloud associate a uno dei progetti.

- Sviluppare modelli cloud per i progetti mediante la tela di progettazione. Vedere [Introduzione alle progettazioni di Cloud Assembly](#).
- Distribuire i modelli cloud nelle zone cloud del progetto in base a criteri e vincoli.
- Gestire le distribuzioni, compresa l'eliminazione delle applicazioni inutilizzate. Vedere [Gestione delle distribuzioni di Cloud Assembly](#).

Benvenuto in Cloud Assembly. Per un esempio di come definire l'infrastruttura, quindi creare e distribuire un modello cloud, vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).



Tutorial su Cloud Assembly

2

I tutorial illustrano come eseguire le attività comuni e aiutano a migliorare le competenze di Cloud Assembly.

Quando si inizia, si ricorda che in aggiunta ai passaggi nelle esercitazioni sono disponibili ulteriori informazioni in questa guida. Vengono forniti collegamenti agli argomenti pertinenti.

Accesso all'assistenza per l'utente

Inoltre, è importante ricordare che l'assistenza per l'utente è disponibile in tutta l'applicazione.

L'assistenza per l'utente consente di comprendere le funzionalità e fornisce le informazioni necessarie per decidere come popolare le caselle di testo. La documentazione esterna offre un maggior dettaglio nelle informazioni, esempi di codici e casi d'uso.

Tipo di assistenza	Come accedere all'assistenza	Esempio
Guida indicazioni a livello di campo	Fare clic sull'icona Informazioni (i) accanto a un campo.	
Guida del pannello di supporto contestuale	Fare clic sull'icona della guida (?) accanto al nome e all'organizzazione.	
Accedere alla documentazione esterna	Fare clic sul titolo di un articolo etichettato Docs oppure fare clic su Visualizza ulteriori informazioni in VMware Docs .	

Questo capitolo include i seguenti argomenti:

- [Tutorial: Distribuzione di una macchina virtuale in Cloud Assembly](#)
- [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni di vSphere in Cloud Assembly](#)
- [Tutorial: configurazione di Cloud Assembly per il provisioning di un carico di lavoro di produzione](#)
- [Tutorial: utilizzo dei tag in Cloud Assembly per gestire le risorse di vSphere](#)
- [Tutorial: aggiunta di un modello cloud di Cloud Assembly al catalogo di Service Broker con un modulo di richiesta personalizzato](#)
- [Tutorial: onboarding e gestione delle risorse di vSphere in vRealize Automation](#)

- [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#)
- [Tutorial: configurazione di VMware Cloud on AWS per vRealize Automation](#)
- [Tutorial: configurazione dell'integrazione di un provider IPAM esterno specifico del provider per vRealize Automation](#)

Tutorial: Distribuzione di una macchina virtuale in Cloud Assembly

In qualità di amministratore di Cloud Assembly, è possibile distribuire una macchina virtuale semplice che non richiede la creazione di un modello cloud. Se si utilizza per la prima volta Cloud Assembly, questo tutorial illustra il processo di configurazione, la creazione della macchina virtuale e mostra dove gestire la macchina distribuita.

Questo è un modo semplice per distribuire rapidamente una macchina in base a modelli di immagine, caratteristiche di dimensionamento, storage e reti definite dal provider di cloud. È un test rapido dell'account cloud e dei progetti.

È possibile creare una macchina virtuale per uno qualsiasi dei seguenti provider di servizi cloud.

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- vCenter Server
- VMware Cloud on AWS

La piattaforma Google Cloud è l'esempio utilizzato in questo tutorial.

Prima di iniziare

- Verificare di disporre del ruolo di Amministratore di Cloud Assembly. Vedere [Ruoli utente di organizzazione e servizio in vRealize Automation](#). Se non si dispone di questo ruolo utente, non viene nemmeno visualizzata l'opzione di creazione di una nuova macchina virtuale.

Passaggio 1: aggiungere un account cloud

Gli account cloud forniscono le credenziali che Cloud Assembly utilizza per connettersi al provider di cloud.

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud**.
- 2 Fare clic su **Aggiungi account cloud** e selezionare il tipo di account.

È possibile accedere ai dettagli della configurazione utilizzando i seguenti link.

- [Creazione di un account cloud di Amazon Web Services in vRealize Automation](#)
- [Creazione di un account cloud di Google Cloud Platform in vRealize Automation](#)

- Creazione di un account cloud di Microsoft Azure in vRealize Automation
- Creazione di un account cloud di vCenter in vRealize Automation
- Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation

Dopo aver aggiunto l'account cloud, Cloud Assembly raccoglie le informazioni sulle risorse dall'account del provider cloud di destinazione che verranno utilizzate in seguito per distribuire una macchina virtuale.

Passaggio 2: creare un progetto

Il progetto associa gli utenti e le zone cloud dell'account cloud.

In questo tutorial, il nome del progetto è Creazione progetto macchina virtuale. Questo progetto è un progetto dimostrativo che include zone cloud per tutte le piattaforme supportate.

- 1 Selezionare **Infrastruttura > Amministrazione > Progetti**.
- 2 Fare clic su **Nuovo progetto**.
- 3 Immettere un nome.

In questo tutorial, il nome è **Creazione progetto macchina virtuale**.

- 4 Se si desidera che altri utenti utilizzino questo progetto, fare clic sulla scheda **Utenti** e aggiungere tutti gli utenti al progetto.
- 5 Fare clic sulla scheda **Provisioning** e quindi su **Aggiungi zona** per aggiungere almeno una zona cloud per gli account cloud in cui si sta eseguendo la distribuzione.

Tenere presente che questo è un progetto dimostrativo che include una zona cloud per ogni piattaforma del fornitore cloud di supporto.

Create VM Project DELETE

Summary Users **Provisioning** Kubernetes Provisioning Integrations

Zones
Specify the zones that can be used when users provision deployments in this project. ⓘ

+ADD ZONE X REMOVE

<input type="checkbox"/>	Name	Status	Description	Priority	Instances	Memory Limit (MB)	CPU Limit	Storage Limit (GB)	Capability Tags
<input type="checkbox"/>	dsadsa-vsphere / SDDC-Datacenter	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	yingzhi-GCP / us-east1	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	AWS / af-south-1	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	vc65 / Datacenter	--		0	Unlimited	Unlimited	Unlimited	Unlimited	
<input type="checkbox"/>	Azure Test / West US	--		0	Unlimited	Unlimited	Unlimited	Unlimited	

1 - 5 of 5 zones

- 6 Fare clic su **Crea**.

Passaggio 3: creare e distribuire una macchina virtuale

- 1 Selezionare **Risorse > Risorse > Macchine virtuali** e quindi fare clic su **Nuova macchina virtuale**.
- 2 Configurare le impostazioni richieste nella pagina Generale della procedura guidata e fare clic su **Avanti**.

Questo tutorial utilizza Google Cloud Platform come account cloud in cui si desidera distribuire la macchina virtuale.

General Location and basic information.

Select the project, cloud zone, and other basic information for your virtual machine.

Name * Google Cloud Create VM
Enter a name for your machine. A suffix or naming policy may also be applied during provisioning

Project * Create VM Project
Select a project with access to your desired cloud zone

Cloud zone * yingzhi-GCP / us-east1
Select the cloud zone where you want to provision this machine

Tags Enter a new tag
Tags are added to the machine when provisioned

NEXT CANCEL

Tenere presente che questi valori sono solo esempi. I valori devono essere quelli specifici del proprio ambiente.

Tabella 2-1. Valori di esempio per la prima pagina della procedura guidata

Impostazione	Valore di esempio
Nome	Google Cloud crea macchina virtuale
Progetto	Creazione progetto macchina virtuale
Zona cloud	yingzhi-GCP/us-east1

- 3 Selezionare l'immagine e la caratteristica utilizzate per creare la macchina virtuale.

I valori disponibili vengono raccolti dalla zona cloud di destinazione. L'immagine è il sistema operativo e la caratteristica sono le opzioni di dimensione definite. Alcuni tipi di provider di destinazione richiedono di specificare la CPU e la memoria. Questa destinazione richiede la selezione tra le opzioni definite.

Image and flavor size

Image ⓘ

Image *

Flavor ⓘ

Flavor *

CREATE NEXT

3. Storage

4. Networking

Showing 113 of 113 results. [Show all...](#)

4 Fare clic su **Avanti**.

Per distribuire solo la macchina, fare clic su **Crea**. Per questo tutorial, fare clic su **Avanti** per aggiungere l'archivio e la rete facoltativi per questa macchina virtuale.

5 Per aggiungere un nuovo disco, fare clic su **Aggiungi disco rigido** e inserisci **Nome** e **Dimensione**.

Storage and hard disks

Configure storage for this virtual machine.

Hard Disk 1

☒ New disk ☐ Existing disk

Name *

Size * GB

Type

☐ Encrypted

☐ Persistent

6 Fare clic su **Avanti**.

7 Per aggiungere una scheda di rete, fare clic su **Aggiungi scheda di rete**.

8 Selezionare dai risultati della ricerca.

9 Fare clic su **Crea**.

La visualizzazione passa alla pagina Distribuzioni in modo da poter monitorare lo stato di avanzamento della distribuzione.

Passaggio 4: gestire la nuova macchina virtuale come distribuzione

Una volta completato il processo di distribuzione, è possibile iniziare a gestire la distribuzione.

Per ulteriori informazioni sulla gestione delle distribuzioni, vedere [Gestione delle distribuzioni di Cloud Assembly](#).

Per un elenco di tutte le azioni giorno 2 possibili su tutti i tipi di risorse, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

1 Selezionare **Risorse > Distribuzioni** e individuare la macchina virtuale.

In questo tutorial, il nome della distribuzione è Google Cloud crea macchina virtuale.

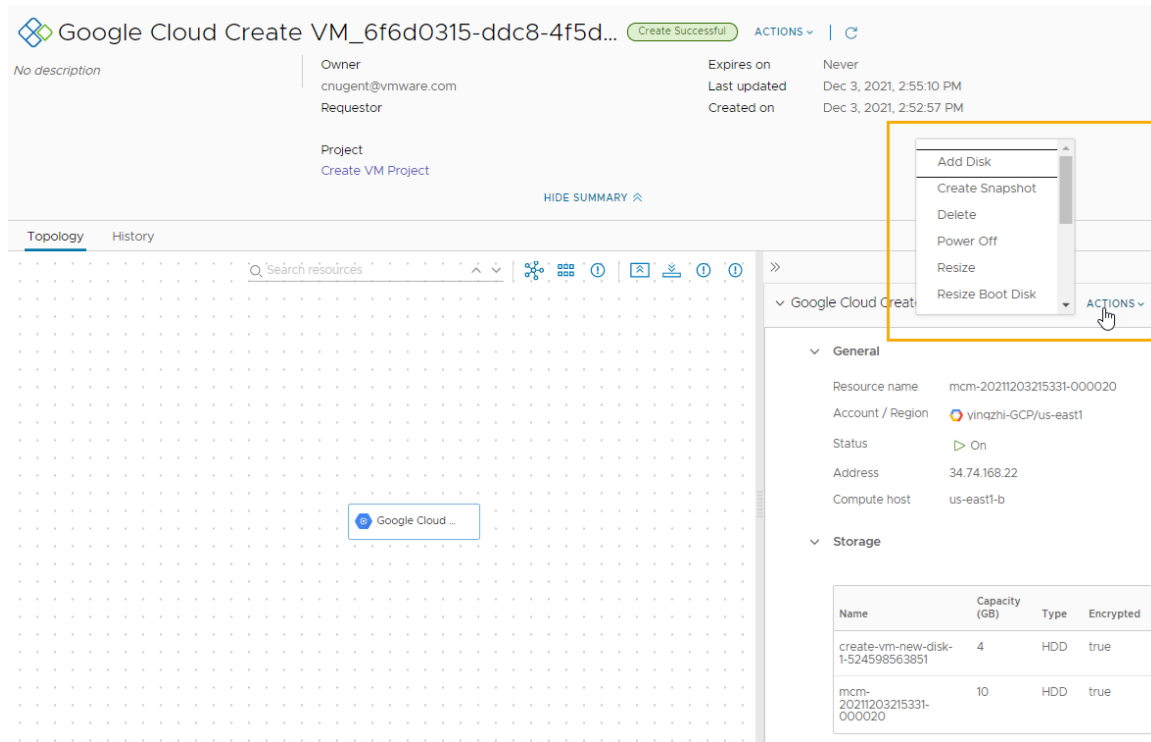
2 Per eseguire un'azione a livello di distribuzione consentita sulla distribuzione da questa visualizzazione, fare clic sui puntini di sospensione verticali e selezionare l'azione.

	Name	Address	Owner	Project	Status	Expires on	Price
>	gcp_811d09ff-efe1-4da4-a949-5be98ab62c...		@vmware.com	Create VM Project		Never	
>	Google Cloud Create VM_6f6d0315-ddc8-4...		@vmware.com	Create VM Project		Never	
>			@vmware.com	cmbu-08-project		Never	
>			@vmware.com	Create VM Project		Never	
>			@vmware.com	Sales		Never	
>			@vmware.com	Sales		Never	

3 Per ulteriori informazioni sulla distribuzione, inclusa la topologia, fare clic sul nome della distribuzione.

Si noti che la topologia di questa distribuzione è semplice. Le distribuzioni più complesse forniscono anche la topologia completa che potrebbe includere macchine, bilanciamenti del carico, connessioni di rete e altri componenti.

È inoltre possibile visualizzare la cronologia della distribuzione, che è un registro di tutte le azioni sui componenti della distribuzione, ed eseguire le azioni consentite a livello di macchina.



Passaggio 5: gestire la nuova macchina virtuale come risorsa

Oltre a gestire la macchina virtuale come distribuzione, è possibile gestirla insieme alle altre risorse. Le risorse possono includere macchine virtuali, volumi di storage e risorse di rete e di sicurezza distribuiti, rilevati e di cui è stato eseguito l'onboarding.

Le risorse individuate sono quelle raccolte dall'istanza del cloud. È possibile gestire le risorse rilevate con un set limitato di azioni giorno 2, ad esempio accensione e spegnimento. Per ulteriori informazioni sull'utilizzo delle risorse rilevate, vedere [Come si utilizzano le risorse rilevate in Cloud Assembly](#).

Le risorse di cui è stato eseguito l'onboarding sono risorse rilevate che sono state sottoposte a gestione completa. Possono essere gestite con le opzioni di azione giorno 2 più robuste. Per ulteriori informazioni su come eseguire l'onboarding delle risorse rilevate, vedere [Che cosa sono i piani di onboarding in Cloud Assembly](#).

Quando si lavora con questa macchina distribuita, è idonea per ulteriori azioni giorno 2. La disponibilità delle azioni dipende dallo stato della macchina e dalle azioni del giorno 2 che si è autorizzati a eseguire.

- 1 Selezionare **Risorse > Risorse > Macchine virtuali**.
- 2 Individuare la macchina.

Virtual Machines ▼ Search resources ⓘ

[+ NEW VM](#)

Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
vm-administrator-VLDX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-N6CE...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
mcm-20211203215331-0...	Google Cloud Create VM_6f...	On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-

- 3 Per eseguire un'azione a livello di macchina consentita sulla macchina da questa visualizzazione, fare clic sui puntini di sospensione verticali e selezionare l'azione.

Virtual Machines ▼ Search resources ⓘ

[+ NEW VM](#)

Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
vm-administrator-VLDX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-N6CE...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
mcm-20211203215331-0...	Google Cloud Create VM_6f...	On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-
vm-administrator-7COL...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-Q628...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-BBJM...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-7RQZ...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-BON...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-2M3...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-BSKX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
Load-Balancer-NSX-Uni...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-X4FT...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-GLA...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-757X...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
Load-Balancer-NSX-Uni...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
e2e-a8n-mcm545178-18...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
mcm-20211203165342-...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
Load-Balancer-NSX-Uni...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
ThinWin7-LinkedClone...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-

- 4 Per rivedere i dettagli della risorsa macchina, fare clic sul nome della macchina.

I dettagli utili in questo esempio includono lo storage, la rete e le proprietà personalizzate.

Virtual Machines ▼ Search resources ⓘ

[+ NEW VM](#)

Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
vm-administrator-VLDX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-N6CE...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
mcm-20211203215331-0...	Google Cloud Create VM_6f...	On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-
vm-administrator-7COL...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-Q628...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-BBJM...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-7RQZ...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-BON...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-2M3...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-BSKX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
Load-Balancer-NSX-Uni...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-X4FT...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-GLA...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-757X...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
Load-Balancer-NSX-Uni...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
e2e-a8n-mcm545178-18...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
mcm-20211203165342-...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
Load-Balancer-NSX-Uni...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
ThinWin7-LinkedClone...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-

Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni di vSphere in Cloud Assembly

Coloro che non conoscono vRealize Automation o desiderano solo usufruire di un corso di aggiornamento troveranno in questo tutorial una guida per l'intero processo di configurazione di Cloud Assembly. È possibile aggiungere endpoint di account cloud vSphere, definire l'infrastruttura, aggiungere utenti ai progetti e quindi progettare e distribuire un carico di lavoro utilizzando VMware Cloud Templates in base ai tipi di risorse di vSphere, imparando il processo man mano che la procedura avanza.

Sebbene questo tutorial copra solo gli aspetti iniziali, grazie a esso si potrà fornire automazione self-service e sviluppo iterativo operanti in più cloud pubblici e privati. Questo tutorial si concentra su VMware vCenter Server e NSX-T. Dopo aver completato questo workflow, sarà possibile applicare ciò che si è appreso per aggiungere altri tipi di account cloud e fornire modelli cloud più sofisticati.

Nel corso dei diversi passaggi saranno forniti esempi di dati. Sostituire gli esempi con i valori validi per l'ambiente in uso.

È possibile eseguire tutti i passaggi descritti in questo tutorial in Cloud Assembly.

Questo processo di configurazione è alla base dell'esperienza di sviluppo con Cloud Assembly. Quando si crea l'infrastruttura e si maturano le competenze nello sviluppo dei modelli cloud, questo workflow sarà ripetuto ed esteso.

Operazioni preliminari

- Verificare di disporre del ruolo di Amministratore di Cloud Assembly. Vedere [Ruoli utente di organizzazione e servizio in vRealize Automation](#).
- Se non sono state utilizzate le procedure guidate di VMware vCenter Server o VMware Cloud Foundation QuickStart nella console di vRealize Automation, è possibile farlo ora.

Questi workflow guidati includono la maggior parte degli aspetti di configurazione contenuti in questo tutorial, ma non tutti.

Questo tutorial è un'esperienza pratica che arricchisce il bagaglio conoscitivo in tema di implementazione di un'infrastruttura e distribuzione di un carico di lavoro.

Consultare [Come impostare Cloud Assembly](#) nella *Guida introduttiva*.

- Se non è ancora stata utilizzata la configurazione guidata disponibile in Cloud Assembly, è possibile farlo a questo punto. La configurazione guidata consente di eseguire la maggior parte delle procedure descritte in questo tutorial. Per aprire la configurazione guidata, fare clic su **Configurazione guidata** sul lato destro della barra delle schede.
- Assicurarsi di disporre delle credenziali di vCenter Server e NSX. Per ulteriori informazioni sulle autorizzazioni necessarie per le credenziali, vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#). Se si intende aggiungere altri utenti ai progetti, verificare che siano membri del servizio Cloud Assembly.

Passaggio 1: aggiungere gli account cloud di vCenter Server e NSX

Gli account cloud forniscono le credenziali utilizzate da vRealize Automation per connettersi a vCenter Server e al server NSX associato.

1 Aggiungere l'account cloud di vCenter Server.

L'account cloud di vCenter Server fornisce le credenziali di vCenter che Cloud Assembly utilizza per individuare le risorse e distribuire i modelli cloud.

Per ulteriori informazioni sugli account cloud di vCenter Server, vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).

- a Selezionare **Infrastruttura > Connessioni > Account cloud**.
- b Fare clic su **Aggiungi account cloud** e selezionare **vCenter**.
- c Immettere i valori.

New Cloud Account

Name * vCenter Server Account

Description

vCenter Server Credentials

vCenter IP address / FQDN * sc2vc05.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

VALIDATE ✓ Credentials validated successfully. ✕

Configuration

Allow provisioning to these datacenters * ☒ wld01-DC

☒ Create a cloud zone for the selected datacenters

NSX cloud account

Capabilities

Capability tags ⓘ

ADD **CANCEL**

Tenere presente che questi valori sono solo esempi. I valori saranno quelli specifici del proprio ambiente.

Impostazione	Valore di esempio
Nome	Account vCenter Server
Indirizzo IP/nome di dominio completo di vCenter	your-dev-vcenter.company.com
Nome utente e password	vCenterCredentials@yourCompany.com

- d Per verificare le credenziali, fare clic su **Convalida**.
- e Per poter eseguire l'operazione **Consenti provisioning a questi data center**, selezionare uno o più data center.
- f Ignorare l'account cloud di NSX. Verrà configurato in un secondo momento, collegando l'account di vCenter Server all'account cloud di NSX.
- g Fare clic su **Aggiungi**.

2 Aggiungere un account cloud di NSX associato.

L'account cloud di NSX-T fornisce le credenziali di NSX-T che Cloud Assembly utilizza per individuare le risorse di rete e distribuire reti con modelli cloud.

Per ulteriori informazioni sugli account cloud di NSX-T, vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).

- a Selezionare **Infrastruttura > Connessioni > Account cloud**.
- b Fare clic su **Aggiungi account cloud** e selezionare NSX-T o NSX-V. Questo tutorial utilizza **NSX-T**.
- c Immettere i valori.

New Cloud Account

Name * NSX-T Account

Description

NSX-T Credentials

NSX-T IP address / FQDN * sc2vc05-vip-nsx-mgmt.cmbu.local ⓘ

Username * mgmt@cmbu.local

Password *

NSX mode Policy ⓘ

VALIDATE ✔ Credentials validated successfully. ✕

Associations

vCenter cloud accounts + ADD ✕ REMOVE

<input type="checkbox"/>	Name	Status	Identifier	Type
<input type="checkbox"/>	vCenter Server Account	✔ OK	sc2vc05.cmbu.local	vCenter

1 - 1 of 1 cloud accounts

Capabilities

Capability tags Enter capability tags ⓘ

ADD CANCEL

Questi valori sono solo esempi. I valori saranno quelli specifici del proprio ambiente.

Impostazione	Valore di esempio
Nome	Account NSX-T
Indirizzo IP/nome di dominio completo di vCenter	your-dev-NSX-vcenter.company.com
Nome utente e password	NSXCredentials@yourCompany.com
Modalità NSX	<p>Se non si sa cosa selezionare</p> <p>È l'occasione giusta per provare la Guida in linea interna al prodotto. Fare clic sull'icona delle informazioni a destra del campo. La guida a livello di campo include informazioni che possono aiutare a configurare quella specifica opzione.</p> <p>In questo esempio, selezionare Criterio.</p>

- d Per verificare le credenziali, fare clic su **Convalida**.
 - e Per associare l'account cloud di vCenter creato nel passaggio precedente, fare clic su **Aggiungi** e quindi selezionare l'**account di vCenter**.
- Questa associazione dell'account cloud di vCenter garantisce la sicurezza della rete.
- f Nella pagina dell'account cloud di NSX, fare clic su **Aggiungi**.

Passaggio 2: definire le risorse di elaborazione della zona cloud


Le zone cloud sono gruppi di risorse di elaborazione in un account/una regione che vengono poi rese disponibili ai progetti. I membri del progetto distribuiscono modelli cloud utilizzando le risorse nelle zone cloud assegnate. Se si desidera avere un controllo più dettagliato sulla posizione in cui vengono distribuiti i modelli cloud del progetto, è possibile creare più zone cloud con risorse di elaborazione diverse.

Attraverso gli account/le regioni, i fornitori di soluzioni cloud collegano le risorse a regioni o datastore isolati. L'account indica il tipo di account cloud, mentre la regione indica la regione o il datastore. vCenter Server utilizza i datastore, mentre le risorse di provisioning sono i cluster e i pool di risorse selezionati.

Per questo tutorial, è necessario assicurarsi che le zone cloud includano le risorse che supportano gli obiettivi del team di sviluppo del progetto e i requisiti di budget e gestione.

Per informazioni sulle zone cloud, vedere [Ulteriori informazioni sulle zone cloud di Cloud Assembly](#).

- 1 Selezionare **Infrastruttura > Configura > Zone cloud**.
- 2 Fare clic sulla zona cloud che è stata aggiunta per l'istanza di vCenter Server e immettere i valori.


vCenter Account Cloud Zone
DELETE

Summary
Compute
Projects

A cloud zone defines a set of compute resources that can be used for provisioning.

Account / region *

vCenter Account / wld01-DC

Name *

vCenter Account Cloud Zone

Description

Placement policy *

DEFAULT

Folder

Select folder

Capabilities

Capability tags are effectively applied to all compute resources in this cloud zone, but only in the context of this cloud zone.

Capability tags

Enter capability tags

SAVE

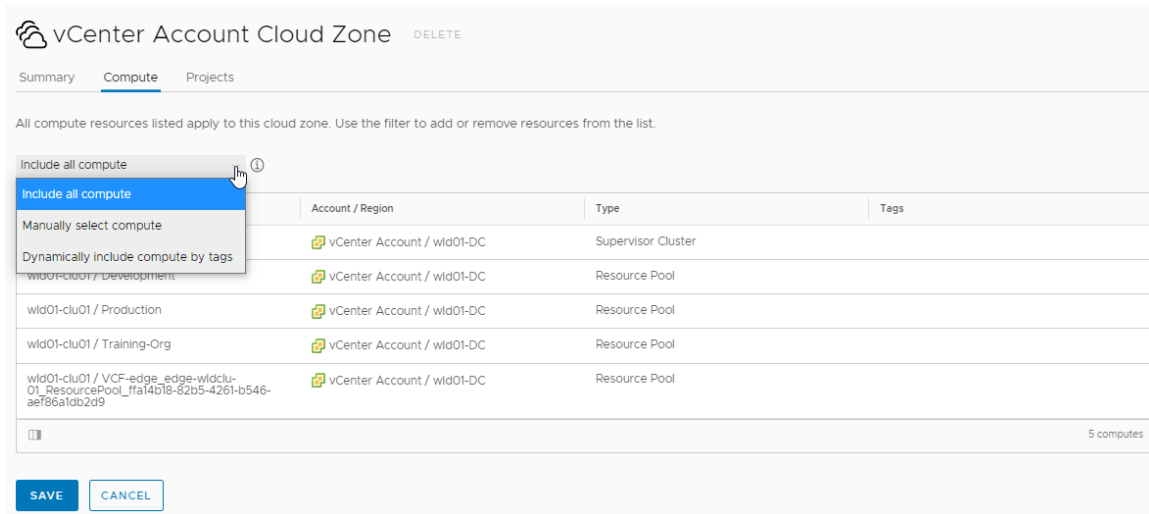
CANCEL

Impostazione	Valore di esempio
Account/Regione	Account vCenter/nome data center
Nome	Zona cloud di vCenter Server Questo valore non può essere modificato dopo averlo creato. Se si desidera configurare un altro data center un vCenter Server diverso, è necessario creare una nuova zona cloud in cui sia possibile selezionare l'account/la regione.
Descrizione	Tutte le risorse di elaborazione di vCenter Server per lo sviluppo.
Criterio	Predefinito Consultare la guida in caso di domande sul valore di un campo.

Tenere presente che tutti i valori sono solo esempi. Le specifiche della zona dipenderanno dall'ambiente in oggetto.

- Fare clic sulla scheda **Risorsa di elaborazione** e verificare che le risorse di elaborazione siano tutte presenti.

Se è necessario escluderne una, passare a **Seleziona manualmente elaborazione e aggiungere** solo quelle che si desidera includere nella zona cloud.



4 Fare clic su **Salva**.

5 Ripetere il processo per tutte le zone cloud aggiuntive, ma è necessario assicurarsi che i nomi delle zone siano univoci.

Passaggio 3: configurare le possibili risorse disponibili per l'account/la regione

Alla zona cloud è stato aggiunto l'account/la regione. A questo punto si può procedere con la definizione delle dimensioni possibili delle macchine (mappatura caratteristiche), mappature delle immagini, profili di rete e profili di storage per l'account cloud. Le definizioni di mappatura e profili vengono valutate per una corrispondenza quando si distribuisce un modello di cloud, per assicurarsi che il carico di lavoro includa i valori appropriati per dimensione macchina (caratteristica), immagine, reti e storage.

1 Configurare le mappature delle caratteristiche per l'account/le regioni.

Le caratteristiche sono talvolta indicate come taglie di t-shirt. In base alla modalità di configurazione del modello cloud, la mappatura della caratteristica applicata determina il numero di CPU e la memoria.

Per informazioni sulle mappature delle caratteristiche, vedere [Ulteriori informazioni sulle mappature delle caratteristiche in vRealize Automation](#).

a Selezionare **Infrastruttura > Configura > Mappature caratteristiche**.

b Fare clic su **Nuova mappatura caratteristica** e immettere i valori che definiscono le macchine di piccole, medie e grandi dimensioni.

Si ricorda che i valori sono puramente esemplificativi. È necessario selezionare l'account/le regioni pertinenti e definire il dimensionamento.

small DELETE

Allows you to define flavors by name in a cloud-agnostic way. ⓘ

Flavor name * small

Configuration *

Account / Region	Value
vCenter Account / wld01-DC	2
	1

GB ▾ - +

Impostazione	Valore di esempio
Nome caratteristica	piccolo
Account/Regione	Account vCenter/data center
Valore CPU	2
Valore memoria	1 GB

- c Fare clic su **Crea**.
- d Per creare dimensioni aggiuntive, configurare mappature di caratteristiche medie e grandi per l'account/la regione.

Impostazione	Valore di esempio
Nome caratteristica	medio
Account/Regione	Account vCenter/data center
Valore CPU	4
Valore memoria	2 GB
Nome caratteristica	grande
Account/Regione	Account vCenter/data center
Valore CPU	8
Valore memoria	4 GB

- 2 Configurare le mappature delle immagini per l'account/le regioni.

Le immagini sono il sistema operativo per le macchine nel modello cloud. Quando si utilizzano immagini vCenter Server, selezionare modelli di vCenter.

Per informazioni sulle mappature delle immagini, vedere [Ulteriori informazioni sulle mappature dell'immagine in vRealize Automation](#).

- a Selezionare **Infrastruttura > Configura > Mappature immagini**.
- b Fare clic su **Nuova mappatura immagine** e cercare le immagini per l'account/la regione.

Si ricorda che i valori sono puramente esemplificativi. È necessario selezionare immagini pertinenti che sono state individuate nel proprio account o nella propria regione.

centos DELETE

Allows you to define images or machine templates by name in a cloud-agnostic way. ⓘ

Image name * centos

Configuration * Account / Region Image Constraints Cloud Configuration

Q vCenter Account / wldi Q centos7 Example: license:none ⓘ + ADD ⋮

Impostazione	Valore di esempio
Nome immagine	CentOS
Account/Regione	Account vCenter
Immagine	centos7


- c Fare clic su **Crea**.
- d Ripetere il processo per creare mappature di immagini aggiuntive. Ad esempio, una mappatura di Ubuntu per l'account/la regione.

3 Configurazione i profili di rete.

I profili di rete definiscono le reti e le impostazioni di rete disponibili per un account/una regione. I profili devono supportare gli ambienti di distribuzione di destinazione.


Questa attività fornisce le informazioni di configurazione minime per una soluzione correttamente funzionante. Per ulteriori informazioni sui profili di rete, iniziare con [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

- a Selezionare **Infrastruttura > Configura > Profilo di rete**.
- b Fare clic su **Nuovo profilo di rete** e creare un profilo per l'account/la regione di account vCenter/data center.

 **Network Profile** [DELETE](#)

[Summary](#) [Networks](#) [Network Policies](#) [Load Balancers](#) [Security Groups](#)


A network profile defines a group of networks and network settings used when machines are provisioned.

Account / region  vCenter Account / wld01-DC

Name *


Description

Capabilities
Capability tags listed here are matched to constraint tags in the cloud template.


Capability tags 

Impostazione	Valore di esempio
Account/Regione	Account vCenter/data center
Nome	Profilo di rete
Descrizione	Reti per i team di sviluppo.







c Fare clic sulla scheda **Reti** e su **Aggiungi rete**.

 **Network Profile** [DELETE](#)

[Summary](#) [Networks](#) [Network Policies](#) [Load Balancers](#) [Security Groups](#)

Networks listed here are used when provisioning to existing, on-demand, or public networks. 

[+ ADD NETWORK](#) [TAGS](#) [MANAGE IP RANGES](#) [REMOVE](#)

<input type="checkbox"/>	Name	Account / Region	Zone	Network Domain	CIDR	Support Public IP	Default for Zone	Origin	Tags
<input type="checkbox"/>	DevProject-004	 NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.64/27	--	--	 Deployed	
<input type="checkbox"/>	External-mcm13/3520-150877845350	 NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	172.16.1.64/28	--	--	 Discovered	
<input type="checkbox"/>	seg-domain-c8e2a5389de-2772-43f5-9eaa-eddc05e35996-vmware-system-nsx-0	 NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	10.244.0.0/28	--	--	 Discovered	external_id.8... ncp/project_u... ncp/cluster.d... ncp/version.1... ncp/project.v...

1 - 3 of 3 networks

d Selezionare le reti NSX che si desidera rendere disponibili per il team di sviluppo delle applicazioni.

In questo esempio, era presente una rete NSX-T denominata DevProject-004.

e Fare clic sulla scheda **Criteri di rete** e creare un criterio.

Impostazione	Valore di esempio
Criterio di isolamento	Nessuna
Router logico di livello 0	Router di livello 0
Cluster edge	Cluster edge

f Fare clic su **Crea**.

4 Configurare i profili di storage.

I profili di storage definiscono i dischi per un account/una regione. I profili devono supportare gli ambienti di distribuzione di destinazione.

Per ulteriori informazioni sui profili di storage, vedere [Ulteriori informazioni sui profili di storage in vRealize Automation](#).

a Selezionare **Infrastruttura > Configura > Profilo di storage**.

b Fare clic su **Nuovo profilo di storage** e creare un profilo per l'account/la regione di vCenter Server/data center.

Se non specificato nella tabella, mantenere i valori predefiniti.

The screenshot shows the 'Storage Profile' configuration interface. It includes fields for Account/region (vCenter Account / wld01-DC), Name (Storage Profile), Description, Disk type (Standard disk selected), Storage policy (Datastore default), Datastore / cluster (wld01-sc2vc05-wld01-clu01-vsan01), Provisioning type (Unspecified), Shares (Unspecified), Limit IOPS, Disk mode (Dependent), and Capability tags. There are also checkboxes for 'Supports encryption' and 'Preferred storage for this region' (checked). Save and Cancel buttons are at the bottom.

Impostazione	Valore di esempio
Account/Regione	Account vCenter/data center
Nome	Profilo di storage
Datastore/cluster	È stato selezionato un datastore con capacità sufficiente e accessibile a tutti gli host.
Storage preferito per questa regione	Selezionare la casella di controllo.

c Fare clic su **Crea**.

Passaggio 4: creare un progetto

Questo è il punto in cui si inizia a valutare concretamente gli obiettivi del progetto.

- Quali utenti devono accedere alle risorse di elaborazione in modo da poter creare e distribuire un modello cloud delle applicazioni? Per ulteriori informazioni su cosa i diversi ruoli del progetto possono visualizzare ed eseguire, vedere [Ruoli utente di organizzazione e servizio in vRealize Automation](#).
- I membri del progetto creeranno applicazioni che vanno dallo sviluppo alla produzione? Quali sono le risorse necessarie?
- Di quali zone cloud hanno bisogno? Quali sono le priorità e i limiti da includere in ogni zona per il progetto?

In questo tutorial si persegue l'obiettivo di supportare il team di sviluppo, in quanto in grado di creare ed estendere un'applicazione software in-house.

Questa attività fornisce le informazioni di configurazione minime per una soluzione correttamente funzionante. Per ulteriori informazioni sui progetti, iniziare con [Ulteriori informazioni sui progetti Cloud Assembly](#).

- 1 Selezionare **Infrastruttura > Amministrazione > Progetti**.

- 2 Fare clic su **Nuovo progetto** e immettere il nome **Development Project**.

- 3 Fare clic sulla scheda **Utenti**, quindi su **Aggiungi utenti**.

Non è necessario aggiungere utenti in questo momento. Tuttavia, se si desidera che altri utenti lavorino con i modelli cloud, questi devono essere membri del progetto.

- 4 Inserire gli indirizzi email per aggiungere utenti come membri del progetto o amministratori, in base alle autorizzazioni che desideri assegnare ai singoli utente.

- 5 Fare clic su **Provisioning** e quindi su **Aggiungi zona > Zona cloud**.

- 6 Aggiungere le zone cloud su cui gli utenti possono eseguire la distribuzione.

È inoltre possibile impostare i limiti delle risorse per la zona cloud nel progetto. In un secondo momento sarà possibile impostare limiti diversi per altri progetti.

Impostazione delle zone cloud del progetto	Valore di esempio
Zona cloud	Zona cloud account vCenter
Priorità di provisioning	1
Limite istanze	5

- 7 Aggiungere eventuali altre zone cloud al progetto.

- 8 Fare clic su **Crea**.

- 9 Per verificare che il progetto sia stato aggiunto alla zona cloud, selezionare **Infrastruttura > Configura > Zone cloud** e aprire la scheda Zona cloud dell'account vCenter in modo da poter esaminare la scheda **Progetti**. Il progetto di sviluppo deve essere visibile.

Passaggio 5: progettare e distribuire un modello cloud di base

Progettare e distribuire il modello cloud per assicurarsi che l'infrastruttura sia configurata correttamente per supportare il modello. In un secondo momento, è possibile creare il modello quando si crea un'applicazione che soddisfa le esigenze del progetto.

Il modo migliore per creare un modello cloud è componente per componente, verificando che venga effettuata la distribuzione dopo ogni modifica. Questo tutorial inizia con una macchina semplice per poi aggiungere iterativamente altre risorse.

Gli esempi di questa procedura utilizzano l'editor di codice YAML. Si tratta di un modo più semplice per fornire all'utente frammenti di codice. Tuttavia, se si preferisce utilizzare un'interfaccia utente basata su finestre di dialogo, fare clic su **Input**.

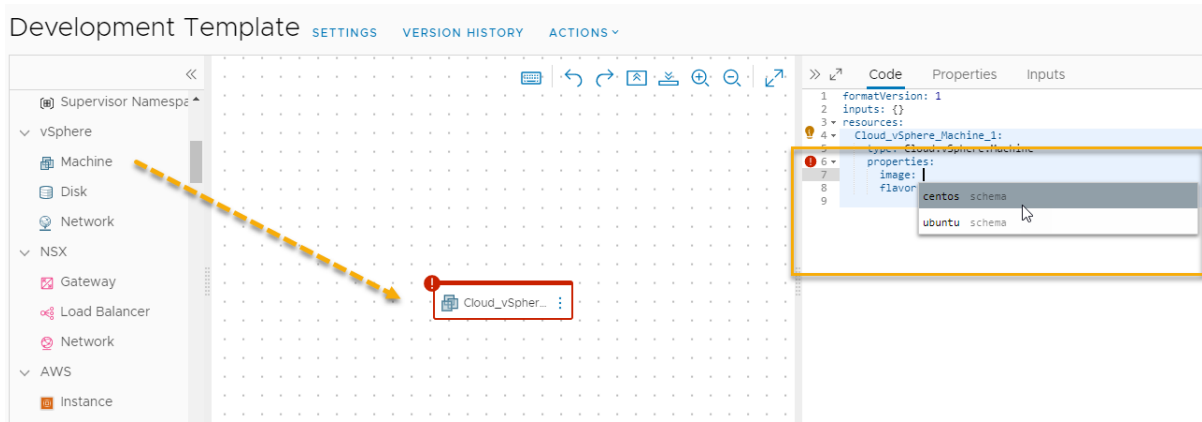
Gli aspetti illustrati in questo tutorial sono solo una parte delle molte possibilità offerte dai modelli cloud. Per ulteriori informazioni, iniziare con [Capitolo 6 Progettazione delle distribuzioni di Cloud Assembly](#).

Questo tutorial utilizza i tipi di risorse di vSphere e NSX. Questi tipi di risorse possono essere distribuiti solo sugli endpoint di account cloud vCenter Server. È inoltre possibile utilizzare i tipi di risorse indipendenti dal cloud per creare modelli cloud che possono essere distribuiti in qualsiasi endpoint. Per un esempio di come configurare l'infrastruttura e progettare il modello per qualsiasi endpoint, vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).



In [Come progettare e distribuire un modello cloud di base](#) è disponibile un video che illustra i passaggi di base di questa procedura.

- 1 Selezionare **Progettazione > Modelli cloud**.
- 2 Selezionare **Nuovo da > Tela vuota**.
- 3 Immettere il **Nome Development Template**, selezionare il **Progetto Development Project** e fare clic su **Crea**.
- 4 Aggiungere una macchina vSphere alla tela di progettazione, verificare e distribuire.



- a Nel riquadro del tipo di risorsa, trascinare una **Macchina vSphere** nella tela.

Si noti che il riquadro **Codice** mostra il codice YAML per la macchina, con un valore vuoto per l'immagine e proprietà di CPU e memoria predefinite. Si sta per rendere questo modello in grado di supportare il dimensionamento flessibile.

- b Per selezionare un valore di immagine, posizionare il puntatore tra gli apici per `image` e selezionare **centos** dall'elenco delle immagini configurate.

Si ricorda che i valori sono puramente esemplificativi. Se non è stata configurata un'immagine centos, selezionare un'immagine che è stata configurata.

- c Creare una riga sotto la proprietà dell'immagine e immettere o selezionare `flavor`, quindi selezionare `small` nell'elenco.

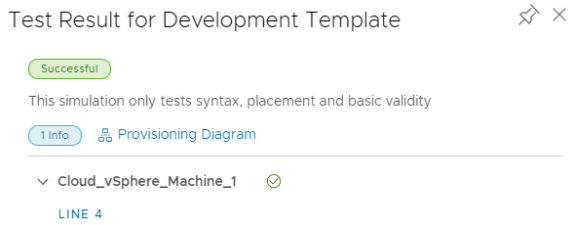
- d Eliminare `cpuCount` e `totalMemory`.

Il codice YAML dovrebbe essere simile a questo esempio.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
```

- e Fare clic su **Test**.

Il test consente di convalidare la sintassi e il posizionamento del modello cloud. Un test terminato con esito positivo non significa che sia possibile distribuire il modello senza errori.



Se il test non riesce, fare clic su **Diagramma di provisioning** e cercare i punti di errore. Per ulteriori informazioni sull'utilizzo del diagramma a scopo di risoluzione dei problemi, vedere [Test di un modello cloud di base](#).

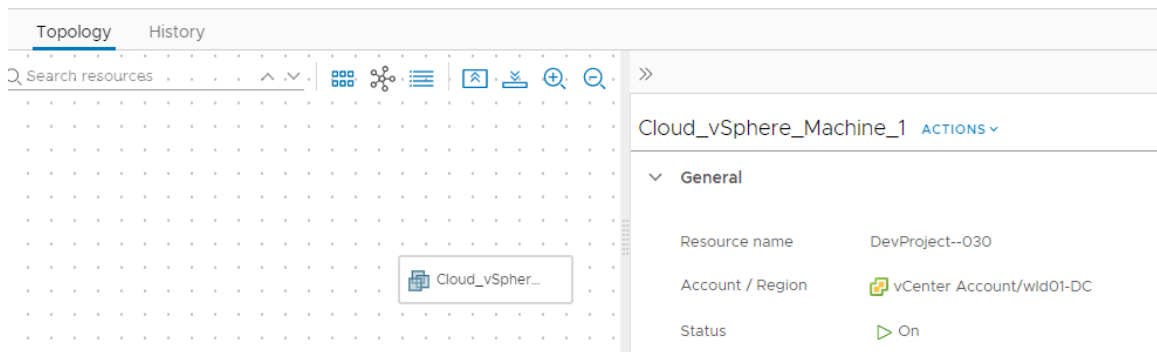
f Fare clic su **Distribuisci**.

g Immettere **DevTemplate-machine** in **Nome distribuzione** e fare clic su **Distribuisci**.

È possibile monitorare lo stato di avanzamento della distribuzione nella pagina dei dettagli della distribuzione DevTemplate o nella pagina Distribuzioni. Selezionare **Risorse > Distribuzioni**.

Se la distribuzione non riesce, è possibile risolvere il problema e rivedere il modello. Vedere [Che cosa è possibile fare se una distribuzione Cloud Assembly non riesce](#).

Una distribuzione corretta ha un aspetto simile a questo esempio nella pagina Distribuzioni.



5 Assegnare una versione al modello e aggiungere una rete.

L'assegnazione della versione a un modello cloud è necessaria per renderlo disponibile nel catalogo Service Broker, ma è utile disporre di una versione funzionante per poterla ripristinare durante lo sviluppo.

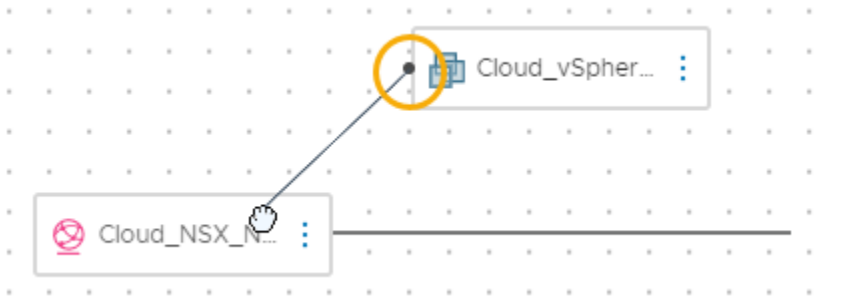
a Aprire il modello nella tela di progettazione.

b Fare clic su **Versione**, inserire una **Descrizione** come ad esempio **Macchina semplice distribuibile** e fare clic su **Crea**.

c Dal riquadro tipo di risorsa, trascinare un tipo di risorsa **Rete NSX** nella tela.

d Connettere la macchina alla rete.

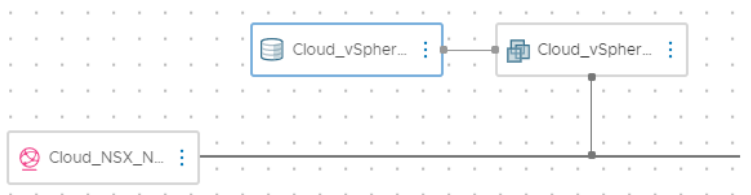
Fare clic sul cerchio piccolo nel componente macchina e trascinare la connessione nella rete.



Si noti che il codice YAML ora assomiglia a questo esempio.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks: []
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Fare clic su **Test** per convalidare il modello.
 - f Fare clic su **Distribuisci**.
 - g Immettere il nome **DevTemplate - machine - network** e fare clic su **Distribuisci**.
 - h Monitorare lo stato di avanzamento e rivedere la distribuzione corretta.
- 6 Assegnare una versione al modello e aggiungere un disco dati.
- a Aprire il modello nella tela di progettazione.
 - b Assegnare una versione al modello.
- Inserire la descrizione **Machine with existing network**.
- c Dal riquadro tipo di risorsa, trascinare un tipo di risorsa **Disco vSphere** nella tela.
 - d Connettere il disco alla macchina.



Si noti che il codice YAML ora assomiglia a questo esempio.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- e Testare il modello.
- f Distribuire il modello utilizzando il nome **DevTemplate - machine - network - storage**.
- g Monitorare lo stato di avanzamento e rivedere la distribuzione corretta.
- h Assegnare una versione al modello.

Inserire la descrizione **Machine with existing network and storage disk**.

Questa versione finale assicura che sia possibile aggiungere un modello funzionante al catalogo dei servizi.

Risultati del tutorial

È stato completato il workflow che ha configurato Cloud Assembly come sistema funzionante. Si è ottenuta quindi la conoscenza dei seguenti concetti.

- Gli account cloud sono le credenziali che connettono Cloud Assembly agli endpoint del fornitore della soluzione cloud.
- Le zone cloud sono le risorse di elaborazione selezionate in account/regioni che successivamente si assegnano a progetti diversi in base alle esigenze dei progetti e agli obiettivi per la gestione dei costi.
- Le risorse dell'infrastruttura sono definizioni delle risorse associate ad account/regioni utilizzati nei modelli cloud.

- I progetti sono le modalità utilizzate per concedere agli utenti l'accesso alle zone cloud in base agli obiettivi di sviluppo delle applicazioni del progetto.
- I modelli cloud sono le definizioni dei carichi di lavoro delle applicazioni che è possibile sviluppare e distribuire in modo iterativo.

Questo tutorial rappresenta la base dell'esperienza di sviluppo con Cloud Assembly. È possibile utilizzare questo processo per creare la propria infrastruttura e acquisire competenze di sviluppo di modelli cloud.

Tutorial: configurazione di Cloud Assembly per il provisioning di un carico di lavoro di produzione

In qualità di amministratore del cloud, si desidera automatizzare il processo di distribuzione per un progetto in modo che quando i progettisti dei modelli cloud creano e distribuiscono i modelli, Cloud Assembly esegua il lavoro automaticamente. Ad esempio, i carichi di lavoro vengono distribuiti con un determinato modello di denominazione della macchina personalizzato, le macchine vengono aggiunte a una specifica unità organizzativa di Active Directory e vengono utilizzati intervalli di IP e DNS specifici.

Automatizzando il processo per le distribuzioni del progetto, è possibile gestire più facilmente più progetti in diversi data center e ambienti cloud.

Non è necessario completare tutte le attività fornite qui. È possibile abbinare le attività nel modo desiderato, in base ai propri obiettivi di gestione.

Prima di iniziare

In questo tutorial è necessario configurare l'infrastruttura e distribuire correttamente un modello cloud con una macchina e una rete. Verificare che nel sistema siano già stati configurati i seguenti elementi.

- Tutti i passaggi specificati nel tutorial sull'infrastruttura sono stati eseguiti correttamente. Vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni di vSphere in Cloud Assembly](#).
- Si dispone del ruolo di amministratore di Cloud Assembly. Vedere [Ruoli utente di organizzazione e servizio in vRealize Automation](#).

Personalizzazione dei nomi delle macchine

L'obiettivo di questa attività consiste nel garantire che le macchine distribuite per il progetto Development Project siano denominate in base al centro di costo del progetto, al tipo di risorsa selezionato al momento della distribuzione e a numeri incrementali per garantire l'unicità. Ad esempio, DevProject-centos-021.

È possibile adattare questo esempio ai propri requisiti di denominazione.

Per ulteriori informazioni sui progetti, vedere [Capitolo 5 Aggiunta e gestione di progetti di Cloud Assembly](#).



In [Come creare un modello di denominazione personalizzata per le distribuzioni](#) è disponibile un video che illustra questo esempio di denominazione personalizzata.

- 1 Selezionare **Infrastruttura > Progetti**.
- 2 Selezionare un progetto esistente o crearne uno nuovo.
Per questo tutorial, il nome del progetto è Development Project.
- 3 Fare clic su **Crea**.
- 4 Nella pagina Progetti, fare clic sul nome del progetto nel riquadro in modo che sia possibile configurarlo.
- 5 Fare clic sulla scheda **Utenti** e aggiungere gli utenti membri di questo progetto.
- 6 Fare clic sulla scheda **Provisioning**.
 - a Nella sezione Zone, fare clic su **Aggiungi zona** e aggiungere le zone cloud possibili in cui vengono distribuiti i carichi di lavoro per questo progetto.
 - b Nella sezione Proprietà personalizzate, aggiungere una proprietà personalizzata con nome **costCenter** e valore **DevProject**.

Name	Value	Encrypted
costCenter	DevProject	<input type="checkbox"/>

Custom Naming

Specify the naming template to be used for machines, networks, security groups and disks provisioned in this project.

Template: ⓘ

Hint: Avoid conflicting names by generating digits in names. \${#####}

- c Nella sezione Denominazione personalizzata, aggiungere il seguente modello di denominazione.

```
$(resource.costCenter)-$(resource.installedOS)-${###}
```

`$(resource.installedOS)` si basa sul sistema operativo selezionato quando si distribuisce il modello cloud.

- 7 Fare clic su **Salva**.
- 8 Aggiornare il modello cloud con un valore di input per il tipo di sistema operativo.

I valori di input rappresentano il modo diretto per personalizzare il modulo di richiesta della distribuzione per gli utenti e semplificare il processo di sviluppo. Creando i valori di input, è possibile utilizzare un singolo modello cloud per distribuire i carichi di lavoro con configurazioni diverse. Ad esempio, dimensione o sistema operativo.

In questo esempio viene utilizzato il modello Development Template creato in un tutorial precedente. Vedere [Passaggio 5: progettare e distribuire un modello cloud di base](#).

- a Selezionare **Progettazione** e aprire il modello Development Template.

- b Nel riquadro Codice, aggiornare il codice YAML con le seguenti modifiche.

- Nella sezione `Inputs`, aggiungere `installedOS`.

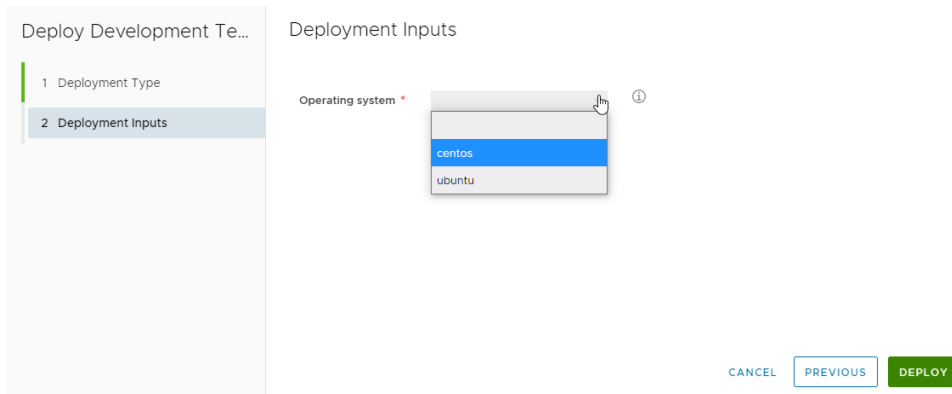
Nel passaggio successivo è possibile vedere che l'input `installedOS` viene utilizzato anche per specificare l'immagine. Quando si aggiungono le stringhe nella sezione `enum`, i valori in questo esempio sono `centos` e `ubuntu`, e devono corrispondere ai nomi delle immagini definiti in **Infrastruttura > Configura > Mappature immagini**. Ad esempio, se il nome della mappatura immagine è CentOS anziché centos, è consigliabile utilizzare CentOS nella sezione degli input.

```
inputs:
  installedOS:
    type: string
    title: OS Type
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
```

- Nella sezione `Cloud_vSphere_Machine_1`, aggiornare `image` a un parametro di input `installedOS` (`${input.installedOS}`) e aggiungere una proprietà personalizzata `installedOS` con lo stesso parametro di input.

```
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ${input.installedOS}
      installedOS: ${input.installedOS}
      flavor: small
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

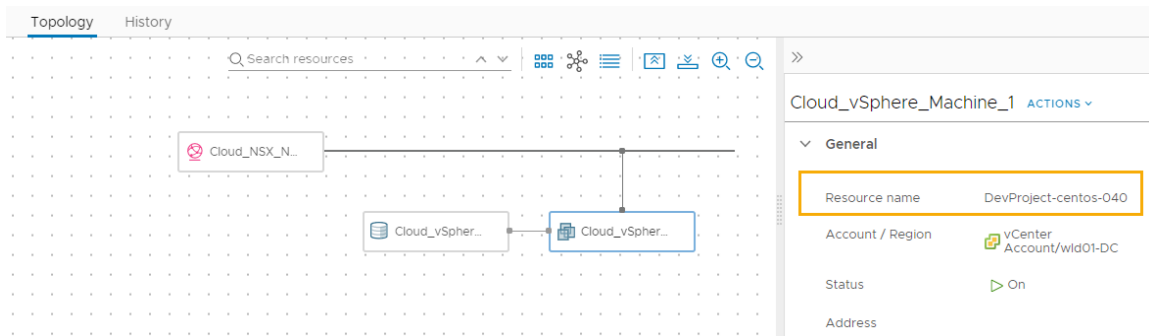
- c Fare clic su **Distribuisce** e immettere il nome **Custom name deployment test**.
- d Fare clic su **Avanti**.
- e Selezionare il sistema operativo **centos** dal menu a discesa.



f Fare clic su **Distribuisci**.

9 Monitorare lo stato di avanzamento e rivedere la distribuzione corretta.

Il nome della macchina in questo esempio è DevProject-centos-026. È importante ricordare che questo esempio si basa sul tutorial a cui si fa riferimento all'inizio di questa attività.



Creazione di record macchina di Active Directory

Quando si esegue il provisioning di un carico di lavoro, è possibile creare record macchina in Active Directory. Configurando Cloud Assembly in modo che esegua automaticamente questa attività per le distribuzioni di un progetto è possibile alleggerire il proprio carico di lavoro di amministratore del cloud.

1 Aggiungere un'integrazione di Active Directory.

a Selezionare **Infrastruttura > Connessioni > Integrazioni**.

Questi passaggi illustrano la configurazione di Active Directory di base in relazione ai record macchina di AD di questo esempio. Per ulteriori informazioni sull'integrazione di Active Directory, vedere [Come creare un'integrazione di Active Directory in Cloud Assembly](#).

b Fare clic su **Aggiungi integrazione** e quindi su **Active Directory**.

c Immettere il nome utilizzato per questa integrazione.

d Immettere **Host/IP LDAP** e le credenziali associate.

e Immettere il **DN di base**.

In questo tutorial l'esempio è **ou=AppDev,dc=cmbu,dc=local**. AppDev è l'unità organizzativa principale per l'unità organizzativa del computer che verrà aggiunta per il progetto.

f Fare clic su **Aggiungi**.

2 Aggiungere il progetto all'integrazione.

3 Nell'integrazione di Active Directory, fare clic sulla scheda **Progetti** e quindi su **Aggiungi progetto**.

Add Projects

Select a project and the OU it will be mapped to by adding its relative DN. The effective DN is created by appending the RDN to the integration base DN (**dc=cmbu,dc=local**).

CANCEL ADD

a Selezionare il progetto App Development.

b Immettere i DN relativi. Ad esempio **OU=AppDev-Computers**.

c Lasciare disattivati gli interruttori **Sostituisce** e **Ignora**.

Questa procedura è incentrata sull'automazione del processo per un progetto. Non vengono trattate le personalizzazioni che è possibile eseguire nei modelli.

d Fare clic su **Aggiungi**.

4 Per salvare le modifiche apportate all'integrazione, fare clic su **Salva**.

5 Distribuire un modello cloud per il progetto e verificare che la macchina sia stata aggiunta all'unità organizzativa di Active Directory corretta.

Impostazione del DNS di rete e dell'intervallo di IP interni

Aggiungere o aggiornare un profilo di rete per includere i server DNS e gli intervalli di indirizzi IP interni.

È necessario aver già creato un account cloud per vSphere, NSX-V o NSX-T. Vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni di vSphere in Cloud Assembly](#) o [Aggiunta di account cloud a Cloud Assembly](#).

1 Selezionare **Infrastruttura > Configura > Profili di rete**.

2 Selezionare un profilo esistente o crearne uno.

3 Nella scheda **Riepilogo**, selezionare **Account/Regione** e immettere un nome.

Per questo tutorial, il nome del profilo di rete è Network Profile.

4 Aggiungere le reti.

a Fare clic sulla scheda **Reti**.

b Fare clic su **Aggiungi rete**.

c Aggiungere una o più reti NSX o vSphere.

d Fare clic su **Aggiungi**.

5 Configurare i server DNS.

a Nell'elenco di reti della scheda **Reti**, fare clic sul nome della rete.

Summary Networks Network Policies Load Balancers Security					
Networks listed here are used when provisioning to existing, on-demand, or p					
+ ADD NETWORK TAGS MANAGE IP RANGES X REMOVE					
<input type="checkbox"/>	Name ↑	Account / Region	Zone	Network Domain	CIDR
<input type="checkbox"/>	DevProject--004	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.64 /27

- b Immettere gli indirizzi IP del server DNS che si desidera utilizzare per questa rete.

DevProject--004

DNS servers

192.168.1.22
192.168.1.23

DNS search domains

company.local

DNS Servers

Use a comma separated list or new lines.

- c Fare clic su **Salva**.

- 6 Specificare l'intervallo di indirizzi IP per la rete.

- a Nell'elenco delle reti, selezionare la casella di controllo accanto al nome della rete.

Network Profile [DELETE](#)

Summary **Networks** Network Policies Load Balancers Security Groups

Networks listed here are used when provisioning to existing, on-demand, or public networks. ⓘ

[+ ADD NETWORK](#)
[TAGS](#)
[MANAGE IP RANGES](#)
[REMOVE](#)

<input type="checkbox"/>	Name	Account / Region	Zone	Network Domain	CIDR	Su Pu
<input type="checkbox"/>	External-mcm1343745-148168716643	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	172.16.12.64/28	
<input type="checkbox"/>	NSX-mcm1376447-151082888186	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.100.32/28	
<input checked="" type="checkbox"/>	NSX-mcm39835-146434698964	NSX-T Account		overlay-tz-sc2vc05-vip-nsx-mgmt.cmbu.local	192.168.1.0/27	

1

- b Fare clic su **Gestisci intervalli IP**.
- c Nella finestra di dialogo Gestisci intervalli IP, fare clic su **Nuovo intervallo IP**.

New IP Range

Network * NSX-mcm1376447-151082888186

Source ☒ Internal ☐ External

Name * DevProject Range

Description

CIDR 192.168.100.32/28

Start IP address * 192.168.100.34

End IP address * 192.168.100.46

- d Immettere un nome.

Ad esempio, **DevProject Range**.

- e Per definire l'intervallo, immettere **Indirizzo IP iniziale** e **Indirizzo IP finale**.
 - f Fare clic su **Aggiungi**.
 - g Aggiungere ulteriori intervalli o fare clic su **Chiudi**.
- 7 Aggiungere la zona cloud contenente la regione o l'account di rete associato che è stato configurato per Development Project.
 - 8 Distribuire un modello cloud per il progetto e verificare che venga eseguito il provisioning della macchina entro l'intervallo di IP specificato.

Tutorial: utilizzo dei tag in Cloud Assembly per gestire le risorse di vSphere

I tag sono metadati avanzati che è possibile associare alle risorse e includere nei modelli. È possibile utilizzare i tag in diversi scenari di gestione, incluso il posizionamento dei carichi di lavoro e le etichette delle risorse.

Introduzione rapida ai tag

Questa sezione è una semplice introduzione ai tag applicati alle procedure indicate. Per informazioni più dettagliate sui tag, vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#).

■ Tag di funzionalità e vincolo

È possibile utilizzare i tag per controllare le distribuzioni in base alle funzionalità delle risorse. Ad esempio, nel caso in cui un amministratore del cloud desideri che i modelli cloud sviluppati iterativamente vengano distribuiti a un pool di risorse specifico per lo sviluppo e i modelli disponibili per la produzione vengano distribuiti a un altro pool di risorse.

- I tag di funzionalità vengono aggiunti alle risorse, definendo le relative funzionalità.
- I tag di vincolo vengono utilizzati nei modelli cloud, definendo le risorse che si desidera utilizzare con le risorse distribuite.

■ Tag di etichette

Per gestire le risorse, è possibile aggiungere tag come etichette o descrizioni di oggetti. Le possibilità di gestione includono risultati di ricerca delle risorse migliori, differenziazione tra oggetti simili, annotazione di oggetti con informazioni personalizzate, indicazione di informazioni a sistemi di terzi, creazione di criteri di appartenenza al raggruppamento di sicurezza, verifica della coerenza tra i domini SDDC collegati.

Prima di iniziare

- Rivedere le risorse e il modello cloud definiti in [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni di vSphere in Cloud Assembly](#). Qui vengono utilizzati i valori di esempio utilizzati in tale tutorial.

Utilizzo dei tag per gestire il posizionamento dei carichi di lavoro

Questo semplice esempio utilizza tag dell'ambiente di sviluppo e produzione per mostrare come utilizzare i tag di funzionalità e vincolo. Prima di tutto, si aggiungono tag di funzionalità nelle risorse di elaborazione del pool di risorse di vCenter Server e quindi si includono i tag nel modello cloud. L'esempio di modello cloud mostra come utilizzare gli input per consentire all'utente che esegue la distribuzione di scegliere se distribuirlo in un pool di risorse di sviluppo o di produzione.

Per un esempio di come utilizzare gli stessi tag per definire il posizionamento in un ambiente multi-cloud, vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).

- 1 Aggiungere i tag di funzionalità ai pool di risorse.
 - a Selezionare **Infrastruttura > Risorse > Elaborazione**.
 - b Aprire la zona cloud e fare clic su **Elaborazione**.



- c Individuare e fare clic sul pool di risorse in cui si desidera distribuire i carichi di lavoro di sviluppo.

In questo tutorial vengono utilizzati i seguenti valori di esempio. Tenere presente che questi valori sono solo esempi. I valori saranno quelli specifici del proprio ambiente.

Pool di risorse di esempio	Tag di esempio
wid01-clu01 / Development	env:dev
wid01-clu01 / Production	env:prod

- d Aggiungere il tag **env.dev** e fare clic **Salva**.

wld01-clu01 / Development

Account / region vCenter Account / wld01-DC

Name wld01-clu01 / Development

Type VM_HOST

Tags env:dev X Enter a new tag

SAVE **CANCEL**

- e Ripetere il processo per il pool di risorse in cui si desidera distribuire i carichi di lavoro di produzione e aggiungere il tag **env:prod**.
- 2 Verificare che i tag di funzionalità siano stati aggiunti ai pool di risorse nella zona cloud.
 - a Selezionare **Infrastruttura > Configura > Zone cloud**.
 - b Aprire la zona cloud associata al progetto e fare clic su **Elaborazione**.

In questo esempio, la zona cloud è Zona cloud account vCenter e i tag sono stati aggiunti ai due pool di risorse, wld01-clu01 / Development e wld01-clu01 / Production.

vCenter Account Cloud Zone DELETE

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Include all compute

Name	Account / Region	Type	Tags
10.176.152.27	vCenter Account / wld01-DC	Host	
wld01-clu01	vCenter Account / wld01-DC	Supervisor Cluster	
wld01-clu01 / Development	vCenter Account / wld01-DC	Resource Pool	env:dev
wld01-clu01 / Production	vCenter Account / wld01-DC	Resource Pool	env:prod
wld01-clu01 / Training-Org	vCenter Account / wld01-DC	Resource Pool	
wld01-clu01 / VCF-edge_edge-wldclu-01_ResourcePool_ffa14b18-82b5-4261-b546-aef86a1db2d9	vCenter Account / wld01-DC	Resource Pool	

- 3 Aggiungere tag di vincolo al modello cloud.

I tag di vincolo vengono utilizzati per limitare la posizione di distribuzione del modello.

- a Selezionare **Progettazione > Modelli cloud** e quindi aprire il modello.
In questo tutorial, il nome del modello è Development Template.
- b Rivedere il codice YAML per il modello nel riquadro Codice.

Il punto di partenza di questa tutorial è il codice YAML.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: medium
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 5
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- c Aggiungere il tag di vincolo alla risorsa Cloud_vSphere_Machine_1 utilizzando `${input.placement}` come variabile.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: medium
      constraints:
        - tag: '${input.placement}'
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
```

- d Definire la variabile di posizionamento nella sezione Input.

```
inputs:
  placement:
    type: string
    enum:
      - env:dev
      - env:prod
    default: env:dev
    title: Select Placement for Deployment
    description: Target Environment
```

- e Verificare che il codice YAML finale sia simile a quello illustrato nell'esempio seguente.

```
formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      constraints:
        - tag: '${input.placement}'
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 5
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
```

- f Per provare la variabile del tag in base alle risorse disponibili, fare clic su **Test**, quindi selezionare **env:dev**.

Testing Development Template

Select Placement for Deployment env:dev ⓘ

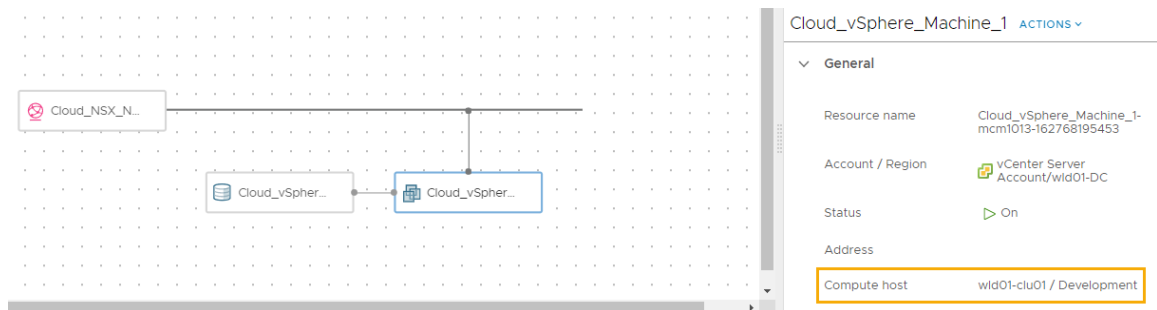
CANCEL TEST

Ripetere il test utilizzando **env:prod**. Quando entrambi i test hanno esito positivo, verificare che il modello funzioni distribuendolo.

- 4 Distribuire il modello per testare il posizionamento dei carichi di lavoro.
 - a Nel progettista del modello cloud, fare clic **Distribuisci**.
 - b Immettere **Deployment Tag Dev** come **Nome della distribuzione** e fare clic su **Avanti**.

- c Selezionare **env:dev** nel menu a discesa **Seleziona posizionamento per la distribuzione** e fare clic su **Distribuisci**.
- 5 Verificare che il modello abbia distribuito le risorse al pool di risorse selezionato.
 - a Selezionare **Risorse > Distribuzioni** e individuare la distribuzione Deployment Tag Dev.
 - b Aprire i dettagli della distribuzione e fare clic **Topologia**.
 - c Fare clic sulla macchina vSphere ed espandere le informazioni della macchina nel riquadro a destra.
 - d Nella sezione **Generale**, individuare **Host di elaborazione** e verificare che il valore corrisponda al pool di risorse corrispondente al tag env:dev.

In questo esempio, il valore è `wid01-clu01 / Development`, a indicare che il carico di lavoro è stato distribuito nel pool di risorse corretto in base al tag di vincolo selezionato.



- e Ripetere il processo di distribuzione, questa volta selezionando **env:prod**.

Aggiunta di tag come etichette che è possibile utilizzare in vCenter Server e NSX-T

È possibile aggiungere tag alle distribuzioni che possono essere utilizzate per gestire le risorse.

In questo esempio, si aggiungono tag per identificare la macchina e la rete MySQL. Aggiungere inoltre un tag per identificare la rete Web. A causa del funzionamento dei tag nelle reti esistenti rispetto alle reti su richiesta, sono disponibili due opzioni.

- Se si utilizza il profilo di rete esistente utilizzato nella sezione precedente, il tag NGINX:web non viene aggiunto agli oggetti esistenti in NSX-T. In questo modo, è possibile ignorare i passaggi di verifica relativi a questo tag in NSX-T.
- Se si crea un profilo di rete su richiesta, è possibile aggiornare la rete nel codice YAML in modo da utilizzare la rete instradata/su richiesta. La rete su richiesta viene utilizzata in questo esempio in modo da poter mostrare il tag NGINX:web nel nuovo oggetto in NSX-T.

Il seguente codice YAML deriva dall'esempio precedente, ad eccezione del fatto che utilizza un `networkType` su richiesta instradato. Include i tag di vincolo.

In questo tutorial vengono utilizzati i seguenti valori di esempio. Tenere presente che questi valori sono solo esempi. I valori saranno quelli specifici del proprio ambiente.

```
formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      constraints:
        - tag: '${input.placement}'
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 5
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: routed
      constraints:
        - tag: 'net:od'
```

- 1 Selezionare **Progettazione > Modelli cloud** e quindi aprire il modello.
- 2 Nelle proprietà Cloud_vSphere_Machine_, aggiungere il seguente tag.

```
tags:
  - key: db
    value: mysql
```

- 3 Aggiungere i tag della scheda NIC della macchina virtuale.

```
tags:
  - key: db
    value: mysql
```


4 Aggiungere i tag di segmento/switch logico di NSX.

```
tags:
- key: NGINX
  value: web
```

5 Verificare che il codice YAML sia simile a quello illustrato nell'esempio seguente.

```
formatVersion: 1
inputs:
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
    description: Target Environment
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      flavor: small
      constraints:
        - tag: '${input.placement}'
      tags:
        - key: db
          value: mysql
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
        tags:
          - key: db
            value: mysql
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 5
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: routed
      constraints:
        - tag: 'net:od'
      tags:
        - key: NGINX
          value: web
```

6 Distribuire il modello.

In questo esempio viene utilizzato il nome **Development template w tags**.

7 Per verificare i tag nella distribuzione, aprire la distribuzione e fare clic sulla scheda **Topologia**.

a Fare clic sulla macchina nella topologia.

b Espandere la sezione **Generale** per la macchina e individuare l'etichetta Tag.

Il valore del tag è `db:mysql`.

c Espandere la sezione **Rete** e individuare la colonna Tag di rete.

Il valore del tag è `db:mysql`.

Development template w tags Create Successful ACTIONS | 🔄

No description

Owner	fritz	Expires on	Never
Requestor	fritz	Last updated	Mar 8, 2021, 4:31:01 PM
Project	Development Project	Created on	Mar 8, 2021, 4:09:14 PM
Cloud Template	Development Template ↓		

HIDE SUMMARY [⌵](#)

Topology History

Search resources

Cloud_NSX_N...

Cloud_vSphere...

Cloud_vSphere_Machine_1 ACTIONS

General

Resource name Cloud_vSphere_Machine_1-mcm1019-163638575175

Account / Region vCenter Server Account/wld01-DC

Status On

Address

Compute host wld01-clu01 / Development

Tags db:mysql

Storage

Network

Index	Name	Address	Assignment Type	Security Groups	Tags
0	DevProject--004		dynamic		db:mysql

Custom properties

d Fare clic sulla rete nella topologia ed espandere la sezione **Generale** per individuare l'etichetta Tag.

Il valore del tag è `NGINX:web`.

Topology History

Search resources

Cloud_NSX_N...

Cloud_vSphere...

Cloud_NSX_Network_1 ACTIONS

General

Resource name Cloud_NSX_Network_1-mcm1292-163799928607

Account NSX-T Account

Network type routed

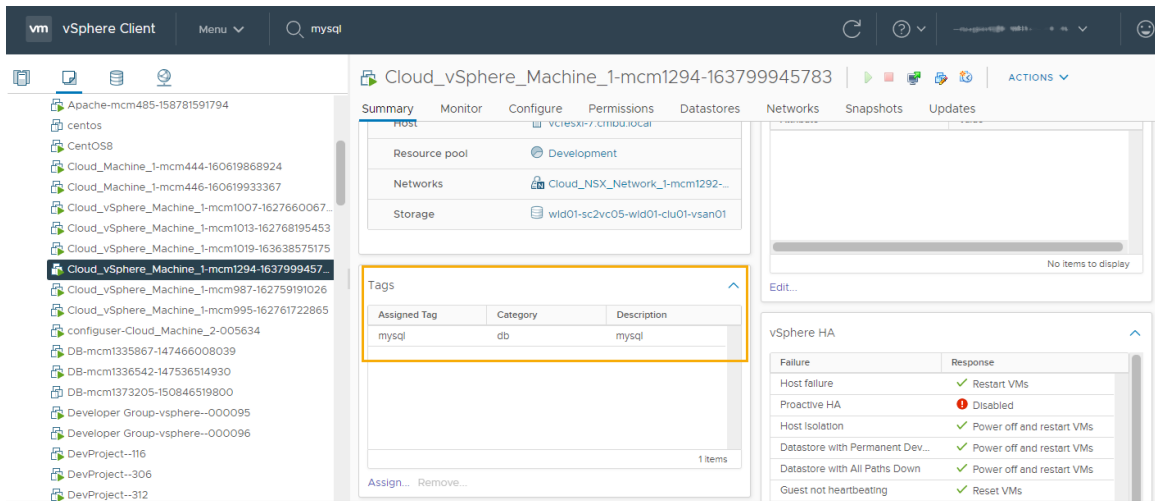
CIDR 192.168.150.0/28

Tags nginx:web

Custom properties

8 Per verificare i tag in vCenter Server, accedere all'istanza vCenter Server in cui è stato distribuito questo carico di lavoro.

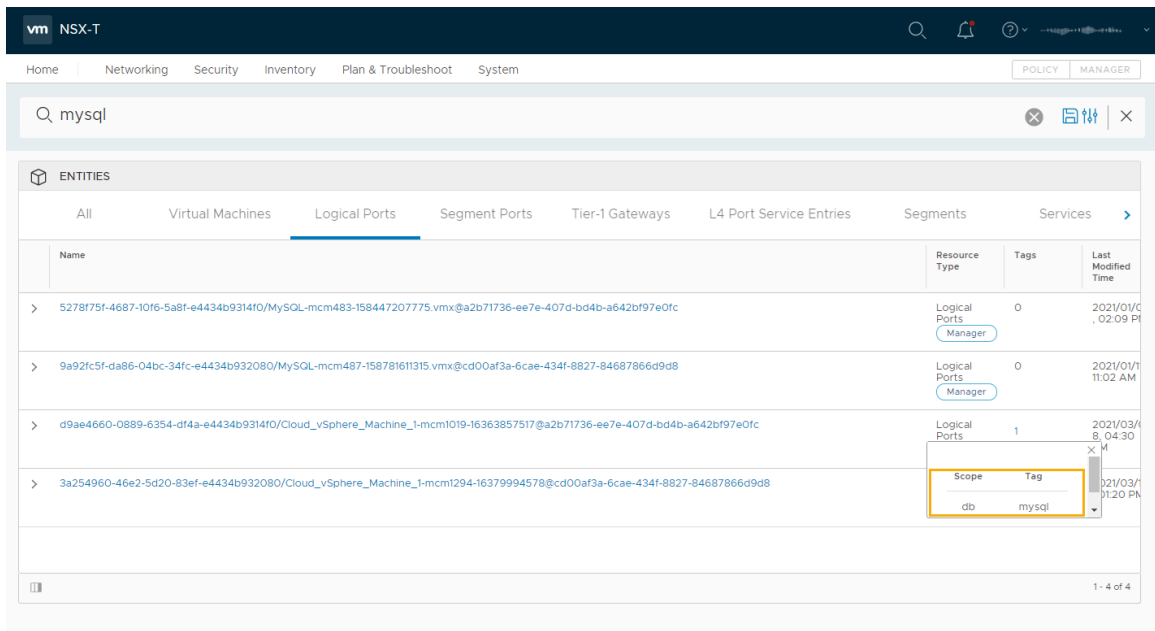
a Individuare la macchina virtuale e individuare il riquadro Tag.



9 Per verificare i tag in NSX-T, accedere all'istanza NSX-T in cui è configurata la rete.

- Fare clic su **Criterio** nell'angolo superiore destro.
- Per individuare il tag `db:mysql` associato alla scheda NIC, cercare **mysql**.
- Fare clic **Porte logiche** e individuare la macchina vSphere distribuita.
- Fare clic sul numero nella colonna Tag.

L'ambito e il tag sono, rispettivamente, `db` e `mysql`.

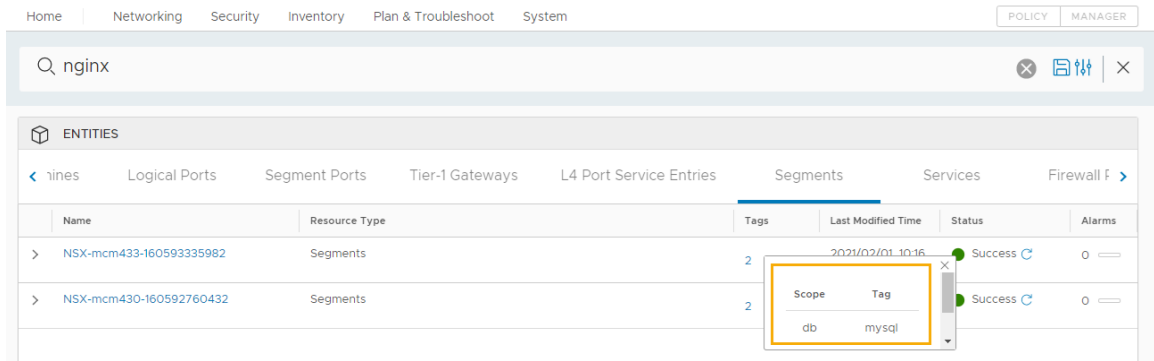


- Per individuare il tag `NGINX:web` associato al segmento, cercare la rete.

In questo esempio, il nome della rete è **Cloud_NSX_Network_1-mcm1292-163799928607**.

- Individuare la riga Segmenti e fare clic sul numero nella colonna Tag.

L'ambito e il tag sono, rispettivamente, `NGINX` e `web`.



Tutorial: aggiunta di un modello cloud di Cloud Assembly al catalogo di Service Broker con un modulo di richiesta personalizzato

Durante lo sviluppo iterativo dei modelli cloud o quando si dispone di un modello finale, è possibile rendere i modelli disponibili per i clienti nel catalogo self-service di Service Broker. Per migliorare ulteriormente l'esperienza utente, è possibile creare un modulo di richiesta personalizzato. Il modulo personalizzato è più avanzato delle semplici opzioni di input del modello.

Operazioni preliminari

- Verificare di disporre dell'infrastruttura che supporti il modello. In caso contrario, iniziare con [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni di vSphere in Cloud Assembly](#) e continuare con gli altri tutorial.
- Verificare di aver contrassegnato alcuni pool di risorse come `env:dev` e `env:prod`. Per ulteriori informazioni, vedere [Tutorial: utilizzo dei tag in Cloud Assembly per gestire le risorse di vSphere](#).
- Assicurarsi di disporre di un modello cloud distribuibile, simile al seguente. Questo tutorial inizia con il modello seguente.

```
formatVersion: 1
inputs:
  installedOS:
    type: string
    title: Operating System
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
  placement:
    type: string
    enum:
      - 'env:dev'
      - 'env:prod'
    default: 'env:dev'
    title: Select Placement for Deployment
```

```

description: Target Environment
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: '${input.installedOS}'
      installedOS: '${input.installedOS}'
      flavor: small
    constraints:
      - tag: '${input.placement}'
    tags:
      - key: db
        value: mysql
    networks:
      - network: '${resource.Cloud_NSX_Network_1.id}'
        tags:
          - key: db
            value: mysql
    attachedDisks:
      - source: '${resource.Cloud_vSphere_Disk_1.id}'
  Cloud_NSX_Network_1:
    type: Cloud.NSX.Network
    properties:
      networkType: existing
    tags:
      - key: NGINX
        value: web

```

Passaggio 1: aggiunta di input al modello cloud

Oltre all'input del tipo di sistema operativo esistente, questa procedura aggiorna l'input placement e aggiunge un input size. Quando si personalizza il modulo di richiesta in Service Broker, questi sono i tre campi del modulo di richiesta che vengono personalizzati.

- 1 In Cloud Assembly, selezionare **Progettazione > Modello cloud** e creare o aprire il modello specificato in precedenza.

Il modello di esempio viene utilizzato per spiegare le diverse opzioni e include valori di esempio. Adattarlo al proprio ambiente.

- 2 Aggiungere la variabile size e definire le dimensioni nella sezione Input.

- a Nella sezione Cloud_vSphere_Machine_1, aggiungere una variabile alla proprietà `flavor`.

```
flavor: '${input.size}'
```

- b Nella sezione Input, aggiungere un input utente denominato `size` in modo che l'utente possa selezionare le dimensioni della distribuzione. In alcuni casi, è denominato anche `t-shirt size` e viene definito per le zone cloud.

```
size:
  type: string
  title: Deployment size
  description: Select the the deployment t-shirt size.
  enum:
    - small
    - medium
    - large
```

- 3 Aggiornare gli input di posizionamento con un termine descrittivo anziché le stringhe di tag.

Questi tag di vincolo verranno associati ai tag di funzionalità aggiunti in [Tutorial: utilizzo dei tag in Cloud Assembly per gestire le risorse di vSphere](#).

- a Nella sezione Input, aggiungere un input utente denominato **placement** in modo che l'utente possa selezionare sviluppo o produzione come posizionamento della distribuzione.

In questo esempio, viene utilizzato l'attributo `oneOf`, che consente di presentare un'etichetta di linguaggio naturale continuando a inviare le stringhe necessarie per il processo di distribuzione. Ad esempio, i tag `env:dev` e `env:prod`.

```
placement:
  type: string
  oneOf:
    - title: Development
      const: 'env:dev'
    - title: Production
      const: 'env:prod'
  default: 'env:dev'
  title: Select Deployment Placement
  description: Target Environment
```

- 4 Rivedere il codice YAML completo per assicurarsi che sia simile a quello illustrato nell'esempio seguente.

```
formatVersion: 1
inputs:
  installedOS:
    type: string
    title: Operating system
    description: Select the operating system.
    enum:
      - centos
      - ubuntu
  placement:
    type: string
    oneOf:
```

```

    - title: Development
      const: 'env:dev'
    - title: Production
      const: 'env:prod'
  default: 'env:dev'
  title: Select Deployment Placement
  description: Target Environment
  size:
    type: string
    title: Deployment size
    description: Select the the deployment t-shirt size.
    enum:
      - small
      - medium
      - large
  resources:
    Cloud_vSphere_Disk_1:
      type: Cloud.vSphere.Disk
      properties:
        capacityGb: 1
    Cloud_vSphere_Machine_1:
      type: Cloud.vSphere.Machine
      properties:
        image: '${input.installedOS}'
        installedOS: '${input.installedOS}'
        flavor: '${input.size}'
      constraints:
        - tag: '${input.placement}'
      tags:
        - key: db
          value: mysql
      networks:
        - network: '${resource.Cloud_NSX_Network_1.id}'
          tags:
            - key: db
              value: mysql
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
    Cloud_NSX_Network_1:
      type: Cloud.NSX.Network
      properties:
        networkType: existing
      tags:
        - key: NGINX
          value: web

```

- 5 Fare clic su **Distribuisci** e verificare che la seconda pagina della richiesta sia simile all'esempio seguente. È quindi possibile verificare che la distribuzione si trovi nello sviluppo selezionato del pool di risorse di produzione dopo la distribuzione.

Deploy Development Te...

1 Deployment Type

2 Deployment Inputs

Operating system * centos ⓘ

Select Deployment Placement Development ⓘ

Deployment size * small ⓘ

CANCEL PREVIOUS DEPLOY

Passaggio 2: controllo della versione e rilascio del modello cloud

Quando si dispone di un modello distribuibile, è possibile renderlo disponibile nel catalogo di Service Broker in modo che gli altri utenti possano utilizzarlo per la distribuzione. Per rendere individuabile il modello cloud in modo da poterlo aggiungere al catalogo, è necessario rilasciarlo. In questa procedura, verrà attribuita una versione al modello per acquisirne uno snapshot e quindi il modello verrà rilasciato.

- 1 Selezionare **Progettazione > Modello cloud** e aprire il modello nella tela di progettazione.
- 2 Fare clic su **Versione** e immettere una descrizione.

Creating Version ✕

Version * 7

Last Version: 6

Description Placement inputs added and tested.

Change Log

Release ☒ Release this version to the catalog
This cloud template is restricted to this project in the catalog. Edit shareability in cloud template level settings.

CANCEL CREATE

- 3 Selezionare la casella di controllo **Rilascia** e fare clic su **Crea**.

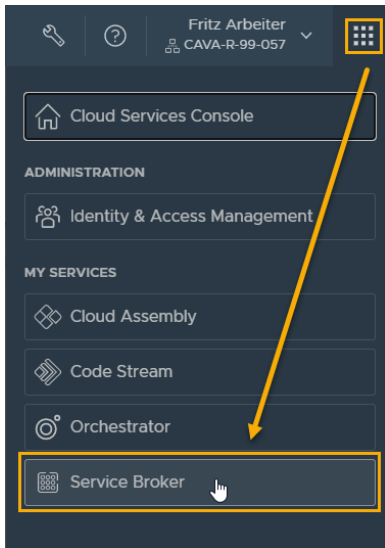
Quando il modello cloud viene rilasciato, non viene automaticamente aggiunto a Service Broker. Il rilascio lo rende individuabile in modo che sia possibile aggiungerlo al catalogo.

Passaggio 3. aggiunta del modello cloud al catalogo di Service Broker

È possibile utilizzare il catalogo di Service Broker per fornire modelli cloud agli altri utenti dell'organizzazione che non devono necessariamente sapere come si crea un modello. Il catalogo consente loro di distribuire il modello.

Per poter aggiungere il modello come elemento di catalogo, è necessario importarlo in Service Broker. È possibile importare solo modelli cloud rilasciati.

- 1 Per aprire Service Broker da Cloud Assembly, fare clic sul menu delle applicazioni nell'angolo superiore destro.



- 2 Fare clic su **Service Broker**.
- 3 Importare il modello cloud.
 - a In Service Broker, selezionare **Contenuto e criteri > Origini contenuto**.
 - b Fare clic su **Nuovo** e quindi selezionare **VMware Cloud Templates**.
 - c Immettere un nome in **Nome**.
In questo tutorial, immettere **Cloud Assembly DevProject**.
 - d In **Progetto**, selezionare il **progetto di sviluppo** creato in Cloud Assembly.
 - e Fare clic su **Convalida**.
Il sistema deve indicare che ha trovato almeno un elemento.
 - f Dopo la convalida, fare clic su **Crea e importa**.
Cloud Assembly DevProject viene aggiunto all'elenco come origine del contenuto.
- 4 Rendere il modello cloud disponibile nel catalogo.
 - a Selezionare **Contenuto e criteri > Condivisione contenuto**.
 - b Nell'elenco a discesa **Progetto**, selezionare **Progetto di sviluppo**.

- c Fare clic su **Aggiungi elementi** e quindi selezionare
- d Nella finestra di dialogo **Condividi elementi**, selezionare **Cloud Assembly DevProject** e fare clic su **Salva**.
- 5 Per verificare che il modello di sviluppo sia stato aggiunto al catalogo, fare clic su **Catalogo**.
- 6 Fare clic su **Richiedi** nella scheda Modello di sviluppo.

Si noti che qui vengono forniti gli input visti nel modello cloud. Il passaggio successivo consiste nella personalizzazione del modulo di richiesta.

New Request

Development Template Version **8** ▾

Project * Development Project ▾

Deployment Name * _____

Operating system * _____ ⓘ

Select Deployment Placement Development ▾ ⓘ

Deployment size * _____ ⓘ

Passaggio 4: creazione di un modulo personalizzato per il modello

L'obiettivo di questo modulo personalizzato è fornire un modulo in cui l'utente seleziona il sistema operativo e il posizionamento in base ai tag env:dev o env:prod. Quindi l'opzione env:dev consente all'utente di selezionare small o medium. L'opzione large non è disponibile. Tuttavia, se l'utente seleziona env:prod, l'opzione per selezionare large non è presente. L'input size è nascosto all'utente ma è incluso nella richiesta.

- 1 Per creare un modulo personalizzato in Service Broker, selezionare **Contenuti e criteri > Contenuto**.
- 2 Fare clic sui puntini di sospensione verticali a sinistra della voce Modello di sviluppo, quindi fare clic su **Modulo personalizzato**.
- 3 Personalizzare l'opzione di input.
 - a Nella tela, fare clic sui campi e configurare le proprietà come specificato nella tabella seguente.

Nome del campo nella tela	Aspetto	Valori	Vincoli
Sistema operativo	<p>Etichetta e tipo</p> <ul style="list-style-type: none"> ■ Etichetta = Sistema operativo 	<p>Opzioni valore</p> <ul style="list-style-type: none"> ■ Opzioni valore = Costante ■ Origine valore = centos CentOS, ubuntu Ubuntu <p>In questo esempio, vengono utilizzate le opzioni dei valori per personalizzare tutti i nomi dei sistemi operativi in minuscolo con il nome del sistema operativo preferito.</p>	
Selezione del posizionamento della distribuzione		<p>Opzioni valore</p> <ul style="list-style-type: none"> ■ Opzioni valore = Costante ■ Origine valore = env:dev Development, env:prod Production 	
Dimensione distribuzione	<p>Visibilità</p> <ul style="list-style-type: none"> ■ Origine valore = Valore condizionale ■ Impostare il valore = Yes se la selezione del posizionamento della distribuzione è uguale a env:dev 	<p>Valore predefinito</p> <ul style="list-style-type: none"> ■ Origine valore = Valore condizionale ■ Impostare il valore = large se la selezione della distribuzione è uguale a env:prod <p>Opzioni valore</p> <ul style="list-style-type: none"> ■ Opzioni valore = Costante ■ Origine valore = small Small, medium Medium <p>Si noti che l'origine del valore non include large. Large non è presente perché è disponibile solo per la produzione ed è il valore necessario. Il valore large è incluso nella richiesta di distribuzione senza un'azione avviata dall'utente.</p>	

b Per attivare il modulo nel catalogo, fare clic su **Abilita**.

- c Fare clic su **Salva**.
- 4 Per garantire risultati corretti inviando almeno una richiesta Development Small e una richiesta Production, testare il modulo nel catalogo.

Utilizzare gli esempi seguenti per verificare i risultati.

- a Eseguire il test del modulo di richiesta Development Small specificando un nome, Test small in questo esempio, e selezionando CentOS, Development e Small come opzioni.

- b Per verificare la distribuzione Development Small, selezionare **Risorse > Distribuzioni** e fare clic sulla distribuzione Test small.
- c Nella scheda Topologia, fare clic su Cloud_vSphere_Machine, quindi individuare la sezione Proprietà personalizzate nel riquadro destro.

Alcuni dei valori da rivedere includono cpuCount = 2 e flavor = small.

Property	Value
costCenter	DevProject
cpuCount	2
datastoreName	wld01-sc2vc05-wld01-clu0
endpointId	d827e01c-df9e-4c80-9f1d
flavor	small
image	centos

- d Eseguire il test del modulo di richiesta Production immettendo un nome, **Test large** in questo esempio, quindi selezionare CentOS e Production come opzioni.

Si tenga presente che il modulo è stato configurato in modo da non visualizzare l'input size, né richiederne l'immissione da parte dell'utente.

New Request

 Development Template Version **3** ▾

Project * Development Project ▾




Deployment Name * Test large

Operating System * CentOS ▾ ⓘ


Select Deployment Placement Production ▾ ⓘ

- e Per verificare la distribuzione Production, selezionare **Risorse > Distribuzioni** e fare clic sulla distribuzione Test large.
- f Nella scheda Topologia, fare clic su Cloud_vSphere_Machine, quindi individuare la sezione Proprietà personalizzate nel riquadro destro.

Alcuni dei valori da rivedere includono cpuCount = 8 e flavor = large.

 test large  Create Successful ACTIONS ▾ | 

No description

Owner	Expires on	Never
fritz	Last updated	May 21, 2021, 5:14:56 PM
Requestor	Created on	May 21, 2021, 4:53:05 PM
fritz		
Project		
Development Project		
Cloud Template	Development Template, version: 6	
		

[HIDE SUMMARY](#) ⤴

Topology History

Search resources

Cloud_NSX_N...

Cloud_vSpher...

Cloud_vSpher...

costCenter DevProject

cpuCount 8

datastoreName wld01-sc2vc05-wld01-clu

endpointId d827e01c-df9e-4c80-9f1d

flavor large

image centos

imageId centos7

Passaggio 5: controllo delle versioni dei modelli cloud nel catalogo

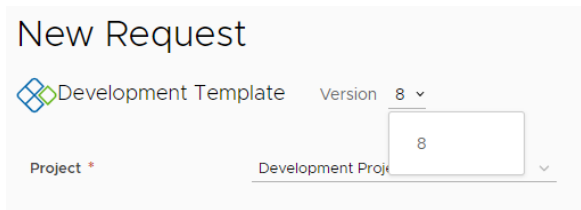
Nella maggior parte dei casi, si desidera rendere disponibili solo i modelli cloud più recenti nel catalogo di Service Broker. La seguente procedura supporta lo sviluppo iterativo, in cui si rilascia una versione del modello e la si aggiunge al catalogo, ma ora il modello è stato migliorato e si desidera sostituire la versione corrente con quella più recente.

Nel passaggio 2 è stata assegnata e rilasciata una versione del modello, quindi si ha già familiarità con il processo. Nel passaggio 3 è stata aggiunta al catalogo. La procedura collega i due passaggi mentre si esegue lo sviluppo iterativo e si aggiorna il catalogo con la versione più recente.

È possibile rendere disponibili più versioni nel catalogo.

- 1 In Cloud Assembly, assegnare una versione al modello che ora si desidera rendere disponibile nel catalogo.
 - a Selezionare **Progettazione > Modello cloud** e aprire il modello nella tela di progettazione.
 - b Fare clic su **Cronologia versioni**.
 - c Individuare la versione che si desidera aggiungere al catalogo e fare clic su **Versione**.
 - d Immettere una **Descrizione**, selezionare la casella di controllo **Rilascia** e fare clic su **Crea**.
 A questo punto, è possibile mantenere la versione precedente nel catalogo. Se si desidera mantenere più versioni, ignorare il passaggio successivo che consente di annullare il rilascio di una versione.
 - e Per rendere disponibile una sola versione del modello nel catalogo, rivedere l'elenco della cronologia delle versioni e fare clic su **Annulla rilascio** per ogni versione che non si desidera mantenere nel catalogo.
- 2 Per aggiornare il catalogo di Service Broker con la versione più recente e sostituire qualsiasi versione precedente, è necessario raccogliere la nuova versione.
 - a In Service Broker, selezionare **Contenuti e criteri > Origini contenuto**.
 - b Fare clic sull'origine del contenuto di Cloud Assembly DevProject utilizzata in questo tutorial.
 - c Fare clic su **Convalida**.
 Dovrebbe essere visualizzato un messaggio che indica che è stato trovato un elemento.
 - d Fare clic su **Salva e importa**.
- 3 Verificare che nel catalogo siano visualizzate le versioni necessarie o nessuna versione.
 - a In Service Broker, fare clic su **Catalogo**.
 - b Individuare l'elemento del catalogo e fare clic su **Richiedi**.
 - c Nella parte superiore del modulo di richiesta, fare clic su **Versione** e verificare la versione o le versioni.

La seguente schermata indica 8.



Tutorial: onboarding e gestione delle risorse di vSphere in vRealize Automation

In qualità di amministratore del cloud che ha aggiunto di recente un nuovo account cloud, si desidera iniziare a gestire alcuni dei carichi di lavoro di vCenter Server utilizzando Cloud Assembly e Service Broker. Questo tutorial illustra il processo di onboarding e come configurare alcune delle opzioni di gestione per i carichi di lavoro di vSphere esistenti.

Le attività di gestione di esempio includono l'aggiunta di risorse a un progetto, la creazione e l'applicazione di un criterio di approvazione in Service Broker e l'esecuzione di alcune azioni giorno 2 sulle risorse per dimostrare gli strumenti di gestione del ciclo di vita e attivare il criterio di approvazione.

In questo tutorial si presuppone che, nonostante non si abbia familiarità con Cloud Assembly, sia stato configurato un nuovo account cloud di vSphere. Quando si aggiunge l'account cloud, Cloud Assembly rileva le risorse attualmente non gestite nell'istanza di vSphere.

Operazioni preliminari

- Aggiungere il nuovo account vCenter Server. Per ulteriori istruzioni, vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).
- Verificare che l'account utente disponga almeno dei ruoli di servizio Amministratore di Cloud Assembly e Amministratore di Service Broker. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Per testare correttamente il criterio di approvazione dalla prospettiva di uno degli utenti, verificare di disporre di un account utente che disponga solo dei seguenti ruoli utente. In questo tutorial, l'utente si chiama Sylvia.
 - Membro dell'organizzazione
 - Utente di Cloud Assembly
 - Utente di Service Broker

Per ulteriori informazioni sui ruoli utente, vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

Passaggio 1: verificare che Cloud Assembly abbia rilevato le risorse

Quando si aggiunge un account di vCenter Server, Cloud Assembly rileva le risorse nell'istanza di vCenter Server. È possibile verificare che le macchine che si desidera iniziare a gestire siano disponibili per l'onboarding.

- 1 In Cloud Assembly, selezionare **Risorse > Risorse > Macchine virtuali**.
- 2 Nella griglia, rivedere di **Origine** e **Account/Regione**.

Il tipo di origine Rilevato indica che la macchina viene rilevata nell'istanza di vSphere anziché distribuita da vRealize Automation o già sottoposta a onboarding.

In questo esempio, Account/Regione è vCenter Account / wld01-DC.

Name	Status	Account / Region	Address	Project	Owner	Creation Time	Origin	Tags
DevProject-116	▶ On	vCenter Account / wld01-DC	N/A			Jul 26, 2021, 2:29:15 PM	Discover	
DevProject-centos-010	▶ On	vCenter Account / wld01-DC	N/A	Onboarding Project	fritz	Jul 26, 2021, 2:29:18 PM	Deployed	db:mysql
DevProject-centos-012	▶ On	vCenter Account / wld01-DC	N/A			Jul 26, 2021, 2:29:18 PM	Discover	
DevProject-centos-013	▶ On	vCenter Account / wld01-DC	N/A			Jul 26, 2021, 2:29:15 PM	Discover	db:mysql
DevProject-centos-016	▶ On	vCenter Account / wld01-DC	N/A	Onboarding Project	sylvia	Jul 26, 2021, 2:29:15 PM	Deployed	db:mysql

Passaggio 2: creare un progetto di destinazione

Creare un progetto a cui assegnare le macchine sottoposte a onboarding. Per gestire le risorse, queste devono far parte di un progetto che includa la zona cloud di origine in cui sono state originariamente distribuite.

Per testare questo tutorial, è necessario disporre di un altro utente che non sia un amministratore. In questo passaggio, in qualità di amministratore, si aggiunge Sylvia come membro del progetto.

Per ulteriori informazioni sui progetti, vedere [Capitolo 5 Aggiunta e gestione di progetti di Cloud Assembly](#).

- 1 In Cloud Assembly, selezionare **Infrastruttura > Progetti > .**
- 2 Nella pagina Progetti, fare clic su **Nuovo progetto**.
- 3 Immettere il **nome** del progetto.

In questo tutorial, il nome del progetto è **Onboarding Project**.

- 4 Fare clic sulla scheda **Utenti**.
 - a Fare clic su **Aggiungi utenti** e aggiungere almeno un utente come membro del progetto.

In questo tutorial, si aggiunge Sylvia.

- b Fare clic su **Aggiungi**.
- 5 Fare clic su **Provisioning**.
 - a Fare clic su **Aggiungi Zona**.
 - b Fare clic su **Zona cloud**.
 - c Selezionare l'account/regione identificato nel passaggio 1.

In questo tutorial, il valore di esempio è vCenter Account / wld01-DC.

New Project

Summary Users **Provisioning** Kubernetes Provisioning

Zones

Specify the zones that can be used when users provision deployments in this project. ⓘ

[+ADD ZONE](#) [X REMOVE](#)

<input type="checkbox"/>	Name	Status	Description	Priority	Instances	Memory Limit (MB)	CPU Limit	Storage Limit (GB)	Capability Tags
<input type="checkbox"/>	vCenter Account / wld01-DC	--		0	Unlimited	Unlimited	Unlimited	Unlimited	

1 - 1 of 1 zones

Specify the placement policy that will be applied when selecting a cloud zone for provisioning.

Placement policy **DEFAULT** ⓘ

- d Fare clic su **Aggiungi**.
- 6 Fare clic su **Crea**.

Passaggio 3: creare ed eseguire un piano di onboarding

In qualità di amministratore del cloud, è possibile eseguire l'onboarding delle macchine rilevate dall'istanza di vSphere in modo da poter applicare la governance e gestire le risorse con le azioni giorno 2.

Per ulteriori informazioni sui piani di onboarding, vedere [Che cosa sono i piani di onboarding in Cloud Assembly](#).

- 1 In Cloud Assembly, selezionare **Infrastruttura > Onboarding** e quindi fare clic su **Nuovo piano di onboarding**.
- 2 Inserire le informazioni di onboarding.

Impostazione	Valore di esempio
Nome del piano	wld01-DC Onboarding Plan
Account cloud	Account vCenter
Progetto predefinito	Progetto di onboarding

- 3 Fare clic su **Crea**.
- 4 Aggiungere le macchine da sottoporre a onboarding.

Non eseguire il piano di onboarding finché non vengono completati tutti i passaggi seguenti.

- a Fare clic su **Macchine**, quindi fare clic su **Aggiungi macchine**.
- b Selezionare le macchine che si desidera includere nel piano, quindi fare clic su **OK**.

Per questo tutorial, sono selezionate solo due macchine.

- c Nella finestra di dialogo Crea distribuzioni, selezionare **Crea distribuzioni del piano per ogni macchina**, quindi fare clic su **Crea**.

Selezionare questa opzione quando si desidera che le macchine vengano distribuite singolarmente in modo da poterle gestire come risorse individuali.

- d Le macchine selezionate vengono aggiunte all'elenco.

	Name	Status	Power	Address	Deployment	Custom properties	Tags
<input type="checkbox"/>	DevProject-centos-013	Pending	On		Deployment-5e3ac...	Inherited	db.mysql
<input type="checkbox"/>	DevProject-centos-204	Pending	On		Deployment-50507...	Inherited	db.mysql

5 Rinominare le distribuzioni.

- a Fare clic su **Distribuzioni** nella pagina di onboarding.
- b Per modificare il nome della distribuzione generata, selezionare una distribuzione e fare clic su **Rinomina**.
- c Immettere il nuovo nome, quindi fare clic su **Salva**.

Ad esempio, Onboarding machine 1.

- d Ripetere se necessario.

6 Assegnare un proprietario alle distribuzioni.

Se non si assegna un proprietario, si diventa proprietari. Il proprietario deve essere un membro del progetto di destinazione.

Questo tutorial assegna tutte le distribuzioni allo stesso proprietario. Facoltativamente, è possibile assegnare diverse distribuzioni a proprietari diversi.

- a Selezionare tutte le distribuzioni e fare clic su **Modifica proprietario**.
- b Selezionare il proprietario e fare clic su **Salva**.

Rivedere il nome della distribuzione e le modifiche del proprietario nella griglia.

wld01-DC Onboarding Plan

Summary Machines Deployments

These deployments will be created or updated when the plan runs. By default each added machine is placed in its own Cloud Assembly deployment.

RENAME EDIT OWNER CLOUD TEMPLATE REMOVE

<input type="checkbox"/>	Deployment Name	Status	Create Cloud Template	Owner	Components
<input type="checkbox"/>	> Onboarded deployment 1	✓		sylvia	1
<input type="checkbox"/>	> Onboarded deployment 2	✓		sylvia	1

2 deployments

SAVE RUN CANCEL

7 Fare clic su **Esegui**.

Dopo aver eseguito il piano di onboarding, non è possibile modificare il nome o assegnare proprietari. Se si aggiungono altre macchine al piano, è possibile modificare il nome o il proprietario.

8 Rivedere le risorse di cui è stato eseguito l'onboarding come distribuzioni.

a Selezionare **Risorse > Distribuzioni**.

b Per individuare le distribuzioni, è possibile cercare in base al nome della distribuzione, al progetto o al proprietario.

Deployments

20 Items of 26

Search deployments

Sort: Created on (descending)

	Name	Address	Owner	Project	Status	Expires on	Price
>	Onboarded machine 1		sylvia	Onboarding Project		Never	
∨	Onboarded machine 2		sylvia	Onboarding Project		Never	
	DevProject-centos-016				On		
>	Resize		fritz	onboard project 2		Never	
>	Resize Boot Disk		fritz	Onboarding Project	Onboard — Failed	Never	
>	Resize Disk		fritz	Onboarding Project		Never	
>	Shutdown		fritz	Onboarding Project		Never	
>	Suspend		fritz	Onboarding Project		Never	
>	Unregister		fritz	Onboarding Project		Never	
>	Update Tags		fritz	Onboarding Project		Never	
>	Delete Snapshot		fritz	Onboarding Project		Never	

Ora che sono state importate le macchine in vRealize Automation, è possibile iniziare a gestirle.

Passaggio 4: ridimensionare una distribuzione

Eseguire questo passaggio come amministratore del cloud per familiarizzare con il funzionamento delle azioni giorno 2. Le modifiche che è possibile apportare alle distribuzioni vengono definite azioni giorno 2. L'utilizzo delle azioni giorno 2 rappresenta il primo passaggio della gestione delle risorse.

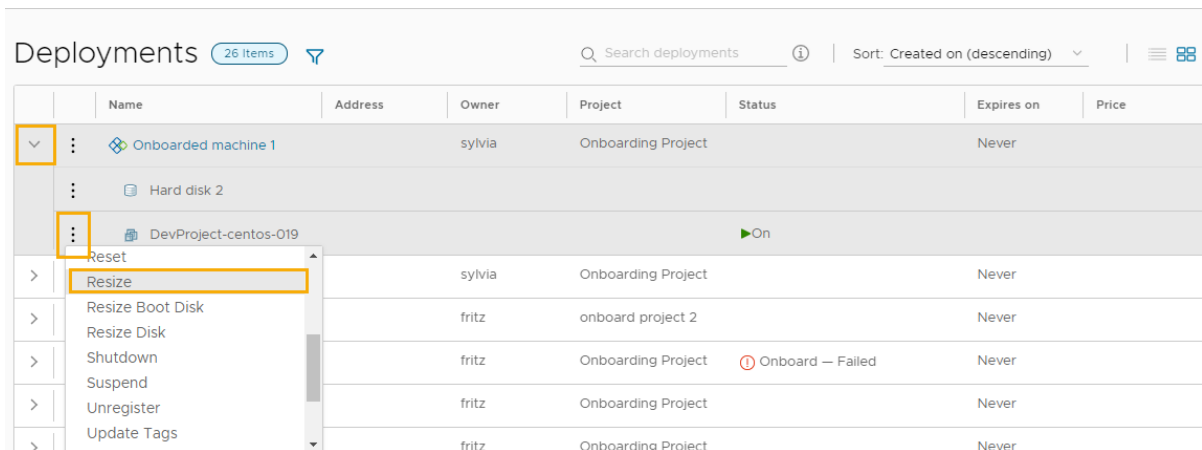
Per questo tutorial, si ritiene che il numero di CPU su una macchina sia troppo elevato e si desidera ridurre il consumo di CPU. Questa procedura presuppone che si stia eseguendo l'azione di ridimensionamento su una macchina vSphere accesa. Presuppone inoltre che non siano presenti criteri del giorno 2 che vietano a un utente di eseguire questa azione.

Le azioni disponibili dipendono dal tipo di risorsa, dallo stato della risorsa e dai criteri del giorno 2. Per ulteriori informazioni sulla creazione delle azioni giorno 2, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

- 1 In Cloud Assembly, selezionare **Risorse > Distribuzioni**, quindi individuare le distribuzioni di cui è stato eseguito l'onboarding.

È possibile utilizzare le opzioni di ricerca o filtro.

- 2 Espandere la distribuzione utilizzando la freccia a sinistra, quindi fare clic sui puntini di sospensione verticali sul nome della macchina e fare clic su **Ridimensiona**.

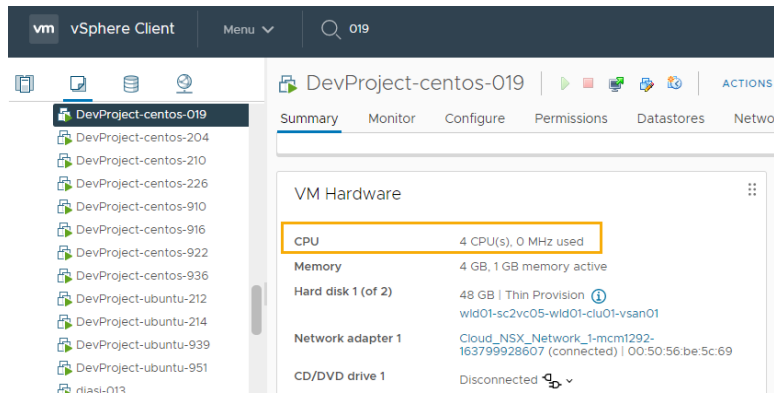


- 3 Nella finestra di dialogo **Ridimensiona**, ridurre il numero di CPU a **4** e fare clic su **Invia**.

Il valore suggerito è un esempio: modificare il conteggio CPU in un valore valido per il proprio ambiente.

L'azione viene eseguita sulla macchina.

- 4 Per verificare che il conteggio CPU sia stato modificato, aprire la distribuzione e controllare la proprietà personalizzata `cpuCount` per la macchina.
- 5 È inoltre possibile verificare il conteggio in vCenter Server.



Passaggio 5: applicazione dei criteri di approvazione

In qualità di amministratore del cloud, è possibile applicare la governance in vRealize Automation per limitare le operazioni che gli utenti possono eseguire o richiedere la loro approvazione prima che possano farlo. Questo tutorial mostra come applicare i criteri di approvazione all'azione di ridimensionamento in modo che gli utenti non possano riconfigurare una macchina, anche in modo irreversibile, senza la propria approvazione o l'approvazione di un altro amministratore.

I criteri vengono creati in Service Broker. Tuttavia, i criteri si applicano alle richieste pertinenti in Cloud Assembly e Service Broker.

In qualità di approvatore, è necessario rispondere alla richiesta di approvazione in Service Broker.

- 1 In Service Broker, selezionare **Contenuto e criteri > Criteri > Definizioni**, quindi fai clic su **Nuovo criterio**.
- 2 Fare clic su **Criterio di approvazione**.
- 3 Configurare il criterio di approvazione.

Resize Approval Policy [DELETE](#)

Approval policies control who must agree to a deployment or day 2 action before the request is provisioned. ⓘ

Type: Approval

Name:

Description:

Scope: ☐ Organization / Multiple Projects ⓘ
Apply the policy to all or a selection of projects in this organization. To target multiple projects, select project based criteria.
☒ Project ⓘ
Apply this policy to a single project in this organization.
 Onboarding Project

Criteria: ⓘ

Approval type: ☒ User based ⓘ ☐ Role based ⓘ

Approver mode: ☒ Any ⓘ ☐ All ⓘ

Approvers: ⓘ

<input type="checkbox"/>	Name	Email	Type
<input type="checkbox"/>	Fritz Arbeiter	fritz	User
<input type="checkbox"/>			1 user

Auto expiry decision: ⓘ

Auto expiry trigger: days ⓘ

Actions: ⓘ

<input type="checkbox"/>	Actions
<input type="checkbox"/>	Cloud.vSphere.Machine.Resize

La tabella seguente include valori di esempio che illustrano come creare il criterio.

Impostazione	Valore di esempio
Nome	Ridimensiona criterio di approvazione
Scope	Selezionare Progetto , quindi selezionare Progetto di onboarding . Il criterio di approvazione viene attivato quando un utente membro del progetto esegue un'azione giorno 2 di ridimensionamento.
Tipo di approvazione	Basato su utente Questo valore consente di assegnare un nome agli approvatori.
Modalità approvatore	Qualsiasi Se si dispone di più approvatori, la richiesta di approvazione può essere risolta da almeno un approvatore.
Approvatori	Aggiungere se stessi come approvatore.
Decisione scadenza automatica	Rifiuta Rifiutando una richiesta non rivista, si riduce il rischio di rendere una macchina inutilizzabile o con risorse eccessive.

Impostazione	Valore di esempio
Trigger scadenza automatica	1
Azioni	<p>Selezionare l'azione di ridimensionamento che attiva il criterio di approvazione.</p> <ol style="list-style-type: none"> 1 Immettere machine.resize nella ricerca. 2 Nell'elenco a discesa dei risultati di ricerca, fare clic su Selezione multipla. 3 Selezionare Cloud.vSphere.Machine.Resize. <p>Per questo tutorial, basato su vSphere, selezionare l'azione vSphere.Machine. Se si desidera che il criterio di azione venga applicato ad altri tipi di risorse, è possibile aggiungere le altre azioni Machine.Resize.</p>

Passaggio 6: richiedere una richiesta di ridimensionamento come utente

In questo passaggio, si accede a Service Broker come membro dell'organizzazione e come utente di Service Broker, e si esegue una richiesta giorno 2 di ridimensionamento. La richiesta crea una richiesta di approvazione. L'utente può eseguire gli stessi passaggi anche in Cloud Assembly.

Nel passaggio successivo a questo, accedere come utente assegnato come approvatore nel passaggio 5 e approvare la richiesta.

- 1 Accedere a Service Broker come utente.

In questo tutorial, l'utente è Sylvia.

- 2 Selezionare **Risorse > Distribuzioni** e individuare Onboarded machine 1.

Questa distribuzione è quella in cui è stata eseguita l'azione di ridimensionamento sulla macchina nel passaggio 4, modificando il numero di CPU da 8 a 4. Se è stato utilizzato un valore diverso, modificare la macchina in modo che sia possibile procedere con il test.

- 3 Eseguire l'azione **Ridimensiona** sulla macchina, aumentando il numero di CPU a 6.
- 4 Si noti che la richiesta è in attesa di approvazione.

Per visualizzare lo stato in sospeso, passare il puntatore del mouse sull'icona delle informazioni nella griglia o aprire la distribuzione e rivedere la scheda **Cronologia**.

Deployments 20 Items of 24 Search deployments Sort: Created on (descending)						
	Name	Address	Owner	Project	Status	Expires on
▼	Onboarded ma...		sylvia	Onboarding P...	1	Never
	Hard disk 2					
	DevProject-c...					
>	Onboarded ma...		sylvia	Onboarding P...		

- 5 In qualità di utente, la modifica richiesta da Sylvia non procede finché non viene approvata.
- 6 Disconnettersi da Service Broker come utente.

Nel passaggio 7 si accede come approvatore assegnato e si risponde alla richiesta.

Passaggio 7: rispondere a una richiesta di approvazione

Quando una richiesta richiede un'approvazione e si è l'approvatore, si riceve un messaggio e-mail. Per questo tutorial, non si attende il messaggio. Al contrario, il processo consente di rispondere direttamente alle richieste di approvazione utilizzando la scheda Approvazioni Service Broker.

- 1 Accedere a Service Broker come utente assegnato come approvatore nel passaggio 5.

In questo tutorial, l'approvatore è Fritz.

- 2 Selezionare **Risorse > Distribuzioni** e individuare Onboarded machine 1.

Lo stato della griglia è lo stesso di Sylvia.

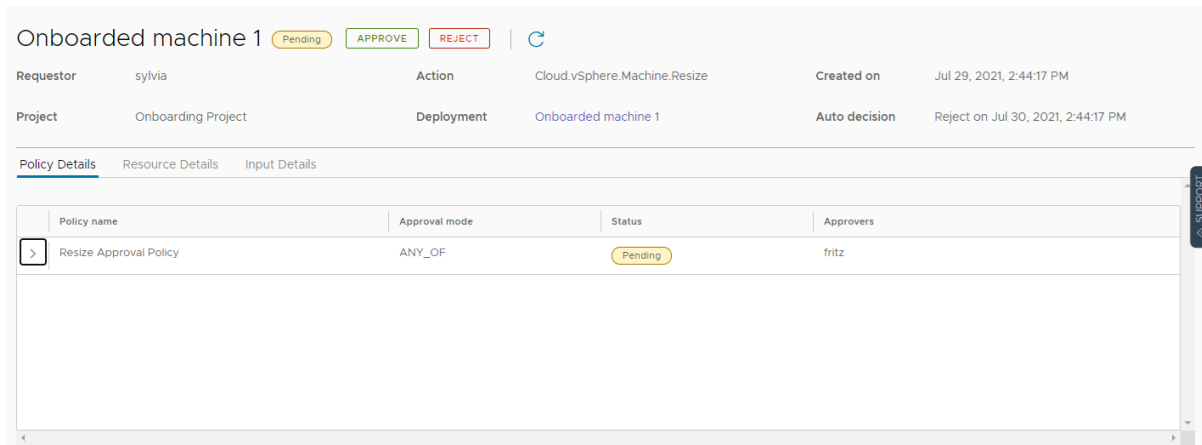
Name	Address	Owner	Project	Status	Expires on	Price
Onboarded machine 1		sylvia	Onboarding Project	Approval Pending	Never	
Hard disk 2						
DevProject-c...						

- 3 Fare clic sulla scheda **Approvazioni**.

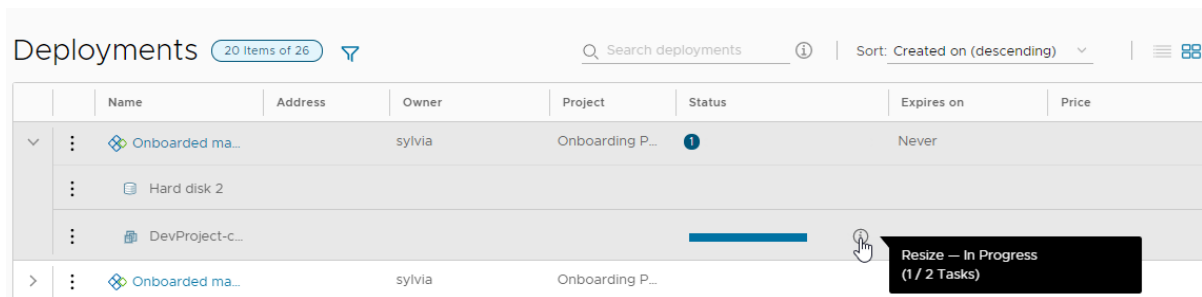
Si noti che è presente una richiesta di approvazione in sospeso.

Name	Status	Expires on	Action	Created on	Policy details
Onboarded machine 1	Pending	Expires on Jul 30, 2021, 2:44:17 PM	Cloud.vSphere.Machine.Resize	Created on: Jul 29, 2021, 2:44:17 PM	Resize Approval Policy

- 4 Per visualizzare i dettagli della richiesta, fare clic sul nome del distribuzione.



- 5 Fare clic su **Approva**, fornire un commento, se necessario, e fare clic su **Approva**.
- 6 Tornare alla pagina **Distribuzioni** per verificare che l'azione di ridimensionamento di Sylvia sia in corso.



- 7 Una volta completata l'azione di ridimensionamento, è possibile verificare il numero di CPU nei dettagli della distribuzione e in vSphere Client.

Questo tutorial ha consentito di eseguire il processo di inserimento delle macchine in vRealize Automation, in modo da poter iniziare a gestire il ciclo di vita della risorsa.

Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly

Questo tutorial di Cloud Assembly end-to-end mostra come distribuire in un'impostazione multi-cloud. È possibile distribuire lo stesso modello cloud in più provider, in questo caso AWS e Microsoft Azure.

In questo esempio, l'applicazione è un sito WordPress. Osservare la configurazione sequenziale per comprendere il processo che porta al completamento di un'intera progettazione.

Tenere presente che i nomi e i valori visualizzati sono solo esempi. Non sarà possibile utilizzarli alla lettera nel proprio ambiente.

Per adattarli alle proprie esigenze di distribuzione e infrastruttura cloud, esaminare dove creare sostituzioni personalizzate rispetto ai valori di esempio.

Parte 1: configurazione dell'infrastruttura Cloud Assembly di esempio

Innanzitutto, configurare le risorse con cui gli utenti tecnici di Cloud Assembly possono successivamente sviluppare, testare e mettere in produzione l'applicazione.

L'infrastruttura include destinazioni cloud e definizioni relative alle macchine, alle reti e allo storage disponibili di cui avrà bisogno il sito WordPress.

Prerequisiti

Accedere a Cloud Assembly come Amministratore Cloud Assembly.

1. Aggiunta di account cloud

In questo passaggio l'amministratore del cloud aggiunge due account cloud. Il progetto di esempio prevede l'esecuzione di attività di sviluppo e test su AWS e il passaggio alla produzione in Azure.

- 1 Passare a **Infrastruttura > Connessioni > Account cloud**.
- 2 Fare clic su **Aggiungi account cloud**, selezionare Amazon Web Services e immettere i valori.

Impostazione	Valore di esempio
ID chiave di accesso	R5SDR3PXVV2ZW8B7YNSM
Chiave di accesso segreta	SZXAINXU4UHNQAQ1E156S
Nome	OurCo-AWS
Descrizione	WordPress

Tenere presente che tutti i valori sono solo esempi. Le specifiche dell'account variano.

- 3 Per verificare le credenziali, fare clic su **Convalida**.
- 4 Fare clic su **Aggiungi**.
- 5 Modificare la **Configurazione** dell'account appena aggiunto e consentire il provisioning alle regioni us-east-1 e us-west-2
- 6 Fare clic su **Aggiungi account cloud**, selezionare Microsoft Azure e immettere i valori.

Impostazione	Valore di esempio
ID sottoscrizione	ef2avpf-dfdv-zxluguii-g4h0-i8ep2jwp4c9arbfe
ID tenant	dso9wv3-4zgc-5nrcy5h3m-4skf-nnovp40wfxsro22r
ID applicazione client	bg224oq-3ptp-mbhi6aa05-q511-uflyjr2sttyik6bs
Chiave privata applicazione client	7uqxi57-0wtn-kymgf9wcj-t2l7-e52e4nu5fig4pmdd
Nome	OurCo-Azure
Descrizione	WordPress

- 7 Per verificare le credenziali, fare clic su **Convalida**.
- 8 Fare clic su **Aggiungi**.
- 9 Modificare la **Configurazione dell'account** appena aggiunto e consentire il provisioning alla regione East US.

2. Aggiunta di zone cloud

In questo passaggio di esempio, l'amministratore del cloud aggiunge tre zone cloud, una per lo sviluppo, una per il test e una per la produzione.

- 1 Passare a **Infrastruttura > Configura > Zone cloud**.
- 2 Fare clic su **Nuova zona cloud** e immettere i valori per l'ambiente di sviluppo.

Impostazione della zona cloud	Valore di esempio
Account/Regione	OurCo-AWS/us-east-1
Nome	OurCo-AWS-US-East
Descrizione	WordPress
Criterio di posizionamento	Predefinito
Tag di funzionalità	env:dev

Tenere presente che tutti i valori sono solo esempi. Le specifiche della zona variano.

- 3 Fare clic su **Risorse di elaborazione** e verificare che le zone previste siano presenti.
- 4 Fare clic su **Crea**.
- 5 Ripetere il processo due volte, con valori per gli ambienti di test e di produzione.

Impostazione della zona cloud	Valore di esempio
Account/Regione	OurCo-AWS/us-west-2
Nome	OurCo-AWS-US-West
Descrizione	WordPress
Criterio di posizionamento	Predefinito
Tag di funzionalità	env:test

Impostazione della zona cloud	Valore di esempio
Account/Regione	OurCo-Azure/East US
Nome	OurCo-Azure-East-US
Descrizione	WordPress

Impostazione della zona cloud	Valore di esempio
Criterio di posizionamento	Predefinito
Tag di funzionalità	env:prod

3. Aggiunta di mappature delle caratteristiche

In questo passaggio di esempio, l'amministratore del cloud aggiunge mappature delle caratteristiche per tenere in considerazione le differenti esigenze di capacità a seconda della distribuzione.

La mappatura delle caratteristiche tiene conto delle distribuzioni di macchine di dimensioni diverse e viene definita in modo informale come taglia di t-shirt.

- 1 Passare a **Infrastruttura > Configura > Mappature delle caratteristiche**. Ogni zona cloud deve consentire caratteristiche di dimensioni piccole, medie e grandi.
- 2 Fare clic su **Nuova mappatura delle caratteristiche** e immettere i valori per la zona cloud di sviluppo.

Impostazione	Valore di esempio
Nome caratteristica	piccolo
Account/Regione Valore	OurCo-AWS/us-east-1 t2.micro
Account/Regione Valore	OurCo-AWS/us-west-2 t2.micro
Account/Regione Valore	OurCo-Azure/East US Standard_A0

Tenere presente che tutti i valori sono solo esempi. Le caratteristiche variano.

- 3 Fare clic su **Crea**.
- 4 Ripetere il processo due volte, con valori per le caratteristiche di dimensioni medie e grandi.

Impostazione	Valore di esempio
Nome caratteristica	medio
Account/Regione Valore	OurCo-AWS/us-east-1 t2.medium
Account/Regione Valore	OurCo-AWS/us-west-2 t2.medium
Account/Regione Valore	OurCo-Azure/East US Standard_A3

Impostazione	Valore di esempio
Nome caratteristica	grande
Account/Regione	OurCo-AWS/us-east-1
Valore	t2.large
Account/Regione	OurCo-AWS/us-west-2
Valore	t2.large
Account/Regione	OurCo-Azure/East US
Valore	Standard_A7

4. Aggiunta di mappature dell'immagine

In questo passaggio di esempio, l'amministratore del cloud aggiunge una mappatura dell'immagine per Ubuntu, l'host per il server di WordPress e il suo server di database MySQL.

Pianificare il sistema operativo aggiungendo mappature dell'immagine. Ogni zona cloud ha bisogno di una mappatura dell'immagine Ubuntu.

- 1 Passare a **Infrastruttura > Configura > Mappature immagine**.
- 2 Fare clic su **Nuova mappatura immagine** e immettere i valori per i server Ubuntu.

Impostazione	Valore di esempio
Nome immagine	ubuntu
Account/Regione	OurCo-AWS/us-east-1
Valore	ubuntu-16.04-server-cloudimg-amd64
Account/Regione	OurCo-AWS/us-west-2
Valore	ubuntu-16.04-server-cloudimg-amd64
Account/Regione	OurCo-Azure/East US
Valore	azul-zulu-ubuntu-1604-923eng

Tenere presente che tutti i valori sono solo esempi. Le immagini possono variare.

- 3 Fare clic su **Crea**.

5. Aggiunta di profili di rete

In questo passaggio di esempio, l'amministratore del cloud aggiunge un profilo di rete a ogni zona cloud.

In ciascun profilo, l'amministratore aggiunge una rete per le macchine WordPress e una seconda rete che sarà posizionata dall'altra parte di un eventuale bilanciamento del carico. La seconda rete sarà quella a cui gli utenti si connetteranno.

- 1 Passare a **Infrastruttura > Configura > Profili di rete**.
- 2 Fare clic su **Nuovo profilo di rete** e creare un profilo per la zona cloud di sviluppo.

Impostazione del profilo di rete	Valore di esempio
Account/Regione	OurCo-AWS/us-east-1
Nome	devnets
Descrizione	WordPress

3 Fare clic su **Reti** e fare clic su **Aggiungi rete**.

4 Selezionare wpnet, appnet-public e fare clic su **Aggiungi**.

Tenere presente che tutti i valori sono solo esempi. I nomi di rete variano.

5 Fare clic su **Crea**.

Questo esempio di Wordpress non richiede di specificare i criteri di rete o le impostazioni di sicurezza della rete.

6 Ripetere il processo due volte per creare un profilo di rete per l'esempio di test di Wordpress e per le zone cloud di produzione. In ogni caso, aggiungere le reti wpnet and appnet-public.

Impostazione del profilo di rete	Valore di esempio
Account/Regione	OurCo-AWS/us-west-2
Nome	testnets
Descrizione	WordPress

Impostazione del profilo di rete	Valore
Account/Regione	OurCo-Azure/East US
Nome	prodnets
Descrizione	WordPress

6. Aggiunta di profili di storage

In questo passaggio di esempio, l'amministratore del cloud aggiunge un profilo di storage a ogni zona cloud.

L'amministratore posiziona lo storage rapido nella zona di produzione e lo storage generale nella zona di sviluppo e nel test.

1 Passare a **Infrastruttura > Configura > Profili di storage**.

2 Fare clic su **Nuovo profilo di storage** e creare un profilo per la zona cloud di sviluppo.

Dopo aver selezionato l'account/regione, vengono visualizzati campi aggiuntivi.

Impostazione del profilo di storage	Valore di esempio
Account/Regione	OurCo-AWS/us-east-1
Nome	OurCo-AWS-US-East-Disk
Descrizione	WordPress
Tipo di dispositivo	EBS
Tipo di volume	SSD per utilizzo generico
Tag di funzionalità	storage:general

Tenere presente che tutti i valori sono solo esempi.

- 3 Fare clic su **Crea**.
- 4 Ripetere il processo per creare un profilo per la zona cloud di test.

Impostazione del profilo di storage	Valore di esempio
Account/Regione	OurCo-AWS/us-west-2
Nome	OurCo-AWS-US-West-Disk
Descrizione	WordPress
Tipo di dispositivo	EBS
Tipo di volume	SSD per utilizzo generico
Tag di funzionalità	storage:general

- 5 Ripetere il processo per creare un profilo per la zona cloud di produzione, che ha impostazioni diverse in quanto è una zona Azure.

Impostazione del profilo di storage	Valore di esempio
Account/Regione	OurCo-Azure/East US
Nome	OurCo-Azure-East-US-Disk
Descrizione	WordPress
Tipo di storage	Dischi gestiti
Tipo di disco	LRS premium
Memorizzazione nella cache del disco del sistema operativo	Sola lettura
Memorizzazione nella cache del disco dati	Sola lettura
Tag di funzionalità	storage:fast

Passaggi successivi

Creare un progetto per identificare gli utenti e definire le impostazioni di provisioning. Vedere [Parte 2: creazione del progetto Cloud Assembly di esempio](#).

Parte 2: creazione del progetto Cloud Assembly di esempio

Il progetto Cloud Assembly di esempio consente agli utenti abilitati di eseguire il provisioning e configura il livello di provisioning possibile.

I progetti definiscono le impostazioni dell'utente e del provisioning.

- Gli utenti e il livello di autorizzazione del loro ruolo
- Priorità delle distribuzioni mentre vengono sottoposte a provisioning in una zona cloud
- Numero massimo di istanze di distribuzione per zona cloud

Procedura

- 1 Passare a **Infrastruttura > Amministrazione > Progetti**.
- 2 Fare clic su **Nuovo progetto** e immettere il nome WordPress.
- 3 Fare clic su **Utenti**, quindi su **Aggiungi utenti**.
- 4 Aggiungere gli indirizzi email e i ruoli per gli utenti.

Per aggiungere correttamente un utente, è necessario che un amministratore di VMware Cloud Services abbia abilitato l'accesso a Cloud Assembly per l'utente.

Tenere presente che gli indirizzi mostrati qui sono solo esempi.

- chris.ladd@ourco.com, membro
- kerry.mott@ourco.com, membro
- pat.tubb@ourco.com, amministratore

- 5 Fare clic su **Provisioning** e su **Aggiungi zona cloud**.
- 6 Aggiungere le zone cloud su cui gli utenti possono eseguire la distribuzione.

Impostazione delle zone cloud del progetto	Valore di esempio
Zona cloud	OurCo-AWS-US-East
Priorità di provisioning	1
Limite di istanze	5
Zona cloud	OurCo-AWS-US-West
Priorità di provisioning	1
Limite di istanze	5
Zona cloud	OurCo-Azure-East-US
Priorità di provisioning	0
Limite di istanze	1

- 7 Fare clic su **Crea**.

- 8 Passare a **Infrastruttura > Configura > Zone cloud** e aprire una zona creata in precedenza.
- 9 Fare clic su **Progetti** e verificare che WordPress sia un progetto a cui è consentito eseguire il provisioning per la zona.
- 10 Controllare le altre zone create.

Operazioni successive

Creare un modello cloud di base.

Parte 3: progettazione e distribuzione del modello di Cloud Assembly di esempio

Quindi, si definisce l'applicazione di esempio, il sito WordPress, sotto forma di un modello cloud generico. Il modello può essere distribuito a diversi fornitori di soluzioni cloud senza che sia necessario modificarne la progettazione.

L'esempio è costituito da un server dell'applicazione WordPress, un server di database MySQL e risorse di supporto. Il modello inizia con alcune risorse, quindi cresce man mano che si modificano le risorse esistenti e se ne aggiungono altre.

Di seguito sono indicati i valori della [Parte 1: configurazione dell'infrastruttura Cloud Assembly di esempio](#), l'infrastruttura impostata da un amministratore del cloud:

- Due account cloud, AWS e Azure.
- Tre ambienti di zona cloud:
 - Sviluppo - OurCo-AWS-US-East
 - Test - OurCo-AWS-US-West
 - Produzione - OurCo-Azure-East-US
- Mappature delle caratteristiche con risorse di elaborazione di piccole, medie e grandi dimensioni per ciascuna zona.
- Mappature delle immagini per Ubuntu configurate in ciascuna zona.
- Profili di rete con subnet interne ed esterne per ciascuna zona.
- Storage su cui distribuire; storage generale per la zona di sviluppo e test e storage rapido per la zona di produzione.
- Il progetto di esempio include tutti i tre ambienti della zona cloud, oltre agli utenti che possono creare progetti.

Prerequisiti

Per monitorare, è necessario conoscere i valori della propria infrastruttura. Questo esempio utilizza AWS per lo sviluppo e il test e Azure per la produzione. Quando si crea il proprio modello cloud, sostituire con i propri valori, in genere impostati dall'amministratore del cloud.

Procedura

1 Creazione un modello cloud di base

In questo esempio di progetto di Cloud Assembly, si inizia con un modello cloud che contiene solo le risorse di base di WordPress, ad esempio un solo server applicazioni.

2 Test di un modello cloud di base

Durante la progettazione, è spesso necessario creare un modello cloud iniziando dalle basi, quindi distribuire e testare con la crescita del modello. In questo esempio vengono illustrato alcuni dei test in corso integrati in Cloud Assembly.

3 Espansione di un modello cloud

Dopo aver creato e testato un modello di Cloud Assembly di base per l'applicazione di esempio, è possibile espanderlo in un'applicazione a più livelli distribuibile allo sviluppo, al test e infine alla produzione.

Creazione un modello cloud di base

In questo esempio di progetto di Cloud Assembly, si inizia con un modello cloud che contiene solo le risorse di base di WordPress, ad esempio un solo server applicazioni.

Cloud Assembly è uno strumento infrastructure-as-code. Si trascinano le risorse nella tela di progettazione per iniziare. Quindi, è possibile completare i dettagli utilizzando l'editor di codice a destra della tela.

L'editor di codice consente di digitare, tagliare e incollare direttamente il codice. Se si sta modificando la modifica del codice, è possibile selezionare una risorsa nella tela, fare clic sulla scheda **Proprietà** dell'editor di codice e immettere i valori. I valori immessi vengono visualizzati nel codice come se fossero stati digitati direttamente.

Procedura

1 Passare a **Progettazione > Modelli cloud** e fare clic su **Nuovo da > Tela vuota**.

2 Denominare il modello cloud **Wordpress-BP**.

3 Selezionare il progetto **WordPress** e fare clic su **Crea**.

4 Dalle risorse a sinistra della pagina di progettazione del modello cloud, trascinare due macchine indipendenti dal cloud sulla tela.

Le macchine fungono da server applicazioni di WordPress (WebTier) e server di database MySQL (DBTier).

- 5 A destra, modificare il codice YAML della macchina per aggiungere nomi, immagini, caratteristiche e tag di vincolo:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: small
      constraints:
        - tag: env:dev
```

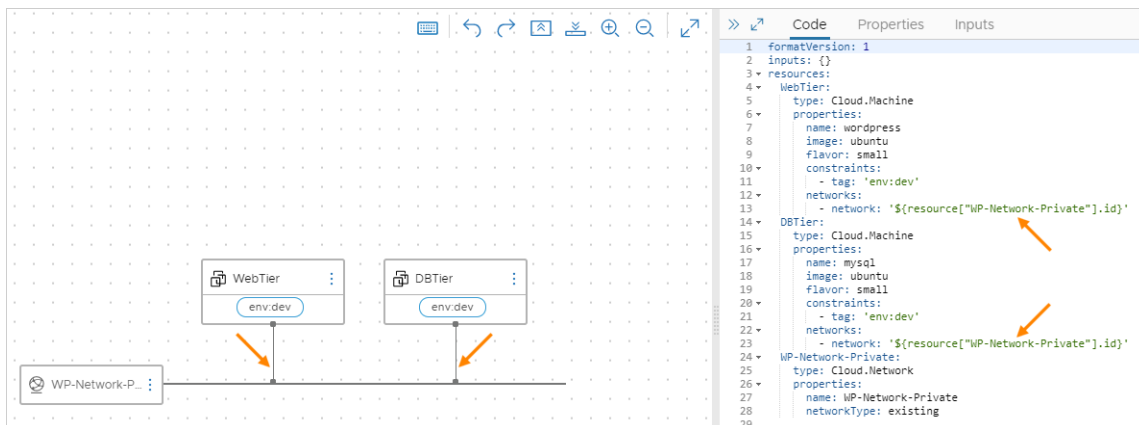
- 6 Trascinare una rete indipendente dal cloud nella tela e modificarne il codice:

```
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing
```

- 7 Connettere le macchine alla rete:

Nella tela, passare il puntatore del mouse sul blocco di rete, fare clic e tenere premuto il punto in cui la linea tocca il blocco di rete, trascinarlo in un blocco macchina e rilasciarlo.

Quando si creano le linee di connessione, si noti che il codice di rete viene aggiunto automaticamente alle macchine nell'editor.



8 Aggiungere la richiesta di input dell'utente.

In alcune posizioni, l'infrastruttura dell'esempio è stata configurata per più opzioni. Ad esempio:

- Ambienti della zona cloud per lo sviluppo, il test e la produzione
- Mappature delle caratteristiche per le macchine piccole, medie e grandi

È possibile impostare un'opzione specifica direttamente nel modello cloud, ma un approccio migliore consiste nel permettere all'utente di selezionare l'opzione al momento della distribuzione del modello. La richiesta di input dell'utente consente di creare un modello che può essere distribuito in molti modi, anziché avere molti modelli hardcoded.

- a Creare una sezione `inputs` nel codice, in modo che gli utenti possano selezionare la dimensione della macchina e l'ambiente di destinazione al momento della distribuzione. Definire i valori selezionabili:

```
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
```

- b Nella sezione `resources` del codice, aggiungere il codice `${input.input-name}` per richiedere la selezione dell'utente:

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
  DBTier:
    type: Cloud.Machine
    properties:
      name: mysql
      image: ubuntu
      flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
```

```
        - network: '${resource["WP-Network-Private"].id}'  
WP-Network-Private:  
  type: Cloud.Network  
  properties:  
    name: WP-Network-Private  
    networkType: existing
```

- 9 Infine, migliorare il codice `WebTier` e `DBTier` utilizzando i seguenti esempi. Il codice `WP-Network-Private` non richiede modifiche aggiuntive.

Si noti che i miglioramenti includono l'accesso al server del database e gli script di inizializzazione `cloudConfig` in fase di distribuzione.

Componente	Esempio
Input DBTier aggiuntivi	<pre> username: type: string minLength: 4 maxLength: 20 pattern: '[a-z]+' title: Database Username description: Database Username userpassword: type: string pattern: '[a-z0-9A-Z@#]+\$' encrypted: true title: Database Password description: Database Password </pre>
Risorsa DBTier	<pre> DBTier: type: Cloud.Machine properties: name: mysql image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.userpassword}' cloudConfig: #cloud-config repo_update: true repo_upgrade: all packages: - mysql-server runcmd: - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/ mysql.cnf - service mysql restart - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';" - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';" - mysql -e "FLUSH PRIVILEGES;" attachedDisks: [] </pre>
Risorsa WebTier	<pre> WebTier: type: Cloud.Machine properties: name: wordpress image: ubuntu flavor: '\${input.size}' constraints: - tag: '\${input.env}' networks: - network: '\${resource["WP-Network-Private"].id}' assignPublicIpAddress: true cloudConfig: </pre>

Componente	Esempio
	<pre> #cloud-config repo_update: true repo_upgrade: all packages: - apache2 - php - php-mysql - libapache2-mod-php - mysql-client - gcc - make - autoconf - libc-dev - pkg-config - libmcrypt-dev - php-pear - php-dev runcmd: - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/ latest.tar.gz -C /var/www/html/mywordpresssite --strip-components 1 - i=0; while [\$i -le 10]; do mysql --connect-timeout=3 -h \$ {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break sleep 15; i=\$((i+1)); done - mysql -u root -pmysqlpassword -h \${DBTier.networks[0].address} -e "create database wordpress_blog;" - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/ html/mywordpresssite/wp-config.php - pecl channel-update pecl.php.net - pecl update-channels - pecl install mcrypt - sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME', 'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD', 'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '\${DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp- config.php - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini - service apache2 reload </pre>

Esempio: Esempio di codice del modello cloud di base completato

```

formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
  title: Environment
  description: Target Environment
size:
  type: string

```



```

enum:
  - small
  - medium
  - large
description: Size of Nodes
title: Tier Machine Size
username:
  type: string
  minLength: 4
  maxLength: 20
  pattern: '[a-z]+'
  title: Database Username
  description: Database Username
userpassword:
  type: string
  pattern: '[a-z0-9A-Z@#]+$'
  encrypted: true
  title: Database Password
  description: Database Password
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      constraints:
        - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - apache2
        - php
        - php-mysql
        - libapache2-mod-php
        - mysql-client
        - gcc
        - make
        - autoconf
        - libc-dev
        - pkg-config
        - libmccrypt-dev
        - php-pear
        - php-dev
      runcmd:
        - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
        https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
        mywordpresssite --strip-components 1
        - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
        {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;

```

```

i=$((i+1)); done
    - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
wordpress_blog;"
    - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/mywordpresssite/
wp-config.php
    - pecl channel-update pecl.php.net
    - pecl update-channels
    - pecl install mcrypt
    - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
${DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
    - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini
    - service apache2 reload
DBTier:
  type: Cloud.Machine
  properties:
    name: mysql
    image: ubuntu
    flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
  networks:
    - network: '${resource["WP-Network-Private"].id}'
      assignPublicIpAddress: true
  remoteAccess:
    authentication: usernamePassword
    username: '${input.username}'
    password: '${input.userpassword}'
  cloudConfig: |
    #cloud-config
    repo_update: true
    repo_upgrade: all
    packages:
      - mysql-server
    runcmd:
      - sed -e '/bind-address/ s/^#*#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
      - service mysql restart
      - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
      - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%;'"
      - mysql -e "FLUSH PRIVILEGES;"
  attachedDisks: []
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing

```

Operazioni successive

Testare il modello cloud controllando la sintassi e distribuirlo.

Test di un modello cloud di base

Durante la progettazione, è spesso necessario creare un modello cloud iniziando dalle basi, quindi distribuire e testare con la crescita del modello. In questo esempio vengono illustrato alcuni dei test in corso integrati in Cloud Assembly.

Per avere la certezza che una distribuzione funzioni nel modo desiderato, è possibile testare e distribuire più volte il modello cloud. Gradualmente, si aggiungono altre risorse, si testano nuovamente e si ridistribuiscono nel corso della procedura.

Prerequisiti

Creare il modello cloud di base. Vedere [Creazione un modello cloud di base](#).

Procedura

- 1 Fare clic su **Modelli cloud** e aprire il modello cloud WordPress-BP.

Viene visualizzato il modello cloud di base, nella tela di progettazione e nell'editor di codice.

- 2 Per verificare la sintassi, il posizionamento e la validità di base del modello, fare clic su **Prova** in basso a sinistra.
- 3 Immettere i valori di input e fare clic su **Prova**.

Testing Basic

Environment: env:dev

Tier Machine Size: small

Database Username: ouradmin

Database Password:

CANCEL TEST

Il test è solo una simulazione: in realtà non distribuisce macchine virtuali o altre risorse.

Test Result for Basic

Successful This simulation only tests syntax, placement and basic validity

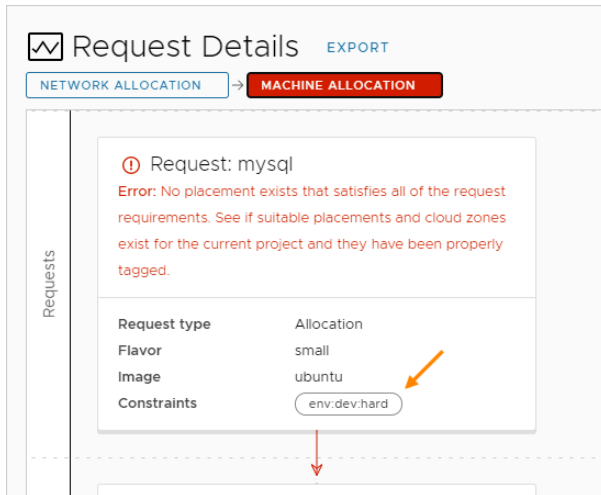
3 Infos Provisioning Diagram

WP-Network-Private ✓
LINE 96

DBTier ✓
LINE 69

WebTier ✓

Il test include un collegamento a un **Diagramma di provisioning**, in cui è possibile esaminare il flusso di distribuzione simulato e visualizzare cosa si è verificato. La simulazione espone i potenziali problemi, ad esempio la mancata disponibilità di funzionalità di risorse definite che corrispondono ai vincoli hard nel modello cloud. Nell'errore di esempio seguente, una zona cloud con tag di funzionalità `env:dev` non è stata trovata in alcuna parte dell'infrastruttura definita.



Una simulazione corretta non garantisce che sia possibile distribuire il modello senza errori.

- 4 Dopo che il modello ha superato la simulazione, fare clic su **Distribuisci** in basso a sinistra.
- 5 Selezionare **Crea una nuova distribuzione**.
- 6 Denominare la distribuzione **WordPress for OurCo** e fare clic su **Avanti**.
- 7 Immettere i valori di input e fare clic su **Distribuisci**.
- 8 Per verificare che il modello sia stato distribuito correttamente, cercare in **Risorse > Distribuzioni**.

Se una distribuzione non riesce, fare clic sul relativo nome e fare clic sulla scheda **Cronologia** per visualizzare i messaggi che consentono di risolvere i problemi.

Timestamp	Status	Resource type	Resource name
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Machine	WebTier
Sep 8, 2020, 1...	CREATE_FINISHED	Cloud.Machine	DBTier
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Machine	DBTier
Sep 8, 2020, 1...	CREATE_FINISHED	Cloud.Network	WP-Network-Private
Sep 8, 2020, 1...	CREATE_IN_PROGRESS	Cloud.Network	WP-Network-Private

Alcune voci della cronologia potrebbero presentare un collegamento **Diagramma di provisioning** all'estrema destra. Il diagramma è simile a quello simulato, in cui si ispeziona il diagramma di flusso dei punti decisionali di Cloud Assembly nel processo di provisioning.

Altri diagrammi di flusso sono disponibili in **Infrastruttura > Attività > Richieste**.

- 9 Per verificare che l'applicazione funzioni, aprire la pagina iniziale di WordPress in un browser.

- a Attendere che i server di WordPress siano completamente creati e inizializzati.

L'inizializzazione potrebbe richiedere più di 30 minuti, a seconda dell'ambiente.

- b Per individuare il FQDN o l'indirizzo IP del sito, andare in **Risorse > Distribuzioni > Topologia**.

- c Nella tela, fare clic su WebTier e trovare l'indirizzo IP nel pannello a destra.

- d Immettere l'indirizzo IP come parte dell'URL completo della pagina iniziale di WordPress.

In questo esempio, l'URL completo è:

`http://{IP-address}/mywordpresssite`

o

`http://{IP-address}/mywordpresssite/wp-admin/install.php`

- 10 Dopo aver esaminato WordPress in un browser, se l'applicazione richiede altre operazioni, apportare modifiche al modello e ridistribuire utilizzando l'opzione **Aggiorna una distribuzione esistente**.

- 11 Prendere in considerazione il controllo delle versioni del modello cloud. È possibile ripristinare una versione funzionante se una modifica causa un errore di distribuzione.

- a Nella pagina di progettazione del modello cloud, fare clic su **Versione**.

- b Nella pagina Creazione della versione, immettere **WP-1.0**.

Non immettere spazi nei nomi delle versioni.

- c Fare clic su **Crea**.

Per rivedere o ripristinare una versione, nella pagina di progettazione fare clic sulla scheda **Cronologia versioni**.

- 12 Con una distribuzione di base ora possibile, provare il primo miglioramento in fase di distribuzione aumentando CPU e memoria nei server dell'applicazione e nel server di database.

Aggiornare entrambi a una dimensione media del nodo. Utilizzando lo stesso modello, selezionare **Medio** al momento della distribuzione, ridistribuire e verificare nuovamente l'applicazione.

Operazioni successive

Espandere il modello cloud in un'applicazione adatta alla produzione aggiungendo ancora più risorse.

Espansione di un modello cloud

Dopo aver creato e testato un modello di Cloud Assembly di base per l'applicazione di esempio, è possibile espanderlo in un'applicazione a più livelli distribuibile allo sviluppo, al test e infine alla produzione.

Per espandere il modello cloud, aggiungere i seguenti miglioramenti.

- Un'opzione per i server applicazioni cluster per una maggiore capacità
- Una rete e un bilanciamento del carico rivolti al pubblico davanti ai server applicazioni
- Un server di backup con storage

Prerequisiti

Creare il modello cloud di base e testarlo. Vedere [Creazione un modello cloud di base](#) e [Test di un modello cloud di base](#).

Procedura

- 1 Fare clic su **Modelli cloud** e aprire il modello cloud WordPress-BP.

Viene visualizzato il modello di base, nella tela di progettazione e nell'editor di codice.

- 2 Apportare aggiunte e modifiche, utilizzando l'esempio di codice e la figura come guida.

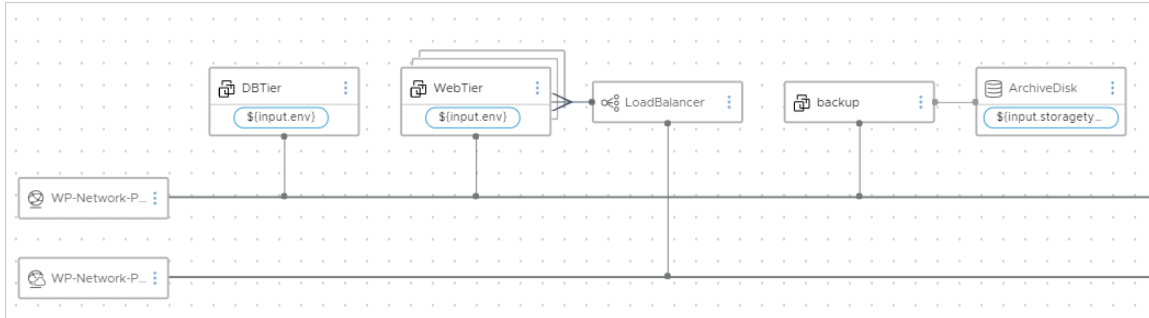
È possibile utilizzare la GUI per trascinare nuove risorse nella tela, ad esempio il bilanciamento del carico, quindi terminare la configurazione nell'editor di codice.

- a Aggiungere una richiesta di input `count` per inserire il server applicazioni WordPress in un cluster.
- b Aggiungere un bilanciamento del carico indipendente dal cloud.
- c connettere il bilanciamento del carico al cluster del server applicazioni WordPress.
- d Aggiungere una macchina di backup indipendente dal cloud.
- e Connettere la macchina di backup alla rete privata/interna.
- f Aggiungere una rete pubblica/esterna indipendente dal cloud.
- g Connettere il bilanciamento del carico alla rete pubblica.
- h Aggiungere un volume di storage indipendente dal cloud da utilizzare come disco di archivio.
- i Connettere il disco di archivio alla macchina di backup.
- j Aggiungere una richiesta di input per la velocità del disco di archiviazione.

3 Distribuire, testare e apportare modifiche nello stesso modo del modello cloud di base.

È possibile aggiornare le distribuzioni esistenti o anche distribuire nuove istanze in modo da poter confrontare le distribuzioni.

L'obiettivo è ottenere un modello coerente e ripetibile che possa essere utilizzato per le distribuzioni di produzione.



Esempio: Esempio di codice del modello cloud di base espanso

```
formatVersion: 1
inputs:
  env:
    type: string
    enum:
      - env:dev
      - env:prod
      - env:test
    default: env:dev
    title: Environment
    description: Target Environment
  size:
    type: string
    enum:
      - small
      - medium
      - large
    description: Size of Nodes
    title: Tier Machine Size
  username:
    type: string
    minLength: 4
    maxLength: 20
    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#]+$'
    encrypted: true
```

```

    title: Database Password
    description: Database Password
  count:
    type: integer
    default: 2
    maximum: 5
    minimum: 2
    title: WordPress Cluster Size
    description: WordPress Cluster Size (Number of Nodes)
  storagetype:
    type: string
    enum:
      - storage:general
      - storage:fast
    description: Archive Storage Disk Type
    title: Archive Disk Type
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      image: ubuntu
      flavor: '${input.size}'
      count: '${input.count}'
      constraints:
        - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - apache2
        - php
        - php-mysql
        - libapache2-mod-php
        - mysql-client
        - gcc
        - make
        - autoconf
        - libc-dev
        - pkg-config
        - libmccrypt-dev
        - php-pear
        - php-dev
      runcmd:
        - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
        https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
        mywordpresssite --strip-components 1
        - i=0; while [ $i -le 10 ]; do mysql --connect-timeout=3 -h $
        {DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
        i=$((i+1)); done
        - mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database

```



```

wordpress_blog;"
  - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/mywordpresssite/
wp-config.php
  - pecl channel-update pecl.php.net
  - pecl update-channels
  - pecl install mcrypt
  - sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
{DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
  - sed -i '950i extension=mcrypt.so' /etc/php/7.4/apache2/php.ini
  - service apache2 reload
DBTier:
  type: Cloud.Machine
  properties:
    name: mysql
    image: ubuntu
    flavor: '${input.size}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    remoteAccess:
      authentication: usernamePassword
      username: '${input.username}'
      password: '${input.userpassword}'
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - mysql-server
      runcmd:
        - sed -e '/bind-address/ s/^#*#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
        - service mysql restart
        - mysql -e "CREATE USER 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
        - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%';"
        - mysql -e "FLUSH PRIVILEGES;"
    attachedDisks: []
LoadBalancer:
  type: Cloud.LoadBalancer
  properties:
    name: myapp-lb
    network: '${resource["WP-Network-Public"].id}'
    instances:
      - '${WebTier.id}'
    routes:
      - protocol: HTTP
        port: '80'
        instanceProtocol: HTTP

```

```

    instancePort: '80'
    healthCheckConfiguration:
      protocol: HTTP
      port: '80'
      urlPath: /mywordpresssite/wp-admin/install.php
      intervalSeconds: 6
      timeoutSeconds: 5
      unhealthyThreshold: 2
      healthyThreshold: 2
    internetFacing: true
WP-Network-Private:
  type: Cloud.Network
  properties:
    name: WP-Network-Private
    networkType: existing
WP-Network-Public:
  type: Cloud.Network
  properties:
    name: WP-Network-Public
    networkType: public
backup:
  type: Cloud.Machine
  properties:
    name: backup
    flavor: '${input.size}'
    image: ubuntu
    networks:
      - network: '${resource["WP-Network-Private"].id}'
    attachedDisks:
      - source: '${resource.ArchiveDisk.id}'
ArchiveDisk:
  type: Cloud.Volume
  properties:
    name: ArchiveDisk
    capacityGb: 5
    constraints:
      - tag: '${input.storagetype}'

```

Operazioni successive

Definire la propria infrastruttura e creare i propri modelli cloud.

Vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#) e [Capitolo 6 Progettazione delle distribuzioni di Cloud Assembly](#).

Tutorial: configurazione di VMware Cloud on AWS per vRealize Automation

Questo tutorial di vRealize Automation illustra il processo di definizione dell'infrastruttura delle risorse e delle impostazioni del modello cloud per la distribuzione in un ambiente VMware Cloud on AWS.

La procedura richiede che un amministratore del cloud abbia già configurato il data center SDDC di VMware Cloud on AWS dell'organizzazione come descritto in *Distribuzione e gestione di un data center definito da software* nella [documentazione della guida rapida di VMware Cloud on AWS](#).

Esaminare la configurazione sequenziale per comprendere il processo di configurazione dell'ambiente per VMware Cloud on AWS. Tenere presente che i valori visualizzati sono solo esempi di casi d'uso. Valutare dove apportare le proprie sostituzioni o utilizzare i valori di esempio per adattarsi alle proprie esigenze di distribuzione e infrastruttura cloud.



Per informazioni correlate, vedere il video sulla [configurazione di VMware Cloud on AWS per Cloud Assembly](#).

Procedura

1 [Configurazione di un workflow di VMware Cloud on AWS di base in vRealize Automation](#)

Questo caso d'uso mostra il processo di definizione dell'infrastruttura delle risorse e di un modello cloud corrispondente per la distribuzione in un ambiente VMware Cloud on AWS.

2 [Configurazione di una rete isolata in un workflow di VMware Cloud on AWS in vRealize Automation](#)

Questa procedura consente di aggiungere una rete isolata per la distribuzione di VMware Cloud on AWS in vRealize Automation.

Configurazione di un workflow di VMware Cloud on AWS di base in vRealize Automation

Questo caso d'uso mostra il processo di definizione dell'infrastruttura delle risorse e di un modello cloud corrispondente per la distribuzione in un ambiente VMware Cloud on AWS.

Questa procedura consente di configurare l'infrastruttura che supporta la distribuzione del modello cloud alle risorse nell'ambiente VMware Cloud on AWS esistente.

Prerequisiti

- Prima di poter creare e configurare un account cloud VMware Cloud on AWS in Cloud Assembly, è necessario far parte di un'organizzazione in un ambiente SDDC VMware Cloud on AWS esistente. Per informazioni sulla configurazione del servizio VMware Cloud on AWS, vedere [Documentazione di VMware Cloud on AWS](#).

- Per semplificare la connessione necessaria tra l'SDDC dell'host di VMware Cloud on AWS esistente in vCenter e un account cloud di VMware Cloud on AWS in Cloud Assembly, è necessario fornire una connessione di rete e aggiungere regole del firewall, utilizzando una VPN o strumenti di rete simili. Vedere [Preparazione dell'SDDC di VMware Cloud on AWS per la connessione con gli account cloud di VMware Cloud on AWS in vRealize Automation](#).

Procedura

1 [Preparazione dell'SDDC di VMware Cloud on AWS per la connessione con gli account cloud di VMware Cloud on AWS in vRealize Automation](#)

Quando si utilizzano account cloud di VMware Cloud on AWS nell'ambiente vRealize Automation è necessario creare una connessione di rete e configurare regole per supportare la comunicazione tra l'SDDC in vCenter e gli account cloud di VMware Cloud on AWS in vRealize Automation.

2 [Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio](#)

In questo passaggio si crea un account cloud di VMware Cloud on AWS in vRealize Automation.

3 [Creazione di una zona cloud per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#)

In questo passaggio viene creata una zona cloud per specificare una risorsa di elaborazione a cui l'utente CloudAdmin può accedere quando lavora con VMware Cloud on AWS in vRealize Automation.

4 [Configurazione dei profili di rete e di storage per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#)

In questo passaggio si configura un profilo di rete e un profilo di storage per specificare le risorse disponibili per un utente CloudAdmin di VMware Cloud on AWS in vRealize Automation.

5 [Creazione di un progetto per supportare le distribuzioni di VMware Cloud on AWS in vRealize Automation](#)

In questo passaggio si definisce un progetto di vRealize Automation che può essere utilizzato per controllare le risorse disponibili per le distribuzioni di VMware Cloud on AWS.

6 [Definizione di un risorsa di macchine di vCenter in una progettazione del modello cloud per supportare la distribuzione di VMware Cloud on AWS in vRealize Automation](#)

In questo passaggio, si trascina una risorsa di macchine di vCenter in una tela di progettazione e si aggiungono impostazioni per una distribuzione di VMware Cloud on AWS in vRealize Automation.

Preparazione dell'SDDC di VMware Cloud on AWS per la connessione con gli account cloud di VMware Cloud on AWS in vRealize Automation

Quando si utilizzano account cloud di VMware Cloud on AWS nell'ambiente vRealize Automation è necessario creare una connessione di rete e configurare regole per supportare la comunicazione tra l'SDDC in vCenter e gli account cloud di VMware Cloud on AWS in vRealize Automation.

Configurare le connessioni e le regole necessarie per supportare la comunicazione dell'SDDC.

Per semplificare la connessione necessaria tra l'SDDC dell'host di VMware Cloud on AWS esistente in vCenter e un account cloud di VMware Cloud on AWS in vRealize Automation, è necessario fornire una connessione di rete tra i due elementi utilizzando una VPN o strumenti di rete simili.

- 1 Configurare una connessione VPN su Internet pubblico o AWS Direct Connect.

Vedere le informazioni sulla configurazione della connettività VPN al data center locale e sulla configurazione di AWS Direct Connect per VMware Cloud on AWS in *Networking e sicurezza di VMware Cloud on AWS* nella [documentazione di VMware Cloud on AWS](#).

- 2 Verificare che il nome di dominio completo di vCenter Server sia risolvibile in un indirizzo IP privato nella rete di gestione.

Vedere le informazioni sull'impostazione dell'indirizzo di risoluzione FQDN vCenter Server in *Networking e sicurezza di VMware Cloud on AWS* nella [documentazione di VMware Cloud on AWS](#).

- 3 Configurare le regole del firewall necessarie.

È necessario configurare le regole del firewall del gateway di gestione nella console VMware Cloud on AWS di SDDC per supportare la comunicazione. Le regole devono trovarsi nella sezione delle regole del firewall di **Gateway di gestione**. Creare le regole del firewall utilizzando le opzioni nella scheda **Networking e sicurezza** nella console dell'SDDC.

- Limitare il traffico di rete verso ESXi per i servizi HTTPS (TCP 443) all'indirizzo IP individuato dell'appliance/server di vRealize Automation o del VIP del bilanciamento del carico di vRealize Automation.
- Limitare il traffico di rete verso vCenter per i servizi ICMP (tutti gli ICMP), SSO (TCP 7444) e HTTPS (TCP 443) all'indirizzo IP individuato dell'appliance/server di vRealize Automation o del VIP del bilanciamento del carico di vRealize Automation.
- Limitare il traffico di rete verso NSX-T Manager per i servizi HTTPS (TCP 443) all'indirizzo IP individuato dell'appliance/server di vRealize Automation o del VIP del bilanciamento del carico di vRealize Automation.

Le regole del firewall richieste sono riepilogate nella tabella seguente.

Tabella 2-2. Riepilogo delle regole del firewall del gateway di gestione necessarie

Nome	Origine	Destinazione	Servizio
vCenter	Blocco CIDR del data center locale	vCenter	Qualsiasi (tutto il traffico)
vCenter Ping	Qualsiasi	vCenter	ICMP (tutti gli ICMP)
NSX Manager	Blocco CIDR del data center locale	NSX Manager	Qualsiasi (tutto il traffico)
On premises to ESXi ping	Blocco CIDR del data center locale	Solo gestione ESXi	ICMP (tutti gli ICMP)
On Premises to ESXi remote console and provisioning	Blocco CIDR del data center locale	Solo gestione ESXi	TCP 902
On-premises to SDDC VM	Blocco CIDR del data center locale	Blocco CIDR della rete logica SDDC	Qualsiasi (tutto il traffico)
SDDC VM to on premises	Blocco CIDR della rete logica SDDC	Blocco CIDR del data center locale	Qualsiasi (tutto il traffico)

Per informazioni correlate, vedere *Networking e sicurezza di VMware Cloud on AWS* e *Guida operativa di VMware Cloud on AWS* nella [documentazione di VMware Cloud on AWS](#).

Dopo aver configurato l'accesso gateway e le regole firewall richieste, è possibile continuare con il processo di creazione di un account cloud di VMware Cloud on AWS. Vedere [Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio](#).

Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio

In questo passaggio si crea un account cloud di VMware Cloud on AWS in vRealize Automation.

Per informazioni correlate, vedere [Documentazione di VMware Cloud on AWS](#).

Prerequisiti

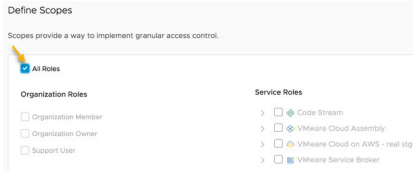
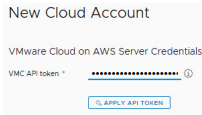
- Questa procedura presuppone che si disponga delle credenziali di amministratore richieste, tra cui le credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter e che sia stato abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Questa procedura presuppone che si disponga del ruolo di utente amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Per semplificare la connessione necessaria tra l'SDDC dell'host di VMware Cloud on AWS esistente in vCenter e un account cloud di VMware Cloud on AWS in vRealize Automation, è

necessario fornire una connessione di rete e aggiungere regole del firewall, utilizzando una VPN o strumenti di rete simili. Vedere [Preparazione dell'SDDC di VMware Cloud on AWS per la connessione con gli account cloud di VMware Cloud on AWS in vRealize Automation](#). Se si utilizza un proxy Internet HTTP esterno, è necessario configurarlo per IPv4.

- Se non si dispone di accesso a Internet esterno, configurare un server proxy Internet. Vedere [Come configurare un server proxy Internet per vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud**.
- 2 Fare clic su **Aggiungi account cloud**, selezionare VMware Cloud on AWS e immettere i valori. La tabella seguente include valori di esempio e informazioni di supporto.

Impostazione	Valore e istruzione di esempio	Descrizione
Token API VMC	<ol style="list-style-type: none"> Fare clic sull'icona della guida <i>i</i> alla fine della riga Token API VMC e fare clic sulla pagina Token API nella casella di testo della Guida per aprire la scheda Token API nella pagina Il mio account dell'organizzazione. Fare clic su Genera token per visualizzare l'opzione Genera nuovo token API. Immettere un nuovo nome di token, ad esempio myinitials_mytoken. Impostare il TTL del token in modo che non scada mai. Se si crea un token impostato per la scadenza, le operazioni di VMware Cloud on AWS da vRealize Automation verranno interrotte quando il token scade e continueranno a non essere eseguite finché non si aggiorna l'account cloud con un nuovo token. Nella sezione Definisci ambiti, selezionare Tutti i ruoli.  Fare clic su Genera. Nella pagina del token generato, fare clic su Copia e fare clic su Continua. Tornare alla pagina Nuovo account cloud, incollare il token copiato nella riga Token API VMC e fare clic su Applica token API.  	<p>È possibile creare un nuovo token o utilizzare un token esistente per l'organizzazione nella pagina Token API collegata.</p> <p>Nella sezione Definisci ambiti, i ruoli minimi richiesti per il token API sono:</p> <ul style="list-style-type: none"> ■ Ruoli organizzativi <ul style="list-style-type: none"> ■ Membro dell'organizzazione ■ Proprietario dell'organizzazione ■ Ruoli servizio - VMware Cloud on AWS <ul style="list-style-type: none"> ■ Amministratore ■ Amministratore di NSX Cloud ■ Auditor di NSX Cloud <p>Nota Copiare, scaricare o stampare il token generato. Se si esce da questa pagina, non è possibile recuperare il token generato.</p> <p>Applicare il token generato o fornito per connettersi all'ambiente SDDC disponibile nella sottoscrizione di VMware Cloud on AWS dell'organizzazione e popolare l'elenco dei nomi di SDDC.</p> <p>Se i servizi vRealize Automation e VMware Cloud on AWS si trovano in organizzazioni diverse, è necessario passare all'organizzazione di VMware Cloud on AWS e quindi generare il token.</p> <p>Per ulteriori informazioni sui token API, vedere Generazione di token API.</p>
Nome SDDC	<p>Per questo esempio, selezionare Datacenter:Datacenter-abz.</p> <p>Il nome SDDC valido compila automaticamente le voci dei nomi di dominio completo di vCenter e NSX-T.</p> <p>Se un proxy cloud è già stato distribuito nell'SDDC, anche il valore del proxy cloud viene compilato automaticamente.</p>	<p>Selezionare dall'elenco di SDDC disponibili dalla propria sottoscrizione di VMware Cloud on AWS. L'elenco di SDDC è basato sul token API VMware Cloud on AWS.</p> <p>Gli SDDC di NSX-V non sono supportati con vRealize Automation e non sono presenti nell'elenco di SDDC disponibili.</p>

Impostazione	Valore e istruzione di esempio	Descrizione
Indirizzo IP/nome di dominio completo di vCenter	L'indirizzo viene popolato automaticamente in base alla selezione di SDDC.	<p>Immettere l'indirizzo IP o il nome di dominio completo di vCenter Server nell'SDDC specificato.</p> <p>L'indirizzo IP predefinito è impostato in maniera predefinita all'indirizzo IP privato. In base al tipo di connettività di rete utilizzata per accedere all'SDDC, l'indirizzo predefinito può essere diverso dall'indirizzo IP del server di NSX Manager nell'SDDC specificato.</p>
Indirizzo IP/nome di dominio completo di NSX Manager	L'indirizzo viene popolato automaticamente in base alla selezione di SDDC.	<p>Specifica l'indirizzo IP o il nome di dominio completo di NSX Manager nell'SDDC specificato.</p> <p>L'indirizzo IP predefinito è impostato in maniera predefinita all'indirizzo IP privato. In base al tipo di connettività di rete utilizzata per accedere all'SDDC, l'indirizzo predefinito può essere diverso dall'indirizzo IP del server di NSX Manager nell'SDDC specificato.</p> <p>Gli account cloud di VMware Cloud on AWS supportano NSX-T.</p>
Nome utente e password di vCenter	Il nome utente viene popolato automaticamente come cloudadmin@vmc.local.	<p>Immettere il nome utente di vCenter per l'SDDC specificato se è diverso da quello predefinito.</p> <p>L'utente specificato richiede le credenziali CloudAdmin. L'utente non richiede le credenziali CloudGlobalAdmin.</p> <p>Immettere la password dell'utente.</p>
Convalida	<p>Fare clic su Convalida.</p> <p>Se si riceve un <code>Error updating endpoint <Nome>: Endpoint already exists</code>, un account cloud è già stato associato a tale SDDC.</p>	L'azione di convalida conferma i diritti di accesso al vCenter specificato e verifica che il vCenter sia in esecuzione.
Nome e descrizione	<p>Immettere OurCo-VMC come nome dell'account cloud.</p> <p>Immettere Esempio di distribuzione per VMC come descrizione dell'account cloud.</p>	
Consenti provisioning a questi data center	Queste informazioni sono di sola lettura.	Elenca i data center disponibili nell'ambiente SDDC di VMware Cloud on AWS specificato.

Impostazione	Valore e istruzione di esempio	Descrizione
Creare una zona cloud	Deselezionare la casella di controllo. Per questo esempio si creerà una zona cloud in un secondo momento nel workflow.	Vedere Ulteriori informazioni sulle zone cloud di Cloud Assembly .
Tag di funzionalità	Lasciare vuoto. Questo workflow non utilizza tag di funzionalità.	Utilizzare i tag in base alla strategia di tag dell'organizzazione. Vedere Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly e Creazione di una strategia di assegnazione dei tag .

Come per le macchine virtuali distribuite in vSphere, è possibile configurare i tag delle macchine per una macchina virtuale da distribuire in VMware Cloud on AWS. È inoltre possibile aggiornare il tag della macchina dopo la distribuzione iniziale. Questi tag della macchina consentono a vRealize Automation di assegnare dinamicamente una macchina virtuale a un gruppo di sicurezza di NSX-T appropriato durante la distribuzione. Per informazioni correlate, vedere [Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation](#).

3 Fare clic su **Aggiungi**.

Risultati

I dati di risorse come macchine e volumi vengono raccolte dal data center dell'SDDC di VMware Cloud on AWS ed elencate nella sezione **Risorse** della scheda vRealize Automation **Infrastruttura**.

Operazioni successive

[Creazione di una zona cloud per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#).

Creazione di una zona cloud per le distribuzioni di VMware Cloud on AWS in vRealize Automation

In questo passaggio viene creata una zona cloud per specificare una risorsa di elaborazione a cui l'utente CloudAdmin può accedere quando lavora con VMware Cloud on AWS in vRealize Automation.

In VMware Cloud on AWS le due credenziali di amministratore principali sono CloudGlobalAdmin e CloudAdmin. Cloud Assembly è progettato per supportare l'utente CloudAdmin. Distribuire alle risorse disponibili per un utente CloudAdmin di VMware Cloud on AWS. Non distribuire alle risorse che richiedono credenziali CloudGlobalAdmin di VMware Cloud on AWS.

Le zone cloud identificano le risorse di elaborazione in cui il modello cloud di un progetto distribuisce macchine, reti e storage. Vedere [Ulteriori informazioni sulle zone cloud di Cloud Assembly](#).

Se non indicato diversamente, i valori dei passaggi immessi in questa procedura sono validi solo per questo workflow di esempio.

Prerequisiti

- Completare la procedura [Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio](#).
- Questa procedura presuppone che si disponga delle credenziali di amministratore richieste, tra cui le credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Questa procedura presuppone che si disponga del ruolo di utente amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

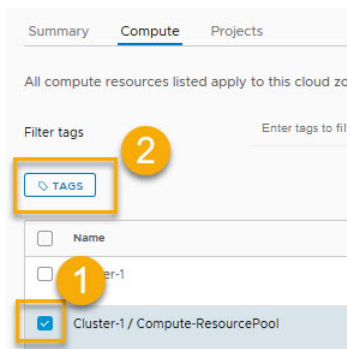
Procedura

- 1 Selezionare **Infrastruttura > Configura > Zone cloud**.
- 2 Fare clic su **Nuova zona cloud** e immettere i valori per l'ambiente VMware Cloud on AWS.

Impostazione	Valore di esempio
Account/Regione	OurCo-VMC / Datacenter:Datacenter-abz Questi sono l'account cloud e la regione associata definiti nel passaggio precedente, Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio .
Nome	VMC_cloud_zone-1
Descrizione	Solo risorse di VMware Cloud on AWS
Criterio di posizionamento	Predefinito
Tag di funzionalità	Lasciare vuoto. Questo workflow non utilizza tag di funzionalità.

- 3 Fare clic sulla scheda **Risorse di elaborazione**.
- 4 Come illustrato nell'area 1 seguente, trovare e selezionare una risorsa di elaborazione disponibile per l'utente CloudAdmin. Per questo esempio, utilizzare la risorsa denominata Cluster 1/ Compute-ResourcePool.

Cluster 1/ Compute-ResourcePool è la risorsa di elaborazione predefinita per VMware Cloud on AWS.



- 5 Come mostrato nell'area 2 precedente, aggiungere il nome del tag `vmc_placements_abz`.

Tags

1 object(s) selected

Add tags

Remove tags

no tags ⓘ

- 6 Filtrare le risorse di elaborazione utilizzate in questa zona cloud immettendo `vmc_placements_abz` nella sezione **Tag filtro**.

- 7 Fare clic su **Salva**.

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	Cluster-1		Cluster	
<input checked="" type="checkbox"/>	Cluster-1 / Compute-ResourcePool	OurCo-VMC / SDDC_test1_abz	ResourcePool	vmc_placements_abz
<input type="checkbox"/>	Cluster-1 / Mgmt-ResourcePool		ResourcePool	

1 ⓘ

Per questo esempio, solo la risorsa di elaborazione denominata Cluster 1/ Compute-ResourcePool è disponibile per l'utente CloudAdmin.

Operazioni successive

[Configurazione dei profili di rete e di storage per le distribuzioni di VMware Cloud on AWS in vRealize Automation.](#)

Configurazione dei profili di rete e di storage per le distribuzioni di VMware Cloud on AWS in vRealize Automation

In questo passaggio si configura un profilo di rete e un profilo di storage per specificare le risorse disponibili per un utente CloudAdmin di VMware Cloud on AWS in vRealize Automation.

Anche se sono necessari un valore di immagini e un valore di caratteristica, non sono valori univoci specifici per le credenziali dell'utente di VMware Cloud on AWS. Per questo esempio si utilizzerà un valore di caratteristica di `small` e un valore di immagine di `ubuntu-16` quando si definisce il modello cloud.

Per informazioni generali sulle mappature e sui profili, vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).

Se non indicato diversamente, i valori dei passaggi immessi in questa procedura sono validi solo per questo workflow di esempio.

Prerequisiti

- Creare una zona cloud. Vedere [Creazione di una zona cloud per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#).

- Questa procedura presuppone che si disponga delle credenziali di amministratore richieste, tra cui le credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Questa procedura presuppone che si disponga del ruolo di utente amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

Procedura

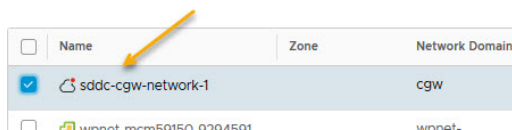
1 Definire un profilo di rete per le distribuzioni di VMware Cloud on AWS.

- a Selezionare **Infrastruttura > Configura > Profili di rete** e fare clic su **Nuovo profilo di rete**.

Impostazione	Valore di esempio
Account/Regione	OurCo-VMC / Datacenter:Datacenter-abz
	Nota Selezionare l'account cloud di VMware Cloud on AWS e il data center SDDC corrispondente creato in Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio .
Nome	vmc-network1
Descrizione	Contiene le reti alle quali possono accedere gli amministratori dei modelli cloud che dispongono delle credenziali CloudAdmin di VMware Cloud on AWS.

- b Fare clic sulla scheda **Rete** e su **Aggiungi rete**.
- c Selezionare una rete su cui un utente di VMware Cloud on AWS con credenziali CloudAdmin può distribuire, ad esempio `sddc-cgw-network-1`.

Add Network



<input type="checkbox"/>	Name	Zone	Network Domain
<input checked="" type="checkbox"/>	sddc-cgw-network-1		cgw
<input type="checkbox"/>	winnet-nom50150-0704501		winnet-

2 Salvare il profilo di rete.

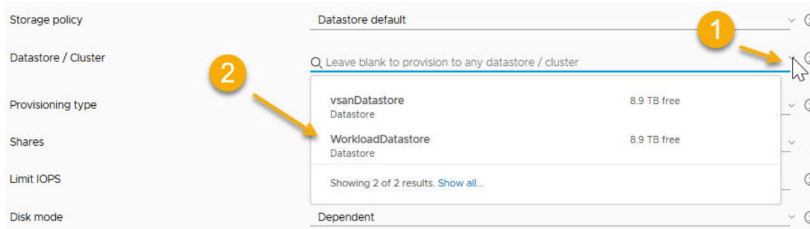
3 Definire un profilo di storage per le distribuzioni di VMware Cloud on AWS.

Configurare un profilo di storage con un datastore/cluster come destinazione, accessibile all'utente CloudAdmin.

- a Selezionare **Infrastruttura > Configura > Profili di storage** e fare clic su **Nuovo profilo di storage**.

Impostazione	Valore di esempio
Account/Regione	OurCo-VMC / Datacenter:Datacenter-abz Selezionare l'account cloud di VMware Cloud on AWS e il data center SDDC corrispondente creato in Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio .
Nome	vmc-storage1
Descrizione	Contiene il cluster di datastore che può essere distribuito dagli amministratori dei modelli cloud che dispongono di credenziali CloudAdmin di VMware Cloud on AWS.

- b Dal menu a discesa **Datastore/cluster**, selezionare il datastore **WorkloadDatastore**.



Per VMware Cloud on AWS nel Cloud Assembly, il criterio di storage deve utilizzare il datastore **WorkloadDatastore** per supportare la distribuzione di VMware Cloud on AWS.

4 Salvare il profilo di storage.

Operazioni successive

[Creazione di un progetto per supportare le distribuzioni di VMware Cloud on AWS in vRealize Automation.](#)

Creazione di un progetto per supportare le distribuzioni di VMware Cloud on AWS in vRealize Automation

In questo passaggio si definisce un progetto di vRealize Automation che può essere utilizzato per controllare le risorse disponibili per le distribuzioni di VMware Cloud on AWS.

Per informazioni sui progetti, vedere [Come funzionano i progetti di Cloud Assembly al momento della distribuzione](#).

Se non indicato diversamente, i valori dei passaggi immessi in questa procedura sono validi solo per questo workflow di esempio.

Prerequisiti

- Completare la procedura [Configurazione dei profili di rete e di storage per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#).
- Questa procedura presuppone che si disponga delle credenziali di amministratore richieste, tra cui le credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Questa procedura presuppone che si disponga del ruolo di utente amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Amministrazione > Progetti**.
- 2 Fare clic su **Nuovo progetto** e immettere il nome del progetto VMC_proj-1_abz.
- 3 Fare clic su **Utenti** e su **Aggiungi utenti**.

Gli utenti hanno bisogno delle credenziali CloudAdmin per la sottoscrizione di VMware Cloud on AWS della propria organizzazione.

- chris.gray@ourco.com, amministratore
- kerry.white@ourco.com, membro

- 4 Fare clic su **Provisioning**, quindi fare clic su **Aggiungi zona cloud**.
- 5 Aggiungere la zona cloud configurata nel passaggio precedente.

Impostazione	Valore di esempio
Zona cloud	VMC_cloud_zone-1 Questa zona cloud è stata creata nel passaggio precedente, Creazione di una zona cloud per le distribuzioni di VMware Cloud on AWS in vRealize Automation .
Priorità di provisioning	1
Limite di istanze	3

- 6 Per questo esempio, ignorare le altre opzioni.

Operazioni successive

Creare un modello cloud da distribuire nell'ambiente VMware Cloud on AWS. Vedere [Definizione di un risorsa di macchine di vCenter in una progettazione del modello cloud per supportare la distribuzione di VMware Cloud on AWS in vRealize Automation](#).

Definizione di un risorsa di macchine di vCenter in una progettazione del modello cloud per supportare la distribuzione di VMware Cloud on AWS in vRealize Automation

In questo passaggio, si trascina una risorsa di macchine di vCenter in una tela di progettazione e si aggiungono impostazioni per una distribuzione di VMware Cloud on AWS in vRealize Automation.

Creare una progettazione del modello cloud che è possibile distribuire alle risorse di VMware Cloud on AWS disponibili.

Se non indicato diversamente, i valori dei passaggi immessi in questa procedura sono validi solo per questo workflow di esempio.

Prerequisiti

- Questa procedura presuppone che si disponga delle credenziali di progettista di modelli cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Questa procedura presuppone che si disponga delle credenziali di VMware Cloud on AWS CloudAdmin per l'SDDC di destinazione in vCenter (Datacenter:Datacenter-abz). Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Configurare l'infrastruttura della risorsa e il progetto come descritto nelle sezioni precedenti.

Procedura

- 1 Fare clic sulla scheda **Progettazione**, quindi fare clic su **Nuovo**.

Impostazione	Valore di esempio
Nome	vmc-bp_abz
Descrizione	1
Progetto	VMC_proj-1_abz Questo è il progetto creato in precedenza, che supporta la zona cloud anch'essa creata in precedenza. Il progetto è ora associato alla zona cloud, che a sua volta è associata all'account cloud/regione di VMware Cloud on AWS creato in precedenza.

- 2 Far scorrere una risorsa di macchine di vSphere nella tela.
- 3 Modificare il seguente codice della risorsa del modello cloud (grassetto) nella risorsa di macchine.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
```



```
image: ubuntu-1604
cpuCount: 1
totalMemoryMB: 1024
folderName: Workloads
```

image può essere qualsiasi valore appropriato per le esigenze di distribuzione.

È necessario aggiungere l'istruzione `folderName: Workloads` al codice di progettazione del modello cloud per supportare la distribuzione di VMware Cloud on AWS. L'impostazione `folderName: Workloads` supporta le credenziali di CloudAdmin nell'ambiente SDDC di VMware Cloud on AWS ed è obbligatoria.

Nota: sebbene l'impostazione `folderName: Workloads` mostrata nell'esempio di codice precedente sia obbligatoria, è possibile aggiungerla direttamente nel codice di progettazione del modello cloud come mostrato in precedenza, oppure aggiungerla nella zona cloud o nel progetto associato. Se l'impostazione è specificata in più di una di queste tre posizioni, la precedenza è la seguente:

- L'impostazione del progetto sostituisce l'impostazione di progettazione del modello cloud e l'impostazione della zona cloud.
- L'impostazione di progettazione del modello cloud sostituisce l'impostazione della zona cloud.

Nota: facoltativamente, è possibile sostituire le impostazioni `cpuCount` e `totalMemoryMB` con una voce `flavor` (dimensionamento), come illustrato di seguito:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu-1604
      flavor: small
      folderName: Workloads
```

Se nella zona cloud il valore della cartella è impostato su **Carichi di lavoro**, non è necessario impostare la proprietà `folderName` nella progettazione del modello cloud, a meno che non si desideri sovrascrivere il valore della cartella della zona cloud.

Operazioni successive

Espandere il workflow di base di VMware Cloud on AWS aggiungendo l'isolamento della rete. Vedere [Configurazione di una rete isolata in un workflow di VMware Cloud on AWS in vRealize Automation](#).

Configurazione di una rete isolata in un workflow di VMware Cloud on AWS in vRealize Automation

Questa procedura consente di aggiungere una rete isolata per la distribuzione di VMware Cloud on AWS in vRealize Automation.

Quando si definisce l'account cloud di VMware Cloud on AWS, sono disponibili le impostazioni di NSX-T configurate nel servizio VMware Cloud on AWS. Per informazioni sulla configurazione delle impostazioni di NSX-T nel servizio VMware Cloud on AWS, vedere la [documentazione del prodotto](#) di VMware Cloud on AWS.

vRealize Automation supporta VMware Cloud on AWS con NSX-T. Non supporta VMware Cloud on AWS con NSX-V.

vRealize Automation supporta l'isolamento di rete per le distribuzioni di VMware Cloud on AWS. Non supporta altri metodi di rete per VMware Cloud on AWS.

Questa estensione del workflow di base di VMware Cloud on AWS descrive i seguenti metodi di creazione di una rete isolata da utilizzare nel modello cloud:

- Configurare l'isolamento basato su rete su richiesta.
- Configurare l'isolamento basato su gruppo di sicurezza su richiesta.

Prerequisiti

Questa procedura si espande nel workflow di base di VMware Cloud on AWS. Utilizza lo stesso account cloud e il profilo di regione, zona cloud, progetto e rete configurati nel workflow di [Tutorial: configurazione di VMware Cloud on AWS per vRealize Automation](#).

Procedura

1 [Definizione di una rete isolata per una distribuzione di VMware Cloud on AWS in vRealize Automation](#)

È possibile configurare l'isolamento di rete per una distribuzione di VMware Cloud on AWS utilizzando una delle seguenti procedure:

2 [Definizione di un componente di rete in un modello cloud per supportare l'isolamento della rete per VMware Cloud on AWS nel vRealize Automation](#)

In questo passaggio si trascina un componente della macchina di rete su una tela di un modello cloud di vRealize Automation e si aggiungono le impostazioni per una distribuzione di rete isolata all'ambiente VMware Cloud on AWS di destinazione.

Definizione di una rete isolata per una distribuzione di VMware Cloud on AWS in vRealize Automation

È possibile configurare l'isolamento di rete per una distribuzione di VMware Cloud on AWS utilizzando una delle seguenti procedure:

- [Configurazione dell'isolamento basato su rete su richiesta in vRealize Automation](#)

- [Configurazione dell'isolamento basato su gruppi di sicurezza su richiesta in vRealize Automation](#)

Configurazione dell'isolamento basato su rete su richiesta in vRealize Automation

È possibile configurare l'isolamento di rete per le esigenze di distribuzione di VMware Cloud on AWS specificando e utilizzando le impostazioni di rete su richiesta in un profilo di rete.

È possibile specificare una rete isolata utilizzando un gruppo di sicurezza o le impostazioni di rete su richiesta. In questo esempio si configura l'isolamento della rete specificando impostazioni di rete su richiesta nel profilo di rete. In seguito, si accede alla rete in un modello cloud e si utilizza tale modello cloud in una distribuzione di VMware Cloud on AWS.

Se non indicato diversamente, i valori dei passaggi immessi in questa procedura sono validi solo per questo workflow di esempio.

Prerequisiti

- Completare il workflow di [Configurazione di un workflow di VMware Cloud on AWS di base in vRealize Automation](#).
- Rivedere [Configurazione di una rete isolata in un workflow di VMware Cloud on AWS in vRealize Automation](#).
- Questa procedura presuppone che si disponga delle credenziali di amministratore richieste, tra cui le credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Questa procedura presuppone che si disponga del ruolo di utente amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

Procedura

- 1 Aprire il profilo di rete utilizzato nel workflow di base di VMware Cloud on AWS, ad esempio `vmc-network1`. Vedere [Configurazione dei profili di rete e di storage per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#).
- 2 Non è necessario effettuare alcuna selezione nella scheda **Reti**.
- 3 Fare clic sulla scheda **Criteri di rete**.
- 4 Selezionare l'opzione **Crea una rete su richiesta** e selezionare il dominio di rete di `cgw` predefinito. Specificare una dimensione appropriata di CIDR e subnet.
- 5 Fare clic su **Salva**.

Quando si utilizza questo profilo di rete, le macchine vengono distribuite in una rete nel dominio di rete predefinito. La rete è isolata dalle altre reti mediante l'accesso alla rete privata o in uscita.

Operazioni successive

Configurare un componente di rete nel modello cloud. Vedere [Definizione di un componente di rete in un modello cloud per supportare l'isolamento della rete per VMware Cloud on AWS nel vRealize Automation](#).

Configurazione dell'isolamento basato su gruppi di sicurezza su richiesta in vRealize Automation

È possibile configurare l'isolamento di rete per le esigenze di distribuzione di VMware Cloud on AWS specificando e utilizzando un gruppo di sicurezza su richiesta in un profilo di rete.

È possibile specificare una rete isolata utilizzando un gruppo di sicurezza o le impostazioni di rete su richiesta. In questo esempio si configura l'isolamento della rete specificando un gruppo di sicurezza su richiesta nel profilo di rete. In seguito, si specifica la rete in un modello cloud e si utilizza tale modello cloud in una distribuzione di VMware Cloud on AWS.

Se non indicato diversamente, i valori dei passaggi immessi in questa procedura sono validi solo per questo workflow di esempio.

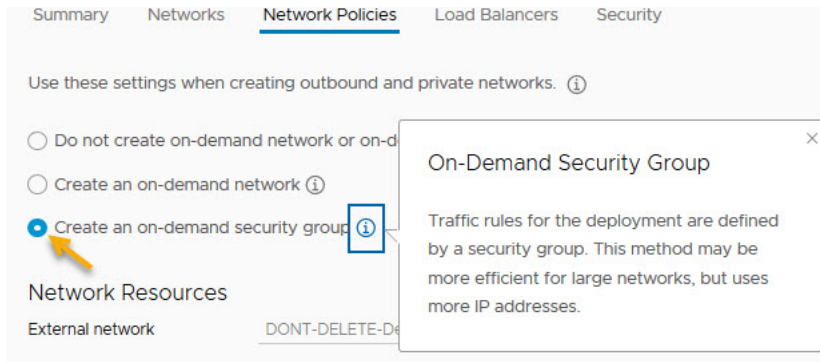
Prerequisiti

- Completare il workflow di [Configurazione di un workflow di VMware Cloud on AWS di base in vRealize Automation](#).
- Rivedere [Configurazione di una rete isolata in un workflow di VMware Cloud on AWS in vRealize Automation](#).
- Questa procedura presuppone che si disponga delle credenziali di amministratore richieste, tra cui le credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Questa procedura presuppone che si disponga del ruolo di utente amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

Procedura

- 1 Aprire il profilo di rete utilizzato nel workflow di base di VMware Cloud on AWS, ad esempio `vmc-network1`. Vedere [Configurazione dei profili di rete e di storage per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#).
- 2 Selezionare la rete esistente utilizzata nel workflow di base di VMware Cloud on AWS, ad esempio `sddc-cgw-network-1`. Vedere [Configurazione dei profili di rete e di storage per le distribuzioni di VMware Cloud on AWS in vRealize Automation](#).
- 3 Fare clic sulla scheda **Criteri di rete**.

4 Selezionare l'opzione **Crea un gruppo di sicurezza su richiesta**.



5 Fare clic su **Salva**.

Quando si utilizza questo profilo di rete, le macchine vengono distribuite nella rete selezionata e sono isolate da un nuovo criterio del gruppo di sicurezza. Il nuovo criterio di sicurezza consente l'accesso alla rete privata o in uscita.

Operazioni successive

Configurare un componente di rete nel modello cloud. Vedere [Definizione di un componente di rete in un modello cloud per supportare l'isolamento della rete per VMware Cloud on AWS nel vRealize Automation](#).

Definizione di un componente di rete in un modello cloud per supportare l'isolamento della rete per VMware Cloud on AWS nel vRealize Automation

In questo passaggio si trascina un componente della macchina di rete su una tela di un modello cloud di vRealize Automation e si aggiungono le impostazioni per una distribuzione di rete isolata all'ambiente VMware Cloud on AWS di destinazione.

Aggiungere l'isolamento della rete al modello cloud creato in precedenza. Il modello cloud è già associato a un progetto e a una zona cloud che supportano la distribuzione nell'ambiente VMware Cloud on AWS, nonché al profilo di rete e alla rete configurati per l'isolamento.

Se non indicato diversamente, i valori dei passaggi immessi in questa procedura sono validi solo per questo workflow di esempio.

Prerequisiti

- Completare la procedura [Configurazione dell'isolamento basato su gruppi di sicurezza su richiesta in vRealize Automation](#) o [Configurazione dell'isolamento basato su rete su richiesta in vRealize Automation](#).
- Questa procedura presuppone che si disponga delle credenziali di progettista di modelli cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Questa procedura presuppone che si disponga delle credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).

Procedura

- 1 Aprire il modello cloud creato nel workflow precedente. Vedere [Definizione di un risorsa di macchine di vCenter in una progettazione del modello cloud per supportare la distribuzione di VMware Cloud on AWS in vRealize Automation](#).
- 2 Dai componenti a sinistra della pagina di progettazione del modello cloud, trascinare un componente di rete nella tela.
- 3 Modificare il codice YAML del componente di rete per specificare un tipo di rete `private` o `outbound`, come mostrato in grassetto.

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: private
```

OPPURE

```
resources: Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: vmc_isolated
    networkType: outbound
```

Operazioni successive

Ora è possibile distribuire o chiudere il modello cloud.

Tutorial: configurazione dell'integrazione di un provider IPAM esterno specifico del provider per vRealize Automation

È possibile utilizzare un provider IPAM esterno per gestire le assegnazioni degli indirizzi IP per le distribuzioni di modelli cloud. In questo tutorial viene descritto come configurare l'integrazione del provider IPAM esterno in vRealize Automation utilizzando Infoblox come provider IPAM esterno.

In questa procedura, si utilizza un pacchetto del provider IPAM esistente, in questo caso un pacchetto Infoblox e un ambiente in esecuzione esistente per creare un punto di integrazione IPAM specifico del provider. È possibile configurare una rete esistente e creare un profilo di rete per supportare l'allocazione degli indirizzi IP dal provider IPAM esterno. Infine, si crea un modello cloud abbinato alla rete e al profilo di rete e si distribuiscono macchine in rete utilizzando i valori IP ottenuti dal provider IPAM esterno.

Le informazioni su come ottenere e configurare il pacchetto del provider IPAM e su come configurare un ambiente in esecuzione che accede a un proxy di estensibilità cloud per supportare l'integrazione del provider IPAM, sono incluse come riferimento.

I valori visualizzati in questo workflow di esempio sono esemplificativi. Non sarà possibile utilizzarli alla lettera nel proprio ambiente. Valutare dove apportare le sostituzioni in base alle esigenze della propria organizzazione.



Per fare riferimento a uno scenario di vRealize Automation simile che illustra con un video un workflow di integrazione Infoblox IPAM, vedere il video sull'[integrazione di Infoblox IPAM plug-in con vRealize Automation o vRealize Automation Cloud](#).

Procedura

1 [Aggiunta degli attributi estendibili obbligatori nell'applicazione Infoblox per l'integrazione con vRealize Automation](#)

Prima di poter scaricare e distribuire il pacchetto del provider Infoblox (`infoblox.zip`) per l'integrazione con vRealize Automation dal sito Web Infoblox o da VMware Marketplace, è necessario aggiungere gli attributi di estendibilità obbligatori in Infoblox.

2 [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#)

Prima di poter definire un punto di integrazione IPAM esterno in vRealize Automation, è necessario un pacchetto del provider IPAM configurato.

3 [Creazione di un ambiente in esecuzione per un punto di integrazione IPAM in vRealize Automation](#)

Prima di poter definire un punto di integrazione IPAM esterno in vRealize Automation, è necessario creare o accedere a un ambiente in esecuzione esistente che funga da intermediario tra il provider IPAM e vRealize Automation. L'ambiente in esecuzione è in genere un account cloud di Amazon Web Services o Microsoft Azure o un punto di integrazione locale di estendibilità basata su azioni associato a un proxy di estendibilità cloud.

4 [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#)

vRealize Automation supporta l'integrazione con un provider IPAM esterno. In questo esempio viene utilizzato Infoblox come provider IPAM esterno.

5 [Configurazione di una rete e di un profilo di rete per l'utilizzo di un IPAM esterno per una rete esistente in vRealize Automation](#)

È possibile definire una rete esistente per utilizzare valori degli indirizzi IP ottenuti e gestiti da un provider IPAM esterno anziché internamente da vRealize Automation.

6 [Definizione e distribuzione di un modello cloud che utilizza l'assegnazione dell'intervallo del provider IPAM esterno in vRealize Automation](#)

È possibile definire un modello cloud per ottenere e gestire le assegnazioni degli indirizzi IP dal provider IPAM esterno. In questo esempio viene utilizzato Infoblox come provider IPAM esterno.

7 Utilizzo delle proprietà specifiche di Infoblox e attributi estendibili per le integrazioni IPAM nei modelli cloud di vRealize Automation

È possibile utilizzare le proprietà specifiche di Infoblox per i progetti di vRealize Automation che contengono integrazioni IPAM esterne per Infoblox.

8 Controllo della raccolta dei dati di rete mediante filtri Infoblox in vRealize Automation

Per Infoblox, è possibile limitare il numero di reti in cui vengono raccolti i dati alle sole reti necessarie per le operazioni di vRealize Automation. In questo modo è possibile ridurre la quantità di dati trasferiti e migliorare le prestazioni del sistema.

Aggiunta degli attributi estendibili obbligatori nell'applicazione Infoblox per l'integrazione con vRealize Automation

Prima di poter scaricare e distribuire il pacchetto del provider Infoblox (`infoblox.zip`) per l'integrazione con vRealize Automation dal sito Web Infoblox o da VMware Marketplace, è necessario aggiungere gli attributi di estendibilità obbligatori in Infoblox.

Questa procedura è applicabile se si sta creando un punto di integrazione IPAM esterno per l'integrazione di Infoblox con Cloud Assembly.

Prima di poter utilizzare il download del file `infoblox.zip`, è necessario accedere al proprio account Infoblox, utilizzando le credenziali di amministratore dell'account dell'organizzazione e creare innanzitutto i seguenti attributi estendibili di Infoblox:

- VMware NIC index
- VMware resource ID

Prerequisiti

- Verificare di disporre di un account con [Infoblox](#) e delle credenziali di accesso corrette per l'account Infoblox dell'organizzazione.
- Verificare che la versione di Infoblox WAPI sia supportata. L'integrazione di IPAM con Infoblox dipende da Infoblox WAPI versione v2.7 di Infoblox. Le appliance Infoblox che supportano WAPI v2.7 sono supportate.
- Rivedere [Utilizzo delle proprietà specifiche di Infoblox e attributi estendibili per le integrazioni IPAM nei modelli cloud di vRealize Automation](#).

Procedura

- 1 Accedere all'account Infoblox utilizzando le credenziali di amministratore.

Queste sono le stesse credenziali di nome utente e password dell'amministratore specificate quando si crea un punto di integrazione IPAM esterno in Cloud Assembly utilizzando la sequenza di menu **Infrastruttura > Connessioni > Integrazioni > .**

- 2 Utilizzare la procedura descritta nella documentazione di Infoblox per creare i seguenti attributi estendibili obbligatori nell'applicazione Infoblox.

- VMware NIC index - Tipo Integer

- VMware resource ID - Tipo String

La procedura è descritta nella sezione *Adding Extensible Attributes* (Aggiunta degli attributi estendibili) dell'argomento della documentazione di Infoblox [About Extensible Attributes](#) (Informazioni sugli attributi estendibili). Vedere anche [Managing Extensible Attributes](#) (Gestione degli attributi estendibili).

Operazioni successive

Dopo aver aggiunto gli attributi obbligatori, è possibile riprendere il processo di download e distribuzione del pacchetto Infoblox come descritto in [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation

Prima di poter definire un punto di integrazione IPAM esterno in vRealize Automation, è necessario un pacchetto del provider IPAM configurato.

È possibile scaricare un pacchetto di integrazione specifico del provider dal sito Web del provider IPAM o da [VMware Marketplace](#).

Nota In questo esempio viene utilizzato il file `Infoblox.zip` del pacchetto Infoblox fornito da VMware, disponibile per il download da [VMware Marketplace](#) nel modo seguente:

- [Plug-in Infoblox versione 1.4](#): compatibile con vRealize Automation versione 8.3- 8.7 e fornisce tutte le funzionalità delle versioni precedenti. Con questa versione, è possibile utilizzare lo stesso nome host con un suffisso DNS diverso per due schede NIC. Per informazioni dettagliate aggiuntive, vedere le note di rilascio del plug-in.
- [Plug-in Infoblox versione 1.3](#): compatibile con vRealize Automation 8.3.x e fornisce ulteriori filtri per la raccolta dei dati di rete. Vedere [Controllo della raccolta dei dati di rete mediante filtri Infoblox in vRealize Automation](#). Se si utilizza vRealize Automation 8.3.x, è possibile utilizzare il plug-in Infoblox 1.4 per sfruttare funzionalità aggiuntive.

Il [plug-in Infoblox v1.3](#) può essere utilizzato con vRealize Automation 8.1 o 8.2, ma solo in alcuni casi e con cautela, come descritto nell'articolo della Knowledge Base [Compatibilità di Infoblox 1.3 con vRealize Automation 8.x \(82142\)](#).

- [Plug-in vRA Cloud Infoblox versione 1.2](#): compatibile con vRealize Automation 8.1.x e 8.2.x
- [Plug-in vRA Cloud Infoblox versione 1.1](#): compatibile con vRealize Automation 8.1.x
- [Plug-in vRA Cloud Infoblox versione 1.0](#): compatibile con vRealize Automation 8.0.1.x con o senza una connessione Internet alla rete globale.
- [Plug-in vRA Cloud Infoblox versione 0.4](#): compatibile con vRealize Automation 8.0.0.x e 8.0.1.x quando è presente una connessione Internet alla rete globale.

L'integrazione di IPAM con Infoblox dipende da Infoblox WAPI versione v2.7 di Infoblox. Tutte le appliance Infoblox che supportano WAPI v2.7 sono supportate.

Per informazioni su come creare un pacchetto di integrazione IPAM per altri provider IPAM, se non ne esiste già uno in [VMware Marketplace](#), vedere [Come utilizzare l'SDK IPAM per creare un pacchetto di integrazione IPAM esterno specifico del provider per vRealize Automation](#).

Il pacchetto del provider IPAM contiene script insieme a metadati e altre configurazioni. Gli script contengono il codice sorgente utilizzato per le operazioni eseguite da vRealize Automation in coordinamento con il provider IPAM esterno. Le operazioni di esempio includono `Allocate an IP address for a virtual machine`, `Fetch a list of IP ranges from the provider` e `Update the MAC address of a host record in the provider`.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre di un account con il provider IPAM esterno, ad esempio [Infoblox](#) o [Bluecat](#) e di disporre delle credenziali di accesso corrette per l'account dell'organizzazione con il provider IPAM.
- Se si utilizza Infoblox come provider IPAM esterno, verificare di aver aggiunto gli attributi estendibili necessari all'account Infoblox prima di continuare. Vedere [Aggiunta degli attributi estendibili obbligatori nell'applicazione Infoblox per l'integrazione con vRealize Automation](#).

Nota Esiste un problema della catena di certificati relativo al modo in cui l'elemento Python nel plug-in Infoblox gestisce i handshake SSL. Per informazioni sul problema e le azioni richieste per risolvere il problema, consultare l'articolo della Knowledge Base [Il plug-in vRA Cloud Infoblox genera un errore della catena di certificati durante il processo di autenticazione \(88057\)](#).

Procedura

- 1 Andare alla pagina di download corretta per il plug-in Infoblox. Per i collegamenti a una versione specifica del plug-in Infoblox, vedere sopra.

Per le opzioni del plug-in Infoblox disponibili nel [VMware Marketplace](#), vedere sopra.
- 2 Accedere e scaricare il pacchetto del plug-in.
- 3 Se non è già stato fatto, aggiungere gli attributi estendibili richiesti in Infoblox. Vedere [Aggiunta degli attributi estendibili obbligatori nell'applicazione Infoblox per l'integrazione con vRealize Automation](#).

Risultati

Il pacchetto è ora disponibile per la distribuzione mediante la sequenza di menu **Integrazioni > Aggiungi integrazione > IPAM > Gestisci provider > Importa pacchetto** come descritto in [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#).

Creazione di un ambiente in esecuzione per un punto di integrazione IPAM in vRealize Automation

Prima di poter definire un punto di integrazione IPAM esterno in vRealize Automation, è necessario creare o accedere a un ambiente in esecuzione esistente che funga da intermediario tra il provider IPAM e vRealize Automation. L'ambiente in esecuzione è in genere un account cloud di Amazon Web Services o Microsoft Azure o un punto di integrazione locale di estendibilità basata su azioni associato a un proxy di estendibilità cloud.

L'integrazione IPAM esterna richiede un ambiente in esecuzione. Quando si definisce il punto di integrazione IPAM, si crea una connessione tra Cloud Assembly e il provider IPAM specificando un ambiente in esecuzione disponibile.

L'integrazione IPAM utilizza una serie di script o plug-in specifici del provider scaricati in un ambiente in esecuzione facilitato da un provider FaaS (Feature-As-a-Services), ad esempio Amazon Web Services Lambda, le funzioni di Microsoft Azure o un punto di integrazione incorporato locale di estendibilità basata su azioni (ABX). L'ambiente in esecuzione viene utilizzato per connettersi al provider IPAM esterno, ad esempio Infoblox.

Nota Un punto di integrazione IPAM di Infoblox richiede un punto di integrazione incorporato locale di estendibilità basata su azioni (ABX).

Ogni tipo di ambiente di runtime presenta vantaggi e svantaggi:

- Un punto di integrazione di estendibilità basata su azioni (ABX):
 - è gratuito, senza costi aggiuntivi per l'utilizzo del fornitore.
 - può connettersi alle appliance del fornitore IPAM che si trovano in un data center locale protetto da una regola NAT o un firewall che non è accessibile pubblicamente, ad esempio Infoblox.
 - è più lento e ha leggermente meno prestazioni disponibili rispetto a un cloud commerciale.
- Amazon Web Services
 - prevede costi di utilizzo/connessione FaaS da parte del fornitore.
 - non può connettersi alle appliance del fornitore IPAM che si trovano in un data center locale protetto da una regola NAT o un firewall che non è accessibile pubblicamente.
 - ha prestazioni veloci ed estremamente affidabili.
- Microsoft Azure
 - prevede costi di utilizzo/connessione FaaS da parte del fornitore.
 - non può connettersi alle appliance del fornitore IPAM che si trovano in un data center locale protetto da una regola NAT o un firewall che non è accessibile pubblicamente.
 - ha prestazioni veloci ed estremamente affidabili.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre di un account con il provider IPAM esterno, ad esempio [Infoblox](#) o [Bluecat](#) e di disporre delle credenziali di accesso corrette per l'account dell'organizzazione con il provider IPAM.
- Verificare di disporre dell'accesso a un pacchetto di integrazione distribuito per il provider IPAM, ad esempio Infoblox o BlueCat. Il pacchetto distribuito viene inizialmente ottenuto come download ZIP dal sito Web del provider IPAM o da [VMware Marketplace](#) e quindi distribuito in Cloud Assembly.

Per informazioni su come distribuire il file ZIP del pacchetto del provider e renderlo disponibile come valore di **Provider** nella pagina Integrazione IPAM, vedere [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

Procedura

- 1 Per creare un'azione di estendibilità basata su FaaS locale da utilizzare come ambiente in esecuzione dell'integrazione IPAM, selezionare **Estendibilità > Libreria > Azioni**.
- 2 Fare clic su **Nuova azione**, immettere un nome e una descrizione per l'azione e specificare un progetto.
- 3 Nel menu a discesa **Provider FaaS**, selezionare **Locale**.
- 4 Compilare il modulo per definire l'azione di estendibilità.

Per ulteriori informazioni sulla creazione delle azioni di estendibilità, vedere [Estensione e automazione dei cicli di vita delle applicazioni con l'estendibilità](#).



Per informazioni relative all'ambiente in esecuzione, guardare questo video sull'[integrazione di Infoblox IPAM plug-in](#) nel blog al minuto 24 circa.

Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation

vRealize Automation supporta l'integrazione con un provider IPAM esterno. In questo esempio viene utilizzato Infoblox come provider IPAM esterno.

È possibile utilizzare un punto di integrazione IPAM specifico del provider per ottenere e gestire gli indirizzi IP e le caratteristiche di rete correlate per le distribuzioni dei modelli cloud.

In questo esempio viene creato un punto di integrazione IPAM esterno per supportare l'accesso all'account dell'organizzazione con un provider IPAM esterno. In questo workflow di esempio, il provider IPAM è Infoblox e il pacchetto di integrazione specifico del provider esiste già. Sebbene queste istruzioni siano specifiche per un'integrazione di Infoblox, possono essere utilizzate come riferimento se si crea un'integrazione IPAM per un altro provider IPAM esterno.

È possibile ottenere un pacchetto di integrazione specifico del provider dal sito Web del provider IPAM o da [VMware Marketplace](#).

In questo esempio viene utilizzato il file `Infoblox.zip` del pacchetto Infoblox fornito da VMware, disponibile per il download da [VMware Marketplace](#). Per informazioni sulle versioni più recenti del plug-in di Infoblox disponibili in [VMware Marketplace](#), vedere [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

Prerequisiti

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre di un account con un provider IPAM esterno e delle credenziali di accesso corrette per l'account dell'organizzazione con il provider IPAM.
- Verificare di poter accedere a un pacchetto di integrazione distribuito per il provider IPAM. Il pacchetto distribuito viene inizialmente ottenuto come download in formato ZIP dal sito Web del provider IPAM o da VMware Solutions Exchange Marketplace e quindi distribuito in vRealize Automation.

Per informazioni su come scaricare e distribuire il file ZIP del pacchetto del provider e renderlo disponibile come valore **Provider** nella pagina Integrazione IPAM, vedere [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

- Verificare di disporre dell'accesso a un ambiente in esecuzione configurato per il provider IPAM. L'ambiente in esecuzione è in genere un punto di integrazione incorporato locale di estendibilità basata su azioni (ABX).

Per informazioni sulle caratteristiche dell'ambiente in esecuzione, vedere [Creazione di un ambiente in esecuzione per un punto di integrazione IPAM in vRealize Automation](#).

- Selezionare gli attributi estendibili obbligatori nell'applicazione Infoblox. Vedere [Aggiunta degli attributi estendibili obbligatori nell'applicazione Infoblox per l'integrazione con vRealize Automation](#).
- Se non si dispone di accesso a Internet esterno, è possibile configurare un server proxy Internet. Vedere [Come configurare un server proxy Internet per vRealize Automation](#).
- Verificare di disporre delle credenziali utente necessarie per accedere e utilizzare il prodotto Infoblox IPAM. Ad esempio, aprire la scheda Amministrazione nell'appliance Infoblox e personalizzare le voci di amministratore, gruppi e ruoli. È necessario essere

membri di un gruppo con autorizzazioni di amministratore o superuser o di un gruppo personalizzato con autorizzazioni DHCP, DNS, IPAM e Grid. Queste impostazioni consentono di accedere a tutte le funzionalità disponibili nel plug-in Infoblox, consentendo di creare un'integrazione di Infoblox IPAM e ai progettisti di utilizzare tale integrazione IPAM in modelli cloud e distribuzioni. Per ulteriori informazioni sulle autorizzazioni degli utenti, vedere la documentazione del prodotto Infoblox.

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Fare clic su **IPAM**.
- 3 Nel menu a discesa **Provider**, selezionare nell'elenco un pacchetto del provider IPAM configurato, ad esempio *Infoblox_hrg*.

Se l'elenco è vuoto, fare clic su **Importa pacchetto del provider**, passare a un file ZIP del pacchetto del provider esistente e selezionarlo. Se non si dispone del file ZIP del provider, è possibile ottenerlo dal sito Web del provider IPAM o da [VMware Marketplace](#).

Per informazioni su come distribuire il file ZIP del pacchetto del provider in vCenter e renderlo disponibile come valore **Provider** nella pagina Integrazione, vedere [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

Per informazioni su come aggiornare un'integrazione IPAM esistente per utilizzare una versione più recente del pacchetto di integrazione IPAM del fornitore, vedere [Come eseguire l'aggiornamento a un pacchetto di integrazione IPAM esterno più recente in vRealize Automation](#).

- 4 Immettere il nome utente e la password dell'amministratore per il proprio account con il provider IPAM esterno, insieme a tutti gli altri campi obbligatori (se presenti), ad esempio il nome host del provider.

In questo esempio il nome host del provider IPAM Infoblox viene ottenuto tramite i passaggi seguenti:

- a In una scheda del browser separata, accedere all'account del provider IPAM utilizzando le credenziali dell'amministratore di Infoblox.
- b Copiare l'URL del nome host.
- c Incollare l'URL del nome host nel campo **Nome host** nella pagina Integrazione IPAM.

- 5 Nell'elenco a discesa **Ambiente in esecuzione**, selezionare un punto di integrazione locale di estendibilità basata su azioni, ad esempio *Infoblox_abx_intg*.

L'ambiente in esecuzione supporta la comunicazione tra vRealize Automation e il provider IPAM esterno.

Nota Se si utilizza un account cloud di Amazon Web Services o Microsoft Azure come ambiente in esecuzione dell'integrazione, assicurarsi che l'appliance del provider IPAM sia accessibile da Internet e non sia protetta da una regola NAT o un firewall e che disponga di un nome DNS risolvibile pubblicamente. Se il provider IPAM non è accessibile, le funzioni di Amazon Web Services Lambda o Microsoft Azure non possono connettersi e l'integrazione non riuscirà. Per informazioni correlate, vedere [Creazione di un ambiente in esecuzione per un punto di integrazione IPAM in vRealize Automation](#).

Il framework IPAM supporta solo un ambiente in esecuzione incorporato locale di estendibilità basata su azioni (ABX).

Nota Un punto di integrazione IPAM di Infoblox richiede un punto di integrazione incorporato locale di estendibilità basata su azioni (ABX).

L'account cloud o il punto di integrazione configurato consente la comunicazione tra vRealize Automation e il provider IPAM, in questo esempio Infoblox, tramite un proxy di estendibilità cloud associato. È possibile selezionare un provider già creato oppure crearne uno.

Per informazioni su come creare un ambiente in esecuzione, vedere [Creazione di un ambiente in esecuzione per un punto di integrazione IPAM in vRealize Automation](#).

- 6 Fare clic su **Convalida**.

Poiché in questo esempio viene utilizzata l'integrazione di estendibilità basata su azioni locale per l'ambiente in esecuzione, è possibile visualizzare l'azione di convalida.

- a Fare clic sulla scheda **Estendibilità**.
- b Fare clic su **Attività > Esecuzioni di azione** e selezionare **Tutte le esecuzioni** o **Esecuzioni dell'integrazione** dal filtro per verificare che un'azione di convalida dell'endpoint sia avviata e in esecuzione.

- 7 Quando viene richiesto di considerare attendibile il certificato autofirmato dal provider IPAM, fare clic su **Accetta**.

Dopo aver accettato il certificato autofirmato, l'azione di convalida può continuare fino al completamento.

- 8 Immettere un **Nome** per questo punto di integrazione IPAM, ad esempio *Infoblox_Integration*, e una **Descrizione**, ad esempio *Infoblox IPAM with ABX integration for team HRG*.

9 Fare clic su **Aggiungi** per salvare il nuovo punto di integrazione IPAM esterno.

Viene imitata un'azione di raccolta dati. Le reti e gli intervalli IP sono dati raccolti dal provider IPAM. È possibile visualizzare l'azione di raccolta dati come segue:

- a Fare clic sulla scheda **Estendibilità**.
- b Fare clic su **Attività > Esecuzioni di azione** e verificare che un'azione di raccolta dati sia avviata e in esecuzione. È possibile aprire e visualizzare il contenuto dell'esecuzione di azione.

Risultati

L'integrazione IPAM esterna specifica del provider è ora disponibile per l'utilizzo con reti e profili di rete.

Configurazione di una rete e di un profilo di rete per l'utilizzo di un IPAM esterno per una rete esistente in vRealize Automation

È possibile definire una rete esistente per utilizzare valori degli indirizzi IP ottenuti e gestiti da un provider IPAM esterno anziché internamente da vRealize Automation.

È possibile definire una rete per accedere alle impostazioni IP esistenti definite nell'account del provider IPAM esterno dell'organizzazione. Questo passaggio si espande nell'integrazione del provider Infoblox creata nel passaggio precedente.

In questo esempio, viene configurato un profilo di rete con reti esistenti i cui dati sono stati raccolti da vCenter. Queste reti vengono quindi configurate per ottenere informazioni IP da un provider IPAM esterno, in questo caso Infoblox. Le macchine virtuali di cui si esegue il provisioning da vRealize Automation che possono essere associate a questo profilo di rete ottengono le impostazioni IP e altre impostazioni correlate a TCP/IP dal provider IPAM esterno.

Per ulteriori informazioni sulle reti, vedere [Risorse di rete in vRealize Automation](#). Per ulteriori informazioni sui profili di rete, vedere [Come aggiungere profili di rete in vRealize Automation](#) e [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

Per informazioni correlate, vedere [Come configurare un profilo di rete per supportare una rete su richiesta per un'integrazione IPAM esterna in vRealize Automation](#).

Prerequisiti

Questa sequenza di passaggi viene mostrata nel contesto di un workflow di integrazione del provider IPAM. Vedere [Tutorial: configurazione dell'integrazione di un provider IPAM esterno specifico del provider per vRealize Automation](#).

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

- Verificare di disporre di un account con il provider IPAM esterno, ad esempio [Infoblox](#) o [Bluecat](#) e di disporre delle credenziali di accesso corrette per l'account dell'organizzazione con il provider IPAM. In questo workflow di esempio, il provider IPAM è Infoblox.
- Verificare di disporre di un punto di integrazione IPAM per il provider IPAM. Vedere [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#).

Procedura

- 1 Per configurare una rete, fare clic su **Infrastruttura > Risorse > Reti**.
- 2 Nella scheda **Reti**, selezionare una rete esistente da utilizzare con il punto di integrazione del provider IPAM. In questo esempio, il nome della rete è *net.23.117-only-IPAM*.

I dati delle reti elencate sono stati raccolti da vRealize Automation da un vCenter nell'organizzazione.

- 3 Per ottenere i valori dal provider IPAM esterno, verificare che, ad eccezione di **Account/ Regione, Nome e Dominio di rete**, tutte le altre impostazioni di rete siano vuote, incluse le seguenti:
 - Dominio (vedere la nota nel passaggio 8)
 - CIDR
 - Gateway predefinito
 - Server DNS
 - Domini di ricerca DNS
- 4 Fare clic sulla scheda **Intervalli IP** e fare clic su **Aggiungi intervallo IP IPAM**.
- 5 Dal menu **Rete**, selezionare la rete appena configurata, ad esempio *net.23.117-only-IPAM*.
- 6 Dal menu **Provider**, selezionare il punto di integrazione IPAM *Infoblox_Integration* creato in precedenza nel workflow.
- 7 Dal menu a discesa **Spazio indirizzi** ora visibile, selezionare una delle viste di rete elencate.

Uno spazio di indirizzi in Infoblox è definito come una vista di rete.

Le viste di rete sono ottenute dall'account del provider IPAM. In questo esempio viene utilizzata la subnet di rete appena configurata, ad esempio *net 23.117-only-IPAM*, il punto di integrazione *Infoblox_Integration* creato in precedenza nel workflow e uno spazio di indirizzi denominato *default*.

I valori dello spazio di indirizzi elencati sono ottenuti dal provider IPAM esterno.

- 8 Nell'elenco delle reti visualizzate che sono disponibili per lo spazio di indirizzi selezionato, selezionare una o più reti, ad esempio 10.23.117.0/24.

Per questo esempio, i valori delle colonne **Domini** e **Server DNS** per la rete selezionata contengono valori di Infoblox.

Nota Se si seleziona una rete nel passaggio 3 con un dominio specificato per vRealize Automation e quindi si seleziona una rete dallo spazio di indirizzi del provider IPAM esterno contenente un valore Dominio, il valore Dominio nella rete del provider IPAM esterno ha la precedenza sul dominio specificato in vRealize Automation. Se l'impostazione dell'intervallo IP IPAM non dispone di un valore Dominio, specificato in Cloud Assembly o nel provider IPAM esterno come descritto in precedenza, il provisioning non riesce.

Per Infoblox, è possibile utilizzare la proprietà del blueprint `Infoblox.IPAM.Network.dnsSuffix` a livello di macchina per sovrascrivere il valore del dominio. Per informazioni correlate, vedere [Utilizzo delle proprietà specifiche di Infoblox e attributi estendibili per le integrazioni IPAM nei modelli cloud di vRealize Automation](#).

- 9 Fare clic su **Aggiungi** per salvare l'intervallo IP IPAM per la rete.

L'intervallo è visibile nella tabella **Intervalli IP**.

- 10 Fare clic sulla scheda **Indirizzi IP**.

Dopo aver eseguito il provisioning di una macchina utilizzando il nuovo intervallo di indirizzi dal provider IPAM esterno, nella tabella **Indirizzi IP** sarà visibile un nuovo record.

- 11 Per configurare un profilo di rete per l'utilizzo della rete, fare clic su **Infrastruttura > Configura > Profili di rete**.

- 12 Denominare il profilo di rete, ad esempio *Infoblox-NP* e aggiungere le seguenti impostazioni di esempio.

- Scheda Riepilogo

- Specificare una regione o un account cloud vSphere.
- Aggiungere un tag di funzionalità per il profilo di rete, ad esempio denominato *infoblox_abx*.

Prendere nota del tag di funzionalità, poiché è necessario utilizzarlo anche come tag di vincolo del modello cloud per creare l'associazione di provisioning nel modello cloud.

- Scheda Reti

- Aggiungere la rete creata in precedenza, ad esempio *net.23.117-only-IPAM*.

- 13 Fare clic su **Salva** per salvare il profilo di rete con queste impostazioni.

Risultati

A questo punto le impostazioni della rete e del profilo di rete sono configurate per un tipo di rete esistente da utilizzare per l'integrazione IPAM Infoblox in un modello cloud.

Definizione e distribuzione di un modello cloud che utilizza l'assegnazione dell'intervallo del provider IPAM esterno in vRealize Automation

È possibile definire un modello cloud per ottenere e gestire le assegnazioni degli indirizzi IP dal provider IPAM esterno. In questo esempio viene utilizzato Infoblox come provider IPAM esterno.

In questo passaggio finale del workflow di integrazione IPAM esterno, viene definito e distribuito un modello cloud che connette la rete e il profilo di rete definiti in precedenza all'account Infoblox dell'organizzazione per ottenere e gestire le assegnazioni di indirizzi IP per le macchine virtuali distribuite dal provider IPAM esterno anziché da vRealize Automation.

Questo workflow utilizza Infoblox come provider IPAM esterno e, in alcuni passaggi, i valori di esempio sono esclusivi di Infoblox, anche se lo scopo è che la procedura possa essere applicata ad altre integrazioni IPAM esterne.



L'articolo di blog [Automate IPAM and DNS for VMs using VMware vRealize Automation and Infoblox DDI](#) di Infoblox fornisce informazioni correlate.

Dopo aver distribuito il modello cloud e aver avviato la macchina virtuale, l'indirizzo IP utilizzato per ogni macchina virtuale nella distribuzione viene visualizzato come voce di rete nella pagina **Risorse > Reti**, come nuovo record host nella rete del provider IPAM nell'account del provider IPAM e nel record di vSphere Web Client per ogni macchina virtuale distribuita in vCenter host.

Prerequisiti

Questa sequenza di passaggi viene illustrata nel contesto di un workflow di integrazione del provider IPAM esterno. Vedere [Tutorial: configurazione dell'integrazione di un provider IPAM esterno specifico del provider per vRealize Automation](#).

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre di un account con il provider IPAM esterno, ad esempio Infoblox o BlueCat e di disporre delle credenziali di accesso corrette per l'account dell'organizzazione con il provider IPAM.
- Verificare di disporre dell'accesso di amministratore all'account host e di tutti i requisiti di ruolo necessari per visualizzare i record di stato nel record di vSphere Web Client per le macchine virtuali distribuite in vCenter host.
- Verificare di disporre di un punto di integrazione IPAM per il provider IPAM esterno. Vedere [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#).

- Verificare di aver configurato una rete e un profilo di rete di vRealize Automation che supportino l'integrazione IPAM esterna per il punto di integrazione IPAM previsto. Vedere [Configurazione di una rete e di un profilo di rete per l'utilizzo di un IPAM esterno per una rete esistente in vRealize Automation](#).
- Verificare che il progetto e la zona cloud siano contrassegnati in modo che corrispondano ai tag nel punto di integrazione IPAM e nella rete o nel profilo di rete. Facoltativamente, configurare il progetto per supportare la denominazione personalizzata delle risorse.

Per ulteriori informazioni rispetto a quelle fornite in merito al ruolo di un progetto e una zona cloud, nonché al ruolo degli altri elementi dell'infrastruttura nel modello cloud, vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#). Per ulteriori informazioni sull'assegnazione dei tag, vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#).

Per informazioni sull'assegnazione di nomi personalizzati alle macchine virtuali mediante le impostazioni del progetto, vedere [Denominazione personalizzata per le risorse distribuite in Cloud Assembly](#).

Procedura

- 1 Fare clic su **Modelli cloud > Nuovo**, immettere le seguenti informazioni nella pagina **Nuovo modello cloud** e fare clic su **Crea**.
 - **Nome** = ipam-bpa
 - **Descrizione** = Modello cloud che utilizza l'integrazione IPAM di Infoblox
 - **Progetto** = 123VC
- 2 Per questo esempio, aggiungere un componente macchina indipendente dal cloud e un componente di rete indipendente dal cloud nella tela del modello cloud e connettere i due componenti.
- 3 Modificare il codice del modello cloud per aggiungere al componente di rete un tag di vincolo che corrisponda al tag di funzionalità aggiunto al profilo di rete. Per questo esempio, il valore del tag è *infoblox_abx*.
- 4 Modificare il codice del modello cloud per specificare *static* come tipo di assegnazione di rete.

Quando si utilizza un provider IPAM esterno, l'impostazione `assignment: static` è obbligatoria.

Per questo esempio, l'indirizzo IP specificato 10.23.117.4 è attualmente disponibile nello spazio degli indirizzi IPAM esterno selezionato per la rete nel profilo di rete associato. Sebbene l'impostazione `assignment: static` sia obbligatoria, l'impostazione `address: value` non lo è. È possibile scegliere di avviare la selezione di indirizzi IP esterni in un determinato valore di indirizzo, ma tale operazione non è obbligatoria. Se non si specifica un'impostazione `address: value`, il provider IPAM esterno seleziona l'indirizzo successivo disponibile nella rete IPAM esterna.

5 Verificare il codice del modello cloud rispetto all'esempio seguente.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      name: ipam
      constraints:
        - tag: infoblox_abx
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: static
          address: 10.23.117.4
          name: '${resource.Cloud_Network_1.name}'
```

Per esempi di proprietà di Infoblox disponibili per la specifica delle impostazioni DNS e DHCP nei modelli cloud, vedere [Utilizzo delle proprietà specifiche di Infoblox e attributi estendibili per le integrazioni IPAM nei modelli cloud di vRealize Automation](#).

- 6 Fare clic su **Distribuisci** nella pagina del modello cloud, denominare la distribuzione *Infoblox-1* e fare clic su **Distribuisci** nella pagina **Tipo di distribuzione**.
- 7 Durante la distribuzione del modello cloud, fare clic sulla scheda **Estendibilità** e selezionare **Attività > Esecuzioni di azione** per visualizzare l'azione di estendibilità *Infoblox_AllocateIP_n* in esecuzione.

Dopo il completamento dell'azione di estendibilità e il provisioning della macchina, l'azione *Infoblox_Update_n* propaga l'indirizzo MAC a Infoblox.

- 8 È possibile accedere all'account Infoblox e aprirlo per visualizzare il nuovo record host per l'indirizzo IPAM nella rete 10.23.117.0/24 associata. È inoltre possibile aprire la scheda DNS in Infoblox per visualizzare il nuovo record host DNS.
- 9 Per verificare che la macchina virtuale venga sottoposta a provisioning, accedere a vCenter host e a vSphere Web Client per individuare la macchina sottoposta a provisioning, nonché visualizzare l'indirizzo IP e il nome DNS.

Dopo l'avvio della macchina virtuale sottoposta a provisioning, l'indirizzo MAC viene propagato in Infoblox da un'azione di estendibilità *Infoblox_AllocateIP*.

- 10 Per visualizzare il nuovo record di rete in vRealize Automation, selezionare **Infrastruttura > Risorse > Reti** e fare clic per aprire la scheda **Indirizzi IP**.

- 11 Se si elimina la distribuzione, gli indirizzi IPAM delle macchine virtuali della distribuzione vengono rilasciati e gli indirizzi IP sono nuovamente disponibili per il provider IPAM esterno per altre allocazioni. L'azione di estensibilità per questo evento in vRealize Automation è *Infoblox_Deallocate*.

Utilizzo delle proprietà specifiche di Infoblox e attributi estensibili per le integrazioni IPAM nei modelli cloud di vRealize Automation

È possibile utilizzare le proprietà specifiche di Infoblox per i progetti di vRealize Automation che contengono integrazioni IPAM esterne per Infoblox.

Le seguenti proprietà di Infoblox sono disponibili per l'utilizzo con le integrazioni IPAM di Infoblox in progettazioni e distribuzioni di modelli cloud. È possibile utilizzarle in vRealize Automation per controllare ulteriormente l'allocazione degli indirizzi IP durante la distribuzione del modello cloud. L'uso di queste proprietà è facoltativo.

Nota Se usi il plug-in Infoblox 1.4 o versioni precedenti, una proprietà Infoblox globale sovrascrive una proprietà Infoblox locale per le proprietà `dnsSuffix`, `dnsView`, `enableDns` e `enableDhcp`. Una proprietà globale si applica a tutte le NIC.

Queste proprietà sono disponibili e incluse nella versione più recente del plug-in Infoblox per vRealize Automation. Per informazioni sulle versioni del plug-in Infoblox e su dove ottenere la versione più recente del plug-in Infoblox per l'integrazione IPAM in vRealize Automation, vedere [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

- `Infoblox.IPAM.createFixedAddress`

Questa proprietà consente di creare un record di indirizzo fisso in Infoblox. I valori possibili sono True e False. Per impostazione predefinita, viene creato un record dell'host. Il valore predefinito è False.

- `Infoblox.IPAM.Network.dnsView`

Questa proprietà consente di utilizzare una vista DNS durante la creazione di un record host all'interno di Infoblox.

- `Infoblox.IPAM.Network.enableDns`

Quando si alloca un IP in Infoblox, questa proprietà consente di creare anche un record DNS. I valori possibili sono True e False. Il valore predefinito è True.

- `Infoblox.IPAM.Network.enableDhcp`

Questa proprietà consente di impostare la configurazione DHCP per l'indirizzo host. I valori possibili sono True e False. Il valore predefinito è True.

- `Infoblox.IPAM.Network.dnsSuffix`

Questa proprietà consente di sovrascrivere l'opzione DHCP *domain* di una rete Infoblox con una nuova. Questa funzionalità è utile se la rete di Infoblox non dispone dell'opzione DHCP *domain* o se l'opzione DHCP *domain* deve essere sovrascritta. Il valore predefinito è null (stringa vuota)

Quando si utilizza un provider IPAM esterno, ad esempio Infoblox, è necessario specificare un suffisso DNS quando si esegue il provisioning di una macchina. Se è richiesto un suffisso DNS, è possibile specificarlo in uno qualsiasi dei seguenti modi:

- Specificare il suffisso DNS nella subnet di rete di vSphere in vRealize Automation.
- Specificare la proprietà `Infoblox.IPAM.Network.dnsSuffix` nel codice della risorsa macchina nel modello cloud di vRealize Automation.

Di seguito è riportato un esempio all'interno della sezione `Infoblox.IPAM.Network.hostnameNicSuffix`.

`Infoblox.IPAM.Network.dnsSuffix` è applicabile solo se `Infoblox.IPAM.Network.enableDns` è impostato su `True`.

- `Infoblox.IPAM.Network.hostnameNicSuffix`

È possibile utilizzare questa proprietà per specificare un suffisso dell'indice della NIC durante la generazione di un nome host.

In questo modo è possibile eseguire il provisioning di una macchina con più NIC in modo che i nomi host per ciascuna NIC siano distinti da un suffisso definito in modo personalizzato. Come illustrato nell'esempio seguente, è possibile eseguire il provisioning di una macchina, ad esempio *my-machine*, dotata di 2 NIC in modo che il suffisso del nome host per la prima NIC sia `-nic1` e quello per la seconda sia `-nic2`.

È inoltre possibile specificare un suffisso DNS, come mostrato nell'esempio. La proprietà `Infoblox.IPAM.Network.dnsSuffix` viene utilizzata con il valore `test.local` per fare in modo che la prima NIC sia denominata *my-machine-nic1.test.local* e l'altra sia denominata *my-machine-nic2.test.local*.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      Infoblox.IPAM.Network.dnsSuffix: test.local
      Infoblox.IPAM.Network0.hostnameNicSuffix: -nic1
      Infoblox.IPAM.Network1.hostnameNicSuffix: -nic2
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          deviceIndex: 0
        - network: '${resource.Cloud_Network_2.id}'
          deviceIndex: 1
```

```

Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
Cloud_Network_2:
  type: Cloud.Network
  properties:
    networkType: existing

```

Questa proprietà è stata introdotta con la versione 1.3 del plug-in Infoblox. Vedere [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

- È possibile specificare le proprietà anche utilizzando una sottoscrizione di estendibilità.

Per informazioni correlate sugli attributi estendibili di Infoblox rispetto a questo caso d'uso, vedere [Aggiunta degli attributi estendibili obbligatori nell'applicazione Infoblox per l'integrazione con vRealize Automation](#).

Utilizzo delle proprietà di Infoblox in schede NIC di macchine diverse in un modello cloud

Le seguenti proprietà di Infoblox possono supportare un valore diverso per ciascuna scheda NIC della macchina nel modello cloud:

- `Infoblox.IPAM.Network.enableDhcp`
- `Infoblox.IPAM.Network.dnsView`
- `Infoblox.IPAM.Network.enableDns`
- `Infoblox.IPAM.Network.hostnameNicSuffix`

Ad esempio, per utilizzare un valore `Infoblox.IPAM.Network.dnsView` diverso per ciascuna scheda NIC, utilizzare una voce `Infoblox.IPAM.Network<nicIndex>.dnsView` per ciascuna scheda NIC. L'esempio seguente mostra valori `Infoblox.IPAM.Network.dnsView` diversi per due schede NIC.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      Infoblox.IPAM.Network0.dnsView: default
      Infoblox.IPAM.Network1.dnsView: my-net
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          deviceIndex: 0
        - network: '${resource.Cloud_Network_2.id}'
          deviceIndex: 1
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing

```



```
Cloud_Network_2:
  type: Cloud.Network
  properties:
    networkType: existing
```

Per impostazione predefinita, l'integrazione di Infoblox crea un record host DNS nella vista DNS *default* in Infoblox. Se l'amministratore di Infoblox ha creato viste DNS *custom*, è possibile sovrascrivere il comportamento di integrazione predefinito e specificare una vista denominata utilizzando la proprietà `Infoblox.IPAM.Network.dnsView` nel componente macchina. Ad esempio, è possibile aggiungere la proprietà seguente al componente `Cloud_Machine_1` per specificare una vista DNS denominata in Infoblox.

```
Cloud_Machine_1:
  type: Cloud.Machine
  properties:
    image: ubuntu
    flavor: small
    Infoblox.IPAM.Network.dnsView: <dns-view-name>
```

Per informazioni sulla configurazione e l'utilizzo delle viste DNS, vedere [DNS Views](#) (Viste DNS) nella documentazione del prodotto di Infoblox. Per alcuni esempi nel workflow di integrazione di Infoblox, vedere [Definizione e distribuzione di un modello cloud che utilizza l'assegnazione dell'intervallo del provider IPAM esterno in vRealize Automation](#).

Come specificare le proprietà di Infoblox

È possibile specificare una proprietà di Infoblox utilizzando uno dei metodi seguenti in Cloud Assembly:

- È possibile specificare le proprietà in un progetto utilizzando la sezione **Proprietà personalizzate** nella pagina **Infrastruttura > Amministrazione > Progetti**. Utilizzando questo metodo, le proprietà specificate vengono applicate a tutte le macchine sottoposte a provisioning nell'ambito di questo progetto.
- È possibile specificare le proprietà in ciascun componente macchina in un modello cloud. Di seguito viene mostrato il codice del modello cloud di esempio che illustra l'uso della proprietà `Infoblox.IPAM.Network.dnsView`:

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      Infoblox.IPAM.Network.dnsView: default
      image: ubuntu
      cpuCount: 1
      totalMemoryMB: 1024
      networks:
        - network: '${resource.Cloud_Network_1.id}'
  Cloud_Network_1:
```

```

type: Cloud.Network
properties:
  networkType: existing
  constraints:
    - tag: mk-ipam-demo

```

Controllo della raccolta dei dati di rete mediante filtri Infoblox in vRealize Automation

Per Infoblox, è possibile limitare il numero di reti in cui vengono raccolti i dati alle sole reti necessarie per le operazioni di vRealize Automation. In questo modo è possibile ridurre la quantità di dati trasferiti e migliorare le prestazioni del sistema.

vRealize Automation raccoglie i dati ogni 10 minuti dal sistema IPAM esterno. Per Infoblox, è possibile applicare filtri in diversi modi per individuare solo un sottoinsieme di reti utilizzate dalle operazioni di vRealize Automation e raccogliere dati da tali reti.

Per filtrare la raccolta dei dati per le reti che utilizzano indirizzi IP generati da Infoblox, utilizzare le seguenti proprietà nella scheda di integrazione IPAM. Le proprietà del filtro sono disponibili quando si crea o si modifica il punto di integrazione IPAM esterno per Infoblox.

Questi filtri sono disponibili solo con vRealize Automation 8.3 e versione successiva e con il [plug-in Infoblox 1.3](#) e versione successiva (ad esempio, il [plug-in Infoblox versione 1.4](#)).

Nota Il [plug-in Infoblox versione 1.3](#) può essere utilizzato con vRealize Automation 8.1 o 8.2, ma solo in alcuni casi e con cautela, come descritto nell'articolo della Knowledge Base [Compatibilità di Infoblox 1.3 con vRealize Automation 8.x \(82142\)](#).

- `Infoblox.IPAM.NetworkContainerFilter`

Filtra in contenitori di reti.

- `Infoblox.IPAM.NetworkFilter`

Filtra in reti.

- `Infoblox.IPAM.RangeFilter`

Filtra in intervalli di indirizzi IP.

Prestare attenzione quando si applicano questi filtri di raccolta dei dati alle reti in cui è già stata effettuata la raccolta dei dati. Se si applicano filtri per impedire la raccolta dei dati in alcune reti, le reti in cui non vengono raccolti i dati vengono considerate non necessarie ed eliminate da vRealize Automation. Le reti associate a subnet di vRealize Automation sono un'eccezione. Le reti in cui sono già stati raccolti i dati che non vengono successivamente individuate e sottoposte alla raccolta dei dati, ad esempio perché sono state escluse dall'attività di raccolta dati, vengono eliminate dal database di vRealize Automation. Tuttavia, se le reti in cui sono già stati raccolti i dati sono in uso in vRealize Automation, non vengono eliminate.

Questi filtri vengono applicati come parametri di query nelle richieste di ricerca per i diversi oggetti di rete. È possibile utilizzare tutti i parametri di ricerca supportati da Infoblox. È possibile filtrare in base a CIDR o attributi estendibili basati su espressioni regolari o corrispondenze esatte. Il formato utilizza il formato di filtro Infoblox WAPI, come descritto nella [documentazione di Infoblox WAPI](#). Gli esempi seguenti illustrano i metodi di filtro in base a CIDR o attributi estendibili:

- Filtro in base a CIDR per reti e contenitori di reti. Esempi:
 - Corrispondenza esatta - `Infoblox.IPAM.NetworkFilter: network=192.168.0.0`
 - Corrispondenza in base ad attributo estendibile - `Infoblox.IPAM.NetworkFilter: network~=192.168`
- Filtro in base a CIDR per intervallo di indirizzi IP. Esempio:

Corrispondenza in base a espressione regolare e nome visualizzato della rete -

`Infoblox.IPAM.RangeFilter: network~=192.168.&network_view=my_view`
- Filtro in base ad attributi estendibili per reti, intervalli di indirizzi IP e contenitori di reti.

La sintassi utilizza il formato *filter_name=*ext_attr=ext_attr_value*. Esempi:

 - Corrispondenza esatta - `*Building=Data Center`
 - Corrispondenza in base a espressione regolare con '~' - `*Building~=*Center`
 - Corrispondenza con distinzione tra maiuscole e minuscole con ':' - `*Building:=data center`
 - Esclusione della corrispondenza con '!' - `*Building!=Data Center`
 - Corrispondenza in base a espressione regolare (è possibile combinare distinzione tra maiuscole e minuscole ed esclusione): `*Building! ~:=Data Cent / *Building~:=center`
- Filtro in base a CIDR e attributi estendibili utilizzando la sintassi dei metodi di filtro precedenti.

Esempio:

`network=192.168.&*Building=Data Center`

Per ulteriori informazioni sull'utilizzo di attributi estendibili ed espressioni regolari in queste proprietà, vedere le [espressioni supportate da Infoblox per i parametri di ricerca](#) e la [guida di riferimento a Infoblox REST API](#).

Impostazione di Cloud Assembly per l'organizzazione

3

L'amministratore di Cloud Assembly deve comprendere i ruoli utente e configurare le connessioni con il fornitore dell'account cloud e le applicazioni di integrazione.

Quando si configurano gli account cloud e le integrazioni, si configura la comunicazione tra Cloud Assembly e i sistemi di destinazione.

Questo capitolo include i seguenti argomenti:

- [Che cosa sono i ruoli utente di vRealize Automation](#)
- [Aggiunta di account cloud a Cloud Assembly](#)
- [Integrazione di vRealize Automation con altre applicazioni](#)
- [Che cosa sono i piani di onboarding in Cloud Assembly](#)
- [Configurazione avanzata per l'ambiente Cloud Assembly](#)

Che cosa sono i ruoli utente di vRealize Automation

vRealize Automation include diversi livelli di ruoli utente. Questi livelli controllano l'accesso a organizzazione, servizi, progetti che producono o utilizzano i modelli cloud, elementi di catalogo e pipeline, nonché la possibilità per gli utenti di utilizzare o visualizzare le singole parti dell'interfaccia utente. Questi livelli forniscono agli amministratori del cloud strumenti diversi per applicare qualsiasi livello di granularità richiesto in base alle esigenze operative.

Descrizioni generale dei ruoli

I ruoli utente sono definiti a diversi livelli. I ruoli del livello di servizio sono definiti per ogni servizio.

Dopo questa tabella sono disponibili ulteriori dettagli per i ruoli di servizio.

Ruolo	Autorizzazioni generali	Dove è definito il ruolo
Proprietario dell'organizzazione	<p>Può accedere alla console e aggiungere utenti all'organizzazione.</p> <p>Il proprietario dell'organizzazione non può accedere a un servizio a meno che non disponga di un ruolo di servizio.</p> <p>Ulteriori informazioni su Ruoli utente dell'organizzazione</p>	Console dell'organizzazione
Membro dell'organizzazione	<p>Può accedere alla console.</p> <p>Il membro dell'organizzazione non può accedere a un servizio a meno che non disponga di un ruolo di servizio.</p> <p>Ulteriori informazioni su Ruoli utente dell'organizzazione</p>	Console dell'organizzazione
Amministratore servizio	<p>Può accedere alla console e dispone di privilegi di visualizzazione, aggiornamento ed eliminazione completi nel servizio.</p> <ul style="list-style-type: none"> ■ Ruoli di servizio di Cloud Assembly ■ Ruoli di servizio di Service Broker ■ Ruoli di servizio di Code Stream ■ Ruoli del servizio Assistente migrazione vRA ■ Ruoli del servizio Orchestrator ■ Ruolo del servizio di SaltStack Config 	Console dell'organizzazione
Utente servizio	<p>Può accedere alla console e al servizio con autorizzazioni limitate.</p> <p>Il membro del servizio ha un'interfaccia utente limitata. Ciò che può visualizzare e le operazioni che può eseguire dipendono dall'appartenenza al progetto.</p> <ul style="list-style-type: none"> ■ Ruoli di servizio di Cloud Assembly ■ Ruoli di servizio di Service Broker ■ Ruoli di servizio di Code Stream 	Console dell'organizzazione
Visualizzatore servizio	<p>Può accedere alla console e al servizio in modalità di sola visualizzazione.</p> <ul style="list-style-type: none"> ■ Ruoli di servizio di Cloud Assembly ■ Ruoli di servizio di Service Broker ■ Ruoli di servizio di Code Stream ■ Ruoli del servizio Assistente migrazione vRA ■ Ruoli del servizio Orchestrator 	Console dell'organizzazione

Ruolo	Autorizzazioni generali	Dove è definito il ruolo
Esecutore (solo Code Stream)	Può accedere alla console e gestire le esecuzioni della pipeline. Ruoli di servizio di Code Stream	Console dell'organizzazione
Progettista di workflow di Orchestrator (solo Orchestrator)	Può creare, eseguire, modificare ed eliminare i propri contenuti del client di vRealize Orchestrator. Può aggiungere i propri contenuti al gruppo a cui è assegnato. Non può accedere alle funzionalità di amministrazione e risoluzione dei problemi del client di vRealize Orchestrator. Ruoli del servizio Orchestrator	Console dell'organizzazione
Ruoli di progetto	Possono visualizzare e gestire le risorse del progetto in base al ruolo di progetto. I ruoli di progetto includono amministratore, membro e visualizzatore. Ruoli utente di organizzazione e servizio in vRealize Automation	Cloud Assembly, Service Broker e Code Stream
Ruoli personalizzati	Le autorizzazioni sono definite dall'Amministratore Cloud Assembly per tutti i servizi. Per poter accedere al servizio, l'utente deve avere almeno un ruolo Visualizzatore servizio in tale servizio. I ruoli personalizzati hanno la precedenza sui ruoli servizio. Ruoli utente personalizzati in vRealize Automation	Cloud Assembly e Service Broker
Ruolo integrato di amministratore dell'infrastruttura	Concede autorizzazioni predefinite per le attività in vRealize Automation. Modalità di assegnazione del ruolo integrato di Amministratore dell'infrastruttura Cloud Assembly a un utente	Utilizzo dell'API

Ruoli utente di organizzazione e servizio in vRealize Automation

I ruoli utente dell'organizzazione e del servizio definiti per i servizi di Cloud Assembly, Service Broker e Code Stream determinano ciò che l'utente può visualizzare ed eseguire in ogni servizio.

Ruoli utente dell'organizzazione

I ruoli utente vengono definiti per l'organizzazione nella console di vRealize Automation da un proprietario dell'organizzazione. Sono disponibili due tipi di ruoli: ruoli dell'organizzazione e ruoli di servizio.

I ruoli dell'organizzazione sono globali e si applicano a tutti i servizi dell'organizzazione. I ruoli a livello di organizzazione sono Proprietario dell'organizzazione o Membro dell'organizzazione.

Per ulteriori informazioni sui ruoli dell'organizzazione, vedere [Amministrazione di vRealize Automation](#)

I ruoli di servizio di Cloud Assembly, che sono autorizzazioni specifiche del servizio, sono assegnati anche a livello di organizzazione nella console.

Ruoli di servizio

Questi ruoli di servizio sono assegnati dal proprietario dell'organizzazione.

Questo articolo include informazioni sui seguenti servizi.

- [Ruoli di servizio di Cloud Assembly](#)
- [Ruoli di servizio di Service Broker](#)
- [Ruoli di servizio di Code Stream](#)
- [Ruoli del servizio Assistente migrazione vRA](#)
- [Ruoli del servizio Orchestrator](#)
- [Ruolo del servizio di SaltStack Config](#)

Ruoli di servizio di Cloud Assembly

I ruoli di servizio di Cloud Assembly determinano ciò che è possibile visualizzare ed eseguire in Cloud Assembly. Questi ruoli di servizio sono definiti nella console da un proprietario dell'organizzazione.

Tabella 3-1. Descrizioni dei ruoli di servizio di Cloud Assembly

Ruolo	Descrizione
Amministratore di Cloud Assembly	Utente che dispone di accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può visualizzare ed eseguire tutto, ad esempio aggiungere account cloud, creare nuovi progetti e assegnare un amministratore del progetto.
Utente di Cloud Assembly	Un utente che non dispone del ruolo di amministratore di Cloud Assembly. In un progetto di Cloud Assembly, l'amministratore aggiunge gli utenti ai progetti come membri del progetto, amministratori o visualizzatori. L'amministratore può anche aggiungere un amministratore del progetto.
Visualizzatore di Cloud Assembly	Utente che ha accesso in lettura per visualizzare le informazioni ma che non può creare, aggiornare o eliminare valori. Si tratta di un ruolo di sola lettura in tutti i progetti. Gli utenti con il ruolo di visualizzatore possono visualizzare tutte le informazioni disponibili all'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.

Oltre ai ruoli di servizio, Cloud Assembly dispone di ruoli di progetto. Qualsiasi progetto è disponibile in tutti i servizi.

I ruoli di progetto sono definiti in Cloud Assembly e possono variare tra i progetti.

Nelle tabelle seguenti, che indicano all'utente cosa possono visualizzare ed eseguire i diversi ruoli di servizio e progetto, tenere presente che gli amministratori del servizio dispongono di autorizzazioni complete in tutte le aree dell'interfaccia utente.

Le descrizioni dei ruoli di progetto consentiranno di decidere quali autorizzazioni concedere agli utenti.

- Gli amministratori del progetto sfruttano l'infrastruttura creata dall'amministratore del servizio per garantire che i loro membri del progetto dispongano delle risorse di cui hanno bisogno per le operazioni di sviluppo.
- I membri del progetto lavorano all'interno dei loro progetti per progettare e distribuire modelli cloud. I progetti possono includere solo risorse di proprietà dell'utente o risorse che l'utente condivide con altri membri del progetto.
- I visualizzatori del progetto sono limitati all'accesso di sola lettura, ad eccezione di alcuni casi in cui possono eseguire operazioni non distruttive come il download di modelli cloud.

- I supervisor del progetto sono approvatori in Service Broker per i propri progetti in cui viene definito un criterio di approvazione con un approvatore del supervisore del progetto. Per fornire al supervisore un contesto per le approvazioni, è consigliabile concedergli anche il ruolo di membro o visualizzatore del progetto.

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly

Contesto dell'interfaccia utente		Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
Attività				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
Accesso a Cloud Assembly							
Console	Nella console di vRA, è possibile visualizzare e aprire Cloud Assembly	Sì	Sì	Sì	Sì	Sì	Sì
Infrastruttura							
	Visualizzare e aprire la scheda Infrastruttura	Sì	Sì	Sì	Sì	Sì	Sì
Configurazione - Progetti	Creare progetti	Sì					
	Aggiornare o eliminare i valori da riepilogo del progetto, provisioning, Kubernetes e integrazioni, nonché testare le configurazioni dei progetti.	Sì					
	Aggiungere utenti e gruppi, nonché assegnare ruoli nei progetti.	Sì		Sì. Progetti personali.			

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Visualizzare i progetti	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali
Configurazione - Zone cloud	Creare, aggiornare o eliminare le zone cloud	Sì					
	Visualizzare le zone cloud	Sì	Sì				
	Visualizzare la dashboard Dettagli della zona cloud	Sì	Sì				
	Visualizzare gli avvisi delle zone cloud	Sì	Sì				
Configurazione - Zone Kubernetes	Creare, aggiornare o eliminare le zone Kubernetes	Sì					
	Visualizzare le zone Kubernetes	Sì	Sì				
Configurazione - Caratteristiche	Creare, aggiornare o eliminare le caratteristiche	Sì					
	Visualizzare le caratteristiche	Sì	Sì				
Configurazione - Mappature dell'immagine	Creare, aggiornare o eliminare le mappature delle immagini	Sì					
	Visualizzare le mappature delle immagini	Sì	Sì				

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
Configurazione - Profili di rete	Creare, aggiornare o eliminare i profili di rete	Sì					
	Visualizzare i profili di rete delle immagini	Sì	Sì				
Configurazione - Profili di storage	Creare, aggiornare o eliminare i profili di storage	Sì					
	Visualizzare i profili di storage delle immagini	Sì	Sì				
Configurazione - Schede dei prezzi	Creare, aggiornare o eliminare le schede dei prezzi	Sì					
	Visualizzare le schede dei prezzi	Sì	Sì				
Configurazione - Tag	Creare, aggiornare o eliminare i tag	Sì					
	Visualizzare i tag	Sì	Sì				
Risorse - Risorse di elaborazione	Aggiungere tag alle risorse di elaborazione rilevate	Sì					
	Visualizzare le risorse di elaborazione rilevate	Sì	Sì				

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
Risorse - Reti	Modificare i tag di rete, gli intervalli IP e gli indirizzi IP	Sì					
	Visualizzare le risorse di rete rilevate	Sì	Sì				
Risorse - Sicurezza	Aggiungere tag ai gruppi di sicurezza rilevati	Sì					
	Visualizzare i gruppi di sicurezza rilevati	Sì	Sì				
Risorse - Storage	Aggiungere tag allo storage rilevato	Sì					
	Visualizzare lo storage	Sì	Sì				
Risorse - Kubernetes	Distribuire o aggiungere cluster Kubernetes e creare o aggiungere spazi dei nomi	Sì					
	Visualizzare gli spazi dei nomi e i cluster Kubernetes	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
Attività - Richieste	Eliminare i record delle richieste di distribuzione	Sì					
	Visualizzare i record delle richieste di distribuzione	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
Attività - Registri eventi	Visualizzare i registri eventi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
Connessioni - Account cloud	Creare, aggiornare o eliminare gli account cloud	Sì					
	Visualizzare gli account cloud	Sì	Sì				
Connessioni - Integrazioni	Creare, aggiornare o eliminare le integrazioni	Sì					
	Visualizzare le integrazioni	Sì	Sì				
Onboarding	Creare, aggiornare o eliminare i piani di onboarding	Sì					
	Visualizzare i piani di onboarding	Sì	Sì			Sì. Progetti personali	
Estendibilità							
	Visualizzare e aprire la scheda Estendibilità	Sì	Sì			Sì	
Eventi	Visualizzare gli eventi di estendibilità	Sì	Sì				
Sottoscrizioni	Creare, aggiornare o eliminare le sottoscrizioni di estendibilità	Sì					
	Disattivare le sottoscrizioni	Sì					

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Visualizzare le sottoscrizioni	Sì	Sì				
Libreria - Argomenti dell'evento	Visualizzare gli argomenti dell'evento	Sì	Sì				
Libreria - Azioni	Creare, aggiornare o eliminare le azioni di estendibilità	Sì					
	Visualizzare le azioni di estendibilità	Sì	Sì				
Libreria - Workflow	Visualizzare i workflow di estendibilità	Sì	Sì				
Attività - Esecuzioni di azione	Annullare o eliminare esecuzioni di azione di estendibilità	Sì					
	Visualizzare le esecuzioni di azione di estendibilità	Sì	Sì			Sì. Progetti personali	
Attività - Esecuzioni di workflow	Visualizzare le esecuzioni di workflow di estendibilità	Sì	Sì				
Progettazione							
Progettazione	Aprire la scheda Progettazione	Sì	Sì	Sì.	Sì.	Sì.	Sì
Modelli cloud	Creare, aggiornare ed eliminare modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali		

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Visualizzare modelli cloud	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
	Scaricare modelli cloud	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
	Caricare modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali		
	Distribuire modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali		
	Assegnare una versione e ripristinare i modelli cloud	Sì		Sì. Progetti personali	Sì. Progetti personali		
	Rilasciare modelli cloud nel catalogo	Sì		Sì. Progetti personali	Sì. Progetti personali		
Risorse personalizzate	Creare, aggiornare o eliminare le risorse personalizzate	Sì					
	Visualizzare le risorse personalizzate	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
Azioni personalizzate	Creare, aggiornare o eliminare le azioni personalizzate	Sì					
	Visualizzare le azioni personalizzate	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
Risorse							
	Visualizzare e aprire la scheda Risorse	Sì	Sì	Sì	Sì	Sì	Sì

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
Distribuzioni	Visualizzare le distribuzioni, inclusi dettagli della distribuzione, cronologia delle distribuzioni, prezzo, monitoraggio, avvisi, ottimizzazione e informazioni sulla risoluzione dei problemi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
	Gestire gli avvisi	Sì		Sì. Progetti personali	Sì. progetti personali		
	Eseguire azioni giorno 2 nelle distribuzioni in base ai criteri	Sì		Sì. Progetti personali	Sì. Progetti personali		
Risorse - Tutte le risorse	Visualizzazione di tutte le risorse rilevate	Sì	Sì				

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Eseguire azioni giorno 2 sulle risorse rilevate. Azioni disponibili solo sulle macchine e limitate all'accensione e allo spegnimento per tutte le macchine e console remote per le macchine vSphere.	Sì					
Risorse - Tutte le risorse	Visualizzare le risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	
	Eseguire azioni giorno 2 sulle risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione in base ai criteri	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.		
Risorse - Macchine virtuali	Visualizzare le macchine rilevate	Sì	Sì				

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Eseguire azioni giorno 2 sulle macchine rilevate. Le azioni sono limitate all'accensione e allo spegnimento e alla console remota per le macchine vSphere.	Sì					
	Creare nuova macchina virtuale	Sì					
	Visualizzare le risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione.	Sì		Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	
	Eseguire azioni giorno 2 sulle risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione in base ai criteri	Sì		Sì. Progetti personali.	Sì. Progetti personali.		
Risorse - Volumi	Visualizzare i volumi rilevati	Sì	Sì				
	Nessuna azione giorno 2 disponibile						

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Visualizzare i volumi distribuiti, sottoposti a onboarding e migrati	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	
	Eseguire azioni giorno 2 sui volumi distribuiti, sottoposti a onboarding e migrati in base ai criteri	Sì		Sì. Progetti personali.	Sì. Progetti personali.		
Risorse - Rete e sicurezza	Visualizzare reti, bilanciamenti del carico e gruppi di sicurezza rilevati	Sì	Sì				
	Nessuna azione giorno 2 disponibile						
	Visualizzare le reti, i bilanciamenti del carico e i gruppi di sicurezza distribuiti, di cui è stato eseguito l'onboarding e migrati	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	

Tabella 3-2. Ruoli di servizio e ruoli di progetto di Cloud Assembly (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Cloud Assembly	Visualizzatore di Cloud Assembly	Utente di Cloud Assembly			
				L'utente deve essere un membro o un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Eseguire azioni giorno 2 su reti, bilanciamenti del carico e gruppi di sicurezza distribuiti di cui è stato eseguito l'onboarding e migrati in base ai criteri	Sì		Sì. Progetti personali.	Sì. Progetti personali.		
Avvisi							
	Visualizzare e aprire la scheda Avvisi	Sì	Sì	Sì	Sì	Sì	
	Gestire gli avvisi	Sì		Sì. Progetti personali	Sì. Progetti personali		
	Visualizzare gli avvisi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	

Ruoli di servizio di Service Broker

I ruoli di servizio di Service Broker determinano ciò che è possibile visualizzare ed eseguire in Service Broker. Questi ruoli di servizio sono definiti nella console da un proprietario dell'organizzazione.

Tabella 3-3. Descrizioni dei ruoli di servizio di Service Broker

Ruolo	Descrizione
Amministratore di Service Broker	Deve disporre dell'accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può eseguire tutte le attività, ad esempio la creazione di un nuovo progetto e l'assegnazione di un amministratore del progetto.
Utente di Service Broker	Qualsiasi utente che non disponga del ruolo di amministratore di Service Broker. In un progetto di Service Broker, l'amministratore aggiunge gli utenti ai progetti come membri del progetto, amministratori o visualizzatori. L'amministratore può anche aggiungere un amministratore del progetto.
Visualizzatore di Service Broker	Utente che ha accesso in lettura per visualizzare le informazioni ma che non può creare, aggiornare o eliminare valori. Gli utenti con il ruolo di visualizzatore possono visualizzare tutte le informazioni disponibili all'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.

Oltre ai ruoli di servizio, Service Broker dispone di ruoli di progetto. Qualsiasi progetto è disponibile in tutti i servizi.

I ruoli di progetto sono definiti in Service Broker e possono variare tra i progetti.

Nelle tabelle seguenti, che indicano all'utente cosa possono visualizzare ed eseguire i diversi ruoli di servizio e progetto, tenere presente che gli amministratori del servizio dispongono di autorizzazioni complete in tutte le aree dell'interfaccia utente.

L'utilizzo delle seguenti descrizioni dei ruoli di progetto consentirà di decidere quali autorizzazioni concedere agli utenti.

- Gli amministratori del progetto sfruttano l'infrastruttura creata dall'amministratore del servizio per garantire che i loro membri del progetto dispongano delle risorse di cui hanno bisogno per le operazioni di sviluppo.
- I membri del progetto lavorano all'interno dei loro progetti per progettare e distribuire modelli cloud. Nella tabella seguente, i progetti possono includere solo le risorse di cui si è proprietari o le risorse condivise con altri membri del progetto.
- I visualizzatori del progetto sono limitati all'accesso di sola lettura.

- I supervisor del progetto sono approvatori in Service Broker per i propri progetti in cui viene definito un criterio di approvazione con un approvatore del supervisore del progetto. Per fornire al supervisore un contesto per le approvazioni, è consigliabile concedergli anche il ruolo di membro o visualizzatore del progetto.

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker			
				L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
Accesso a Service Broker							
Console	Nella console, è possibile visualizzare e aprire Service Broker	Sì	Sì	Sì	Sì	Sì	Sì
Infrastruttura							
	Visualizzare e aprire la scheda Infrastruttura	Sì	Sì				
Configurazione - Progetti	Creare progetti	Sì					
	Aggiornare o eliminare i valori da riepilogo del progetto, provisioning, Kubernetes e integrazioni, nonché testare le configurazioni dei progetti.	Sì					
	Aggiungere utenti e gruppi, nonché assegnare ruoli nei progetti.	Sì		Sì. Progetti personali.			
	Visualizzare i progetti	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
Configurazione - Zone cloud	Creare, aggiornare o eliminare le zone cloud	Sì					
	Visualizzare le zone cloud	Sì	Sì				
Configurazione - Zone Kubernetes	Creare, aggiornare o eliminare le zone Kubernetes	Sì					
	Visualizzare le zone Kubernetes	Sì	Sì				
Connessioni - Account cloud	Creare, aggiornare o eliminare gli account cloud	Sì					
	Visualizzare gli account cloud	Sì	Sì				
Connessioni - Integrazioni	Creare, aggiornare o eliminare le integrazioni	Sì					
	Visualizzare le integrazioni	Sì	Sì				
Attività - Richieste	Eliminare i record delle richieste di distribuzione	Sì					
	Visualizzare i record delle richieste di distribuzione	Sì					
Attività - Registri eventi	Visualizzare i registri eventi	Sì					
Contenuto e criteri							

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Visualizzare e aprire la scheda Contenuto e criteri	Sì	Sì				
Origini contenuto	Creare, aggiornare o eliminare le origini del contenuto	Sì					
	Visualizzare le origini del contenuto	Sì	Sì				
Condivisione contenuto	Aggiungere o rimuovere il contenuto condiviso	Sì					
	Visualizzare il contenuto condiviso	Sì	Sì				
Contenuto	Personalizzare modulo e configurare l'elemento	Sì					
	Visualizzare il contenuto	Sì	Sì				
Criteri - Definizioni	Creare, aggiornare o eliminare le definizioni dei criteri	Sì					
	Visualizzare le definizioni dei criteri	Sì	Sì				
Criteri - Imposizione	Visualizzare il registro di imposizioni	Sì	Sì				
Notifiche - Server email	Configurare un server email	Sì					
Catalogo							

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Visualizzare e aprire la scheda Catalogo	Sì	Sì	Sì	Sì	Sì	Sì
	Visualizzare gli elementi del catalogo disponibili	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
	Richiedere un elemento del catalogo	Sì		Sì. Progetti personali	Sì. Progetti personali		
Risorse							
	Visualizzare e aprire la scheda Risorse	Sì	Sì	Sì.	Sì	Sì	Sì
Distribuzioni	Visualizzare le distribuzioni, inclusi dettagli della distribuzione, cronologia delle distribuzioni, prezzo, monitoraggio, avvisi, ottimizzazione e informazioni sulla risoluzione dei problemi	Sì	Sì	Sì. Progetti personali	Sì. Progetti personali	Sì. Progetti personali	
	Gestire gli avvisi	Sì		Sì. Progetti personali	Sì. Progetti personali		
	Eseguire azioni giorno 2 nelle distribuzioni in base ai criteri	Sì		Sì. Progetti personali	Sì. Progetti personali		
Risorse - Tutte le risorse	Visualizzazione di tutte le risorse rilevate	Sì	Sì				

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Eseguire azioni giorno 2 sulle risorse rilevate. Azioni disponibili solo sulle macchine e limitate all'accensione e allo spegnimento per tutte le macchine e console remote per le macchine vSphere.	Sì					
Risorse - Tutte le risorse	Visualizzare le risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	
	Eseguire azioni giorno 2 sulle risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione in base ai criteri	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.		
Risorse - Macchine virtuali	Visualizzare le macchine rilevate	Sì	Sì				

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Eseguire azioni giorno 2 sulle macchine rilevate. Le azioni sono limitate all'accensione e allo spegnimento e alla console remota per le macchine vSphere.	Sì					
	Creare nuova macchina virtuale	Sì					
	Visualizzare le risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione.	Sì		Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	
	Eseguire azioni giorno 2 sulle risorse distribuite, di cui è stato eseguito l'onboarding e la migrazione in base ai criteri	Sì		Sì. Progetti personali.	Sì. Progetti personali.		
Risorse - Volumi	Visualizzare i volumi rilevati	Sì	Sì				
	Nessuna azione giorno 2 disponibile						

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Visualizzare i volumi distribuiti, sottoposti a onboarding e migrati	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	
	Eseguire azioni giorno 2 sui volumi distribuiti, sottoposti a onboarding e migrati in base ai criteri	Sì		Sì. Progetti personali.	Sì. Progetti personali.		
Risorse - Rete e sicurezza	Visualizzare reti, bilanciamenti del carico e gruppi di sicurezza rilevati	Sì	Sì				
	Nessuna azione giorno 2 disponibile						
	Visualizzare le reti, i bilanciamenti del carico e i gruppi di sicurezza distribuiti, di cui è stato eseguito l'onboarding e migrati	Sì	Sì	Sì. Progetti personali.	Sì. Progetti personali.	Sì. Progetti personali.	

Tabella 3-4. Ruoli di servizio e ruoli di progetto di Service Broker (continua)

Contesto dell'interfaccia utente	Attività	Amministratore di Service Broker	Visualizzatore di Service Broker	Utente di Service Broker L'utente deve essere un amministratore del progetto per visualizzare ed eseguire attività correlate al progetto.			
				Amministratore del progetto	Membro del progetto	Visualizzatore del progetto	Supervisore del progetto
	Eseguire azioni giorno 2 su reti, bilanciamenti del carico e gruppi di sicurezza distribuiti di cui è stato eseguito l'onboarding e migrati in base ai criteri	Sì		Sì. Progetti personali.	Sì. Progetti personali.		
Approvazioni							
	Visualizzare e aprire la scheda Approvazioni	Sì	Sì	Sì	Sì	Sì	Sì
	Rispondere alle richieste di approvazione	Sì		Sì. L'approvatore dei progetti e del criterio è l'amministratore del progetto	Solo se l'utente è un approvatore denominato	Solo se l'utente è un approvatore denominato	Sì. L'approvatore dei progetti e del criterio è il supervisore del progetto

Ruoli di servizio di Code Stream

I ruoli di servizio di Code Stream determinano ciò che è possibile visualizzare ed eseguire in Code Stream. Questi ruoli sono definiti nella console dal proprietario dell'organizzazione. Qualsiasi progetto è disponibile in tutti i servizi.

Tabella 3-5. Descrizioni dei ruoli servizio di Code Stream

Ruolo	Descrizione
Amministratore di Code Stream	Utente che dispone di accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può visualizzare qualsiasi contenuto ed eseguire qualsiasi operazione, inclusi creare progetti, integrare endpoint, aggiungere trigger, creare pipeline e dashboard personalizzate, contrassegnare endpoint e variabili come risorse limitate, eseguire pipeline che utilizzano risorse limitate e richiedere che le pipeline siano pubblicate in Service Broker.
Sviluppatore Code Stream	Un utente che può lavorare con le pipeline, ma non può lavorare con endpoint o variabili limitati. Se una pipeline include una variabile o un endpoint limitato, questo utente deve ottenere l'approvazione nell'attività della pipeline che utilizza l'endpoint o la variabile con restrizioni.
Esecutore Code Stream	Utente che può eseguire pipeline e approvare o rifiutare le attività operative degli utenti. Questo utente può riprendere, sospendere e annullare le esecuzioni delle pipeline, ma non può modificare le pipeline.
Utente di Code Stream	Utente che può accedere a Code Stream, ma che non dispone di alcun altro privilegio in Code Stream.
Visualizzatore di Code Stream	Utente che ha accesso in lettura per visualizzare pipeline, endpoint, esecuzioni di pipeline e dashboard, ma che non può crearli, aggiornarli o eliminarli. Un utente che dispone anche del ruolo di visualizzatore del servizio può visualizzare tutte le informazioni disponibili per l'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.

Oltre ai ruoli di servizio, Code Stream dispone di ruoli di progetto. Qualsiasi progetto è disponibile in tutti i servizi.

I ruoli di progetto sono definiti in Code Stream e possono variare tra i progetti.

Nelle tabelle seguenti, che descrivono cosa possono visualizzare ed eseguire i diversi ruoli servizio e progetto, è necessario tenere presente che gli amministratori dei servizi hanno autorizzazione completa in tutte le aree dell'interfaccia utente.

Utilizzare le seguenti descrizioni dei ruoli di progetto come ausilio nel decidere quali autorizzazioni concedere agli utenti.

- Gli amministratori del progetto sfruttano l'infrastruttura creata dall'amministratore del servizio per garantire che i loro membri del progetto dispongano delle risorse di cui hanno bisogno per le operazioni di sviluppo. L'amministratore del progetto può aggiungere membri.
- I membri del progetto che hanno un ruolo servizio possono utilizzare i servizi.
- I visualizzatori del progetto possono visualizzare i progetti ma non possono crearli, aggiornarli o eliminarli.

Tutte le azioni ad eccezione delle limitazioni indica che questo ruolo dispone dell'autorizzazione a eseguire azioni di creazione, lettura, aggiornamento ed eliminazione su entità, ad eccezione di variabili ed endpoint limitati.

Tabella 3-6. Funzionalità dei ruoli di servizio di Code Stream

Contesto dell'interfaccia utente	Funzionalità	Ruolo di amministratore di Code Stream	Ruolo di sviluppatore di Code Stream	Ruolo di esecutore di Code Stream	Ruolo di visualizzatore di Code Stream	Ruolo di utente di Code Stream
Pipeline						
	Visualizzare pipeline	Sì	Sì	Sì	Sì	
	Creare pipeline	Sì	Sì			
	Eseguire pipeline	Sì	Sì	Sì		
	Eseguire le pipeline che includono variabili o endpoint limitati	Sì				
	Aggiornare pipeline	Sì	Sì			
	Eliminare pipeline	Sì	Sì			
Esecuzioni di pipeline						
	Visualizzare esecuzioni di pipeline	Sì	Sì	Sì	Sì	
	Riprendere, sospendere e annullare le esecuzioni delle pipeline	Sì	Sì	Sì		
	Riprendere le pipeline che vengono interrotte per l'approvazione su risorse limitate	Sì				
Integrazioni personalizzate						
	Creare integrazioni personalizzate	Sì	Sì			
	Leggere integrazioni personalizzate	Sì	Sì	Sì	Sì	

Tabella 3-6. Funzionalità dei ruoli di servizio di Code Stream (continua)

Contesto dell'interfaccia utente	Funzionalità	Ruolo di amministratore di Code Stream	Ruolo di sviluppatore di Code Stream	Ruolo di esecutore di Code Stream	Ruolo di visualizzatore di Code Stream	Ruolo di utente di Code Stream
	Aggiornare integrazioni personalizzate	Sì	Sì			
Endpoint						
	Visualizzare esecuzioni	Sì	Sì	Sì	Sì	
	Creare esecuzioni	Sì	Sì			
	Aggiornare esecuzioni	Sì	Sì			
	Eliminare esecuzioni	Sì	Sì			
Contrassegnare le risorse come limitate						
	Contrassegnare una variabile o un endpoint come limitati	Sì				
Dashboard						
	Visualizzare dashboard	Sì	Sì	Sì	Sì	
	Creare dashboard	Sì	Sì			
	Aggiornare dashboard	Sì	Sì			
	Eliminare dashboard	Sì	Sì			

Ruoli del servizio Assistente migrazione vRA

I ruoli del servizio Assistente migrazione vRA determinano cosa è possibile visualizzare ed eseguire nell'assistente migrazione di vRA e in Cloud Assembly. Questi ruoli di servizio sono definiti nella console da un proprietario dell'organizzazione.

Tabella 3-7. Descrizioni dei ruoli del servizio Assistente migrazione di vRealize Automation

Ruolo	Descrizione
Amministratore assistente migrazione	<p>Utente che dispone di privilegi di visualizzazione, aggiornamento ed eliminazione completi nell'assistente migrazione di vRA e in Cloud Assembly.</p> <p>Questo ruolo deve anche includere almeno il ruolo Visualizzatore di Cloud Assembly.</p>
Visualizzatore assistente migrazione	<p>Utente che dispone dell'accesso in lettura per visualizzare le informazioni ma che non può creare, aggiornare o eliminare i valori nell'assistente migrazione vRA o in Cloud Assembly.</p> <p>Questo ruolo deve anche includere almeno il ruolo Visualizzatore di Cloud Assembly.</p>

Ruoli del servizio Orchestrator

I ruoli di servizio Orchestrator determinano ciò che è possibile visualizzare ed eseguire nel client di vRealize Orchestrator. Questi ruoli di servizio sono definiti nella console da un proprietario dell'organizzazione.

Tabella 3-8. Descrizione dei ruoli del servizio vRealize Orchestrator

Ruolo	Descrizione
Amministratore Orchestrator	<p>Utente che dispone di privilegi di visualizzazione, aggiornamento ed eliminazione completi in vRealize Orchestrator. Un amministratore può inoltre accedere ai contenuti creati da gruppi specifici.</p>
Visualizzatore Orchestrator	<p>Utente che dispone dell'accesso in lettura per visualizzare funzionalità e contenuti, inclusi tutti i gruppi e i contenuti dei gruppi, ma che non può creare, aggiornare, eseguire, eliminare valori o esportare contenuti.</p>
Progettista di workflow di Orchestrator	<p>Utente che può creare, eseguire, modificare ed eliminare i propri contenuti del client di vRealize Orchestrator. Può aggiungere i propri contenuti al gruppo a cui è assegnato. Il progettista di workflow non può accedere alle funzionalità di amministrazione e risoluzione dei problemi del client di vRealize Orchestrator.</p>

Ruolo del servizio di SaltStack Config

Il ruolo del servizio SaltStack Config determina ciò che è possibile visualizzare ed eseguire nelle vRealize Automation. Il ruolo del servizio è definito nella console da un proprietario dell'organizzazione.

Tabella 3-9. Descrizione del ruolo del servizio SaltStack Config di vRealize Automation

Ruolo	Descrizione
Amministratore di SaltStack Config	Utente che può accedere al riquadro SaltStack Config nella console quando è configurata l'integrazione con Cloud Assembly. Per accedere all'istanza di SaltStack Config, l'utente deve disporre delle autorizzazioni di amministratore di SaltStack definite in SaltStack Config. L'utente deve inoltre ricoprire il ruolo di amministratore di Cloud Assembly.

Ruoli utente personalizzati in vRealize Automation

Gli amministratori di Cloud Assembly possono creare ruoli personalizzati che definiscono gli elementi visualizzabili e le operazioni eseguibili dagli utenti in vRealize Automation. A questi ruoli possono quindi essere assegnati utenti.

Autorizzazioni dei ruoli utente personalizzati

Utilizzando Cloud Assembly, è possibile definire ruoli utente più granulari e quindi assegnare gli utenti a tali ruoli. I ruoli personalizzati presentano due categorie: visualizzazione e gestione.

- **Visualizzazione.** Un utente assegnato a un ruolo con questa autorizzazione può vedere tutti gli elementi per tutti i progetti nelle sezioni selezionate dell'interfaccia utente. Questo ruolo è utile per gli utenti che devono visualizzare account, configurazioni o valori assegnati.
- **Gestione.** Un utente assegnato a un ruolo con questa autorizzazione può vedere tutti gli elementi e dispone di autorizzazioni complete per l'aggiunta, la modifica e l'eliminazione per tutti i progetti nelle sezioni selezionate dell'interfaccia utente.

Queste autorizzazioni estendono i privilegi concessi dagli altri ruoli e non sono limitate dall'appartenenza al progetto. Ad esempio, è possibile espandere le autorizzazioni di un amministratore di progetto per gestire parti dell'infrastruttura o fornire a un visualizzatore servizi la possibilità di esaminare e rispondere alle richieste di approvazione.

Per definire i ruoli utente e assegnare gli utenti, aprire Cloud Assembly o Service Broker in qualità di amministratore servizio e scegliere **Infrastruttura > Amministrazione > Ruoli personalizzati**. Non è possibile configurare i ruoli personalizzati in Code Stream, tuttavia i ruoli si applicano a tutti i servizi.

Tabella 3-10. Ruoli personalizzati

Interfaccia utente	Autorizzazione	Descrizione
Infrastruttura		
	Visualizza account cloud	Visualizzare gli account cloud.
	Gestisci account cloud	Creare, aggiornare ed eliminare gli account cloud.

Tabella 3-10. Ruoli personalizzati (continua)

Interfaccia utente	Autorizzazione	Descrizione
	Visualizza mappature delle immagini	Visualizzare le mappature delle immagini.
	Gestisci mappature delle immagini	Creare, aggiornare ed eliminare mappature di immagini.
	Visualizza mappature delle caratteristiche	Visualizzare le mappature delle caratteristiche.
	Gestisci mappature delle caratteristiche	Creare, aggiornare ed eliminare le mappature di caratteristiche.
	Visualizza zone cloud	Visualizzare le zone cloud, i dettagli e gli avvisi.
	Gestisci zone cloud	Creare, aggiornare ed eliminare zone cloud. Gestire gli avvisi.
	Visualizza richieste	Visualizza le richieste di attività.
	Gestisci richieste	Eliminare richieste dall'elenco.
	Visualizza integrazioni	Visualizzare le integrazioni.
	Gestisci integrazioni	Creare, aggiornare ed eliminare le integrazioni.
	Visualizza progetti	Visualizzare i progetti.
	Gestisci progetti	Creare progetti. Aggiungere utenti e assegnare ruoli nei progetti. Aggiornare o eliminare i valori da riepilogo del progetto, utenti, provisioning, Kubernetes, integrazioni e configurazioni del progetto di prova.
	Visualizza piani di onboarding	Visualizzare i piani di onboarding
	Gestisci piani di onboarding	Creare, aggiornare, eseguire ed eliminare piani di onboarding
Catalogo		
	Visualizza contenuto	
	Gestisci contenuto	Aggiungere, aggiornare, eliminare le origini di contenuti. Condividere contenuti. Personalizzare i contenuti, incluse le icone del catalogo e i moduli di richiesta.
Criteri		
	Visualizza criteri	Visualizzare le definizioni dei criteri.

Tabella 3-10. Ruoli personalizzati (continua)

Interfaccia utente	Autorizzazione	Descrizione
	Gestisci criteri	Creare, aggiornare ed eliminare le definizioni dei criteri.
Distribuzioni		
	Visualizza distribuzioni	Visualizzare tutte le distribuzioni, inclusi dettagli della distribuzione, la cronologia delle distribuzioni, gli avvisi e le informazioni sulla risoluzione dei problemi.
	Gestisci distribuzioni	Visualizzare tutte le distribuzioni, rispondere agli avvisi ed eseguire tutte le azioni del giorno 2 che i criteri di giorno 2 consentono a un amministratore di eseguire su distribuzioni e componenti delle distribuzioni.
Modelli cloud		
	Visualizza modelli cloud	Visualizzare modelli cloud.
	Gestisci modelli cloud	Creare, aggiornare, testare, eliminare, assegnare una versione, condividere modelli cloud e rilasciare/annullare il rilascio di una versione di modello cloud.
	Modifica modelli cloud	Creare, aggiornare, testare, assegnare una versione, condividere modelli cloud e rilasciare/annullare il rilascio di una versione di modello cloud. Il ruolo non dispone dell'autorizzazione per eliminare modelli cloud.
	Distribuisci modelli cloud	Testare e distribuire qualsiasi modello cloud in qualsiasi progetto.
	Distribuisci contenuti di modelli cloud in linea	Distribuire qualsiasi modello cloud nei progetti a cui sono associati gli assegnatari. I ruoli del progetto possono essere amministratore, membro o visualizzatore.
XaaS		
	Visualizza risorse personalizzate	Visualizzare le risorse personalizzate.
	Gestisci risorse personalizzate	Creare, aggiornare o eliminare risorse personalizzate.
	Visualizza azioni risorsa	Visualizzare le azioni personalizzate.

Tabella 3-10. Ruoli personalizzati (continua)

Interfaccia utente	Autorizzazione	Descrizione
	Gestisci azioni risorsa	Creare, aggiornare o eliminare le azioni personalizzate
Estendibilità		
	Visualizza risorse estendibilità	Visualizza eventi, sottoscrizioni, argomenti degli eventi, azioni, workflow, esecuzioni di azioni ed esecuzioni di workflow.
	Gestisci risorse estendibilità	<p>Creare, aggiornare, eliminare e disattivare le sottoscrizioni di estendibilità.</p> <p>Creare, aggiornare ed eliminare le azioni di estendibilità. Annullare ed eliminare le esecuzioni delle azioni di estendibilità.</p>
Pipeline		
	Gestisci pipeline	<p>Creare, modificare ed eliminare le configurazioni di pipeline, endpoint, variabili e trigger.</p> <p>Sono esclusi i modelli con restrizioni.</p>
	Gestisci pipeline limitate	<p>Creare, modificare ed eliminare le configurazioni di pipeline, endpoint, variabili e trigger.</p> <p>Sono inclusi i modelli con restrizioni.</p>
	Gestisci integrazioni personalizzate	Aggiungere, modificare ed eliminare integrazioni personalizzate.
	Esegui pipeline	Eseguire trigger ed esecuzioni di modelli di pipeline, nonché sospendere, annullare, riprendere ed eseguire di nuovo trigger ed esecuzioni.
	Esegui pipeline limitate	<p>Eseguire trigger ed esecuzioni di modelli di pipeline, nonché sospendere, annullare, riprendere ed eseguire di nuovo trigger ed esecuzioni.</p> <p>Risolvere variabili ed endpoint con restrizioni.</p>
	Gestisci esecuzioni	<p>Eseguire trigger ed esecuzioni di modelli di pipeline, nonché sospendere, annullare, riprendere ed eseguire di nuovo trigger ed esecuzioni.</p> <p>Risolvere variabili ed endpoint con restrizioni.</p> <p>Eliminare le esecuzioni.</p>

Tabella 3-10. Ruoli personalizzati (continua)

Interfaccia utente	Autorizzazione	Descrizione
Approvazione		
	Gestisci approvazioni	<p>Visualizzare la scheda Approvazioni in cui è possibile approvare o rifiutare le richieste di approvazione.</p> <p>L'approvatore dotato di questo ruolo non riceverà una notifica e-mail su una richiesta di approvazione a meno che non sia un approvatore nel criterio.</p>

Casi d'uso: in che modo i ruoli utente possono consentire il controllo dell'accesso in vRealize Automation

In qualità amministratore del cloud, si desidera controllare le attività che gli utenti possono eseguire in vRealize Automation. In base agli obiettivi di gestione e alle responsabilità del team di sviluppo delle applicazioni, sono disponibili diverse modalità per configurare i ruoli utente in modo da supportare tali obiettivi.

I seguenti esempi di Cloud Assembly e Service Broker si basano su tre casi d'uso. Questi esempi forniscono solo istruzioni sufficienti per illustrare l'applicazione dei ruoli degli utenti.

I destinatari di questi casi d'uso sono l'amministratore del cloud, che è anche considerato l'amministratore del cloud, e gli amministratori del servizio.

I casi d'uso sono uno correlato all'altro. Se si è pronti ad accedere direttamente al caso d'uso 3, potrebbe essere necessario rivedere i casi d'uso 1 e 2 per comprendere meglio il motivo per cui si configurano i ruoli nei modi specificati.

Lo scopo dei casi d'uso è illustrare i ruoli utente, non fornire informazioni dettagliate sulla configurazione dell'infrastruttura, gestire i progetti, creare modelli cloud lavorare con le distribuzioni.

Prima di iniziare, è necessario comprendere i livelli dei ruoli utente configurati da un amministratore del cloud nella console di vRealize Automation.

■ Ruoli dell'organizzazione

I ruoli dell'organizzazione controllano chi può accedere alla console.

In qualità di proprietario di un'organizzazione, è necessario assicurarsi che a tutti gli utenti di qualsiasi servizio venga assegnato almeno un ruolo di membro dell'organizzazione.

Ruolo	Descrizione
Proprietario dell'organizzazione	Un amministratore può aggiungere utenti, modificare il ruolo degli utenti e rimuovere gli utenti dall'organizzazione. Il proprietario gestisce i servizi a cui gli utenti possono accedere.
Membro dell'organizzazione	Un utente generale può accedere alla console dell'organizzazione. Per accedere ai servizi, un proprietario dell'organizzazione deve assegnare i ruoli dei servizi degli utenti.

■ Ruoli di servizio

I ruoli dei servizi controllano chi può accedere ai servizi assegnati.

In qualità di proprietario dell'organizzazione, è necessario assicurarsi che agli utenti che necessitano dell'accesso ai servizi sia assegnato il ruolo appropriato. È possibile utilizzare i ruoli per controllare la quantità di attività dell'utente in ogni servizio.

Tabella 3-11. Descrizioni dei ruoli di servizio di Cloud Assembly

Ruolo	Descrizione
Amministratore di Cloud Assembly	Utente che dispone di accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può visualizzare ed eseguire tutto, ad esempio aggiungere account cloud, creare nuovi progetti e assegnare un amministratore del progetto.
Utente di Cloud Assembly	Un utente che non dispone del ruolo di amministratore di Cloud Assembly. In un progetto di Cloud Assembly, l'amministratore aggiunge gli utenti ai progetti come membri del progetto, amministratori o visualizzatori. L'amministratore può anche aggiungere un amministratore del progetto.
Visualizzatore di Cloud Assembly	Utente che ha accesso in lettura per visualizzare le informazioni ma che non può creare, aggiornare o eliminare valori. Si tratta di un ruolo di sola lettura in tutti i progetti. Gli utenti con il ruolo di visualizzatore possono visualizzare tutte le informazioni disponibili all'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.

Tabella 3-12. Descrizioni dei ruoli di servizio di Service Broker

Ruolo	Descrizione
Amministratore di Service Broker	Deve disporre dell'accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può eseguire tutte le attività, ad esempio la creazione di un nuovo progetto e l'assegnazione di un amministratore del progetto.
Utente di Service Broker	Qualsiasi utente che non disponga del ruolo di amministratore di Service Broker.

Tabella 3-12. Descrizioni dei ruoli di servizio di Service Broker (continua)

Ruolo	Descrizione
	In un progetto di Service Broker, l'amministratore aggiunge gli utenti ai progetti come membri del progetto, amministratori o visualizzatori. L'amministratore può anche aggiungere un amministratore del progetto.
Visualizzatore di Service Broker	<p>Utente che ha accesso in lettura per visualizzare le informazioni ma che non può creare, aggiornare o eliminare valori.</p> <p>Gli utenti con il ruolo di visualizzatore possono visualizzare tutte le informazioni disponibili all'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.</p>

Tabella 3-13. Descrizioni dei ruoli servizio di Code Stream

Ruolo	Descrizione
Amministratore di Code Stream	Utente che dispone di accesso in lettura e scrittura all'intera interfaccia utente e alle risorse API. Questo è l'unico ruolo utente che può visualizzare qualsiasi contenuto ed eseguire qualsiasi operazione, inclusi creare progetti, integrare endpoint, aggiungere trigger, creare pipeline e dashboard personalizzate, contrassegnare endpoint e variabili come risorse limitate, eseguire pipeline che utilizzano risorse limitate e richiedere che le pipeline siano pubblicate in Service Broker.
Sviluppatore Code Stream	Un utente che può lavorare con le pipeline, ma non può lavorare con endpoint o variabili limitati. Se una pipeline include una variabile o un endpoint limitato, questo utente deve ottenere l'approvazione nell'attività della pipeline che utilizza l'endpoint o la variabile con restrizioni.
Esecutore Code Stream	Utente che può eseguire pipeline e approvare o rifiutare le attività operative degli utenti. Questo utente può riprendere, sospendere e annullare le esecuzioni delle pipeline, ma non può modificare le pipeline.
Utente di Code Stream	Utente che può accedere a Code Stream, ma che non dispone di alcun altro privilegio in Code Stream.
Visualizzatore di Code Stream	Utente che ha accesso in lettura per visualizzare pipeline, endpoint, esecuzioni di pipeline e dashboard, ma che non può crearli, aggiornarli o eliminarli. Un utente che dispone anche del ruolo di visualizzatore del servizio può visualizzare tutte le informazioni disponibili per l'amministratore. Non può eseguire alcuna azione a meno che un amministratore non lo renda amministratore del progetto o membro del progetto. Se l'utente è associato a un progetto, dispone delle autorizzazioni correlate al ruolo. Il visualizzatore del progetto non estenderebbe le proprie autorizzazioni nel modo in cui avviene per il ruolo di amministratore o membro.

■ Ruoli di appartenenza al progetto

L'appartenenza al progetto determina quali risorse e modelli cloud dell'infrastruttura sono disponibili.

L'appartenenza al progetto viene definita nel servizio da un utente con ruolo di amministratore del servizio. L'amministratore del servizio deve assicurarsi che agli utenti che necessitano dell'accesso a uno o più progetti sia assegnato il ruolo di progetto appropriato in ogni progetto.

Tabella 3-14. Ruoli di progetto

Ruolo	Descrizione
Amministratore del progetto	Un amministratore del progetto può gestire i propri progetti, creare e distribuire modelli cloud associati ai propri progetti e gestire le distribuzioni dei progetti per tutti i membri del progetto.
Membro del progetto	Un membro del progetto può creare e distribuire modelli cloud associati ai propri progetti, gestire le proprie distribuzioni e gestire tutte le distribuzioni condivise.
Visualizzatore del progetto	Un visualizzatore del progetto è un membro del progetto con accesso in sola lettura ai modelli cloud, alle distribuzioni e alle risorse del progetto.

■ Ruoli personalizzati

I ruoli personalizzati vengono creati da Cloud Assembly per perfezionare i ruoli di membro e visualizzatore.

Le procedure fornite in questi casi d'uso hanno lo scopo di evidenziare i ruoli utente. Non sono procedure dettagliate o definitive per la configurazione di vRealize Automation.

Quando si configurano i ruoli, tenere presente che gli utenti che eseguono le operazioni dell'API sono soggetti ai ruoli assegnati in questa sezione.

Prerequisiti

- Verificare di disporre del ruolo di proprietario dell'organizzazione. È necessario visualizzare la scheda **Gestione identità e accessi** dopo aver effettuato l'accesso alla console. In caso contrario, contattare il proprietario dell'organizzazione.
- Verificare di rivestire il ruolo di amministratore del servizio per i vari servizi. Se non si è certi del proprio ruolo, contattare il proprietario dell'organizzazione.
- Verificare che gli utenti siano stati aggiunti a vRealize Automation.

Quando si installa vRealize Automation, gli utenti di Active Directory vengono aggiunti come parte del processo.

- Per un elenco di attività e ruoli più dettagliato per i vari ruoli, vedere [Organizzazione e ruoli utente dei servizi in vRealize Automation](#).

Procedura

1 Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni

In qualità di amministratore del cloud di vRealize Automation, l'utente è responsabile della gestione dell'accesso e del budget per le risorse dell'infrastruttura. Aggiungere se stessi e altri due utenti come amministratori. Questo team di piccole dimensioni può creare l'infrastruttura e sviluppare i modelli cloud che corrispondono agli obiettivi aziendali dei team che utilizzano i modelli cloud. L'utente e il gruppo di amministratori di piccole dimensioni distribuiscono i modelli cloud per i consumatori non amministratori, senza consentire ai non amministratori di accedere a vRealize Automation.

2 Caso d'uso ruolo utente 2: configurazione dei ruoli utente di vRealize Automation per supportare team di sviluppo più grandi e il catalogo

In qualità di proprietario dell'organizzazione di vRealize Automation, l'utente è responsabile della gestione dell'accesso e del budget per le risorse dell'infrastruttura. Si dispone di un team di sviluppatori di modelli cloud che creano e distribuiscono in modo iterativo i modelli per progetti diversi finché non sono pronti per la distribuzione ai consumatori. È quindi possibile inviare le risorse distribuibili ai clienti in un catalogo.

3 Caso d'uso ruolo utente 3: configurazione dei ruoli utente personalizzati di vRealize Automation per perfezionare i ruoli di sistema

Il proprietario dell'organizzazione o l'amministratore del servizio di vRealize Automation può gestire l'accesso degli utenti utilizzando i ruoli del sistema di organizzazione e servizio. Si desidera però creare anche ruoli personalizzati per gli utenti selezionati ed eseguire attività o visualizzare contenuti che non rientrano nei rispettivi ruoli di sistema.

Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni

In qualità di amministratore del cloud di vRealize Automation, l'utente è responsabile della gestione dell'accesso e del budget per le risorse dell'infrastruttura. Aggiungere se stessi e altri due utenti come amministratori. Questo team di piccole dimensioni può creare l'infrastruttura e sviluppare i modelli cloud che corrispondono agli obiettivi aziendali dei team che utilizzano i modelli cloud. L'utente e il gruppo di amministratori di piccole dimensioni distribuiscono i modelli cloud per i consumatori non amministratori, senza consentire ai non amministratori di accedere a vRealize Automation.

In questo caso d'uso, si è proprietari dell'organizzazione e si dispone di un team di piccole dimensioni in cui tutti hanno il ruolo di amministratore del servizio.

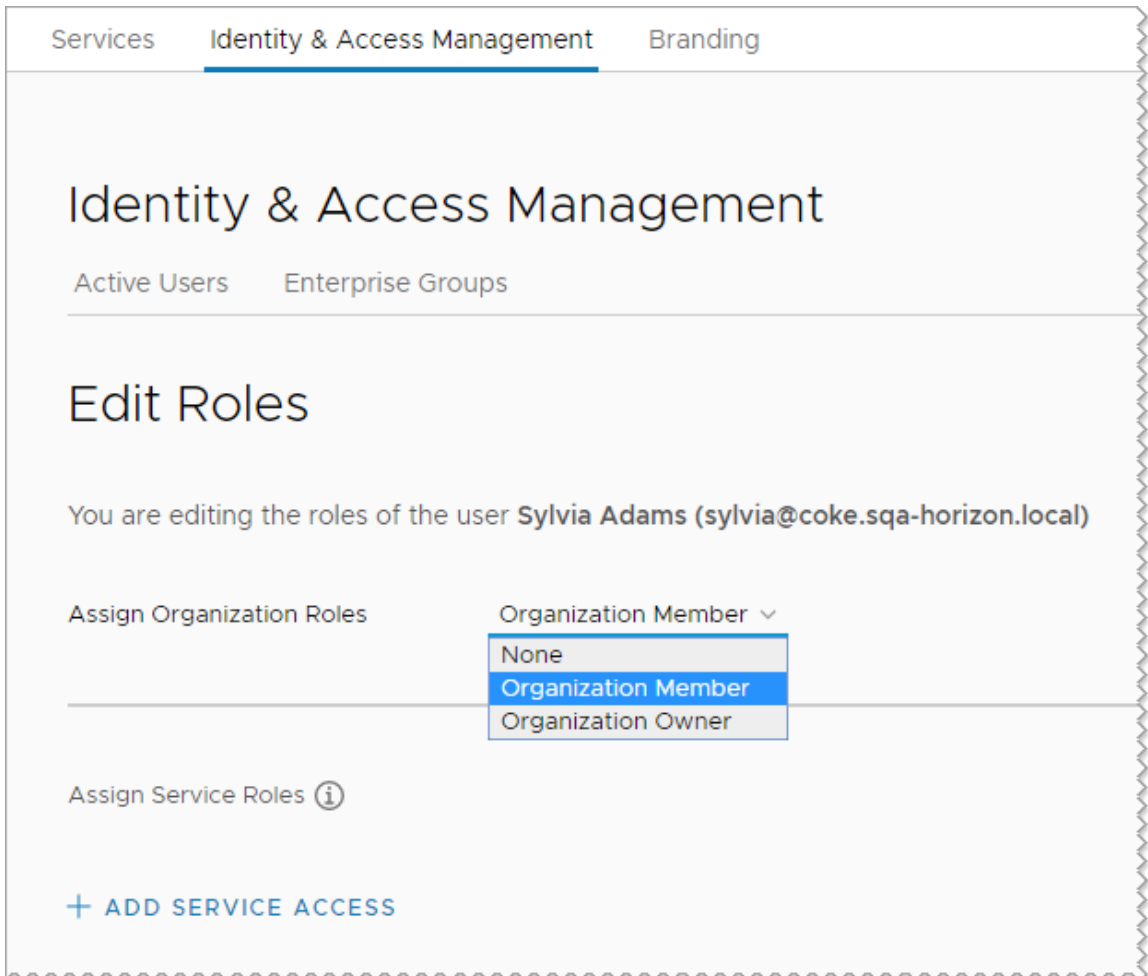
La seguente procedura segue un utente lungo tutto il processo. È possibile eseguire ogni passaggio per più utenti.

Prerequisiti

- Verificare di soddisfare tutti i prerequisiti previsti nell'introduzione del caso d'uso. Vedere [Casi d'uso: in che modo i ruoli utente possono consentire il controllo dell'accesso in vRealize Automation](#).

Procedura

- 1 Assegnare i ruoli dell'organizzazione. Fare clic su **Gestione identità e accessi**.
 - a Effettuare l'accesso alla console di vRealize Automation.
 - b Fare clic su **Gestione identità e accessi**.
 - c Selezionare il nome utente e fare clic su **Modifica ruoli**.
 - d Nel menu a discesa **Assegna ruoli organizzazione**, selezionare **Membro dell'organizzazione**.



Il ruolo di membro dell'organizzazione garantisce che l'utente possa accedere alla console e a tutti i servizi a cui è stato aggiunto. Non può gestire gli utenti dell'organizzazione.

Lasciare aperta la pagina Modifica ruolo per questo utente e continuare con il passaggio successivo.

- 2 Assegnare il ruolo Amministratore di Cloud Assembly a se stessi e a uno o due altri amministratori in questo scenario.

Il ruolo di amministratore del servizio dispone di privilegi completi per aggiungere, modificare ed eliminare l'infrastruttura, i progetti, i modelli cloud e le distribuzioni. La definizione di un ruolo di amministratore per una persona e il ruolo utente per una un'altra è contemplata nello scenario 2. In questo esempio si utilizza Sylvia.

- a Fare clic su **Aggiungi accesso al servizio**.
- b Configurare l'utente con il valore seguente.

Servizio	Ruolo
Cloud Assembly	Amministratore di Cloud Assembly

[Services](#)
[Identity & Access Management](#)
[Branding](#)

Identity & Access Management

Active Users Enterprise Groups

Edit Roles

You are editing the roles of the user **Sylvia Adams** (sylvia@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Cloud Assembly ▾
 with roles
 Cloud Assembly Administrator ▾
 ×

[+ ADD SERVICE ACCESS](#)

- 3 Creare un progetto in Cloud Assembly da utilizzare per raggruppare le risorse e gestire la fatturazione delle risorse per gruppi di business diversi.

- a Nella console, fare clic sulla scheda **Servizi**, quindi fare clic su **Cloud Assembly**.
- b Selezionare **Infrastruttura > Progetti > Nuovo progetto**.

Questo caso d'uso sui ruoli utente è incentrato su esempi che consentono di comprendere come implementare i ruoli utente, non sulla creazione del sistema completamente definito.

Per informazioni sulla configurazione dell'infrastruttura, vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#). Per ulteriori informazioni sui progetti, vedere [Capitolo 5 Aggiunta e gestione di progetti di Cloud Assembly](#).

- c Immettere **WebAppTeam** come nome del progetto.

- d Fare clic su **Utenti**, quindi fare clic su **Aggiungi utenti**.
- e Immettere gli indirizzi e-mail degli utenti che possono aiutare a creare e gestire l'infrastruttura e i modelli cloud.

Ad esempio, tony@mycompany.com, syliva@mycompany.com.

- f Nel menu a discesa **Assegna ruolo**, selezionare **Amministratore**.

In qualità di amministratori di Cloud Assembly, questi due utenti dispongono già di accesso amministratore agli account cloud, all'infrastruttura e a tutti i progetti. Questo passaggio consente di comprendere i ruoli utilizzati negli scenari successivi. Negli scenari successivi, è possibile definire l'amministratore del progetto e i ruoli dei membri del progetto, che dispongono di autorizzazioni diverse.

- g Fare clic sulla scheda **Provisioning** e aggiungere una o più zone cloud.

Un altro promemoria. Questo caso d'uso riguarda i ruoli utente.

- 4 Sviluppare un modello cloud semplice in modo da poter testare il progetto WebAppTeam.

Questa sezione del modello cloud è abbreviata. Il focus sono gli utenti e i ruoli utente come definiti dai progetti, non come creare un modello cloud.

- a Selezionare **Modelli cloud > Nuovo**.
- b Per il nome del nuovo modello cloud, immettere **WebApp**.
- c Per **Progetto**, selezionare WebAppTeam.

- d Selezionare **Condividi solo con il progetto**.

Questa impostazione garantisce che il modello cloud sia disponibile solo per i membri del progetto. Quando si è pronti a fornire i modelli cloud ad altri team, è possibile selezionare **Consenti a un amministratore di condividere con qualsiasi progetto in questa organizzazione**. La condivisione del modello cloud con altri progetti significa che non è necessario mantenere istanze duplicate degli stessi modelli di base. È possibile spostare i modelli cloud dai progetti di sviluppo ai progetti di produzione in modo che i consumatori del catalogo possano distribuirli alle risorse dell'infrastruttura di produzione.

- e Fare clic su **Crea**.

- f Nel progettista di modelli cloud, trascinare il componente **Indipendente dal cloud > Macchina** nella tela.

Per ulteriori informazioni sulla configurazione dei modelli cloud, vedere [Capitolo 6 Progettazione delle distribuzioni di Cloud Assembly](#).

- g Fare clic su **Distribuisci**.
- h Continuare a iterare nel modello cloud finché non si è pronti a fornirlo ai consumatori.
- i Fare clic su **Versione** e rilasciare la versione del modello cloud.

5 Inviare agli utenti le informazioni di accesso utilizzando il metodo più comune.

Risultati

In questo caso d'uso, sono stati creati due colleghi membri dell'organizzazione. Sylvia è stata quindi resa amministratore di Cloud Assembly. Tony è stato reso amministratore del progetto WebApp. Questa configurazione dei ruoli utente è valida solo per i team di piccole dimensioni in cui si forniscono applicazioni distribuite ai consumatori anziché fornire loro accesso self-service o un catalogo.

Caso d'uso ruolo utente 2: configurazione dei ruoli utente di vRealize Automation per supportare team di sviluppo più grandi e il catalogo

In qualità di proprietario dell'organizzazione di vRealize Automation, l'utente è responsabile della gestione dell'accesso e del budget per le risorse dell'infrastruttura. Si dispone di un team di sviluppatori di modelli cloud che creano e distribuiscono in modo iterativo i modelli per progetti diversi finché non sono pronti per la distribuzione ai consumatori. È quindi possibile inviare le risorse distribuibili ai clienti in un catalogo.

Questo caso d'uso presuppone che si comprenda che il caso d'uso 1 sia destinato esclusivamente agli amministratori. A questo punto si desidera espandere il sistema per supportare più team e obiettivi più grandi.

- Consentire agli sviluppatori di creare e distribuire i propri modelli cloud di applicazioni durante lo sviluppo. Aggiungersi come amministratore, quindi aggiungere altri utenti sia con il ruolo di utente del servizio che con il ruolo di visualizzatore del servizio. Successivamente, è possibile aggiungere gli utenti come membri del progetto. I membri del progetto possono sviluppare e distribuire i propri modelli cloud.
- Pubblicare i modelli cloud in un catalogo in cui renderli disponibili per la distribuzione da parte dei non sviluppatori. A questo punto si assegnano ruoli utente per Service Broker. Service Broker fornisce un catalogo per i clienti dei modelli cloud. È inoltre possibile utilizzarlo per creare criteri, inclusi lease e autorizzazioni, ma tale funzionalità non fa parte di questo caso d'uso dei ruoli utente.

Prerequisiti

- Rivedere il primo caso d'uso. Vedere [Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni](#).

- Identificare i seguenti utenti in base alle autorizzazioni che si desidera essi debbano avere:
 - Sviluppatori di modelli cloud che saranno utenti e visualizzatori di Cloud Assembly
 - Un amministratore di Service Broker
 - Utenti non sviluppatori che saranno clienti del catalogo come utenti di Service Broker

Procedura

- 1 Assegnare i ruoli dei membri dell'organizzazione agli utenti sviluppatori di modelli cloud.
Per istruzioni, vedere il [Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni](#).
- 2 Assegnare il ruolo di membro del servizio di Cloud Assembly agli sviluppatori di modelli cloud.
 - a Fare clic su **Aggiungi accesso al servizio**.

The screenshot shows the 'Identity & Access Management' console. The 'Edit Roles' section is active for the user 'Tony Anteater (tony@coke.sqa-horizon.local)'. Under 'Assign Organization Roles', 'Organization Member' is selected. Under 'Assign Service Roles', 'Cloud Assembly' is selected, and the role 'Cloud Assembly User' is assigned. A '+ ADD SERVICE ACCESS' button is visible at the bottom.

- b Configurare l'utente con il valore seguente.

Servizio	Ruolo
Cloud Assembly	Utente di Cloud Assembly
Cloud Assembly	Visualizzatore di Cloud Assembly

In questo caso d'uso, gli sviluppatori devono visualizzare l'infrastruttura per assicurarsi che stiano creando modelli cloud distribuibili. Gli utenti che verranno assegnati come amministratori del progetto e membri del progetto nel passaggio successivo non possono visualizzare l'infrastruttura. I visualizzatori del servizio possono visualizzare la configurazione dell'infrastruttura, ma non possono apportare modifiche. In qualità di amministratore del cloud, si continua ad assumere il controllo, ma è necessario conferire loro l'accesso alle informazioni necessarie per sviluppare modelli cloud.

3 Creare progetti in Cloud Assembly utilizzati per raggruppare gli utenti di risorse.

In questo caso d'uso, è possibile creare due progetti. Il primo progetto è **PersonnelAppDev** e il secondo è **PayrollAppDev**.

- Nella console, fare clic sulla scheda **Servizi**, quindi fare clic su **Cloud Assembly**.
- Selezionare **Infrastruttura > Progetti > Nuovo progetto**.
- Immettere **PersonnelAppDev** come nome.
- Fare clic su **Utenti**, quindi fare clic su **Aggiungi utenti**.
- Aggiungere i membri del progetto e assegnare un amministratore del progetto.

Ruolo del progetto	Descrizione
Utente del progetto	Un membro del progetto è il ruolo principale degli sviluppatori in un progetto. I progetti determinano le risorse cloud disponibili quando si è pronti a testare il lavoro di sviluppo distribuendo un modello cloud.
Amministratore del progetto	Un amministratore di progetto supporta i propri sviluppatori aggiungendo e rimuovendo gli utenti per i progetti. È inoltre possibile eliminare i progetti. Per creare un progetto, è necessario disporre dei privilegi di amministratore del servizio.

- Per gli utenti che si aggiungono come membri del progetto, immettere l'indirizzo e-mail di ciascun utente, separato da una virgola, e selezionare **Utente** nel menu a discesa **Assegna ruolo**.

Ad esempio, `tony@mycompany.com,sylvia@mycompany.com`.

PersonnelAppDev DELETE

Summary **Users** Provisioning Kubernetes Provisioning Integrations

Deployment sharing ☒ Deployments are shared between all users in the project

User roles Specify the users and groups related to this project.

[+ ADD USERS](#) [+ ADD GROUPS](#) [X REMOVE](#)

Q Search users or groups

<input type="checkbox"/>	Name	Account	Role
<input type="checkbox"/>	Sylvia Adams	sylvia	Administrator
<input type="checkbox"/>	Gloria Martinez	gloria	Member
<input type="checkbox"/>	Tony Anteater	tony	Member

1 - 3 of 3 users

SAVE **CANCEL**

- Per gli amministratori designati, selezionare **Amministratore** nel menu a discesa **Assegna ruolo** e specificare l'indirizzo e-mail necessario.

- h Fare clic sulla scheda **Provisioning** e aggiungere una o più zone cloud.

Quando gli sviluppatori di modelli cloud che fanno parte di questo progetto distribuiscono un modello, vengono distribuiti nelle risorse disponibili nelle zone cloud. È necessario assicurarsi che le risorse della zona cloud corrispondano alle esigenze dei modelli del team di sviluppo del progetto.

- i Ripetere il processo per aggiungere il progetto PayrollAppDev con un amministratore e gli utenti necessari.
- 4 Fornire all'utente del servizio le informazioni di accesso necessarie e verificare che i membri di ciascun progetto possano eseguire le attività seguenti.

- a Aprire Cloud Assembly.
- b Vedere l'infrastruttura in tutti i progetti.
- c Creare un modello cloud per il progetto di cui sono membri.
- d Distribuire il modello cloud nelle risorse delle zone cloud definite nel progetto.
- e Gestire le distribuzioni.

- 5 Assegnare i ruoli dei membri dell'organizzazione agli utenti sviluppatori di modelli cloud.

Per istruzioni, vedere il [Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni](#).

- 6 Assegnare i ruoli a un amministratore del catalogo, ai consumatori del catalogo e agli sviluppatori di modelli cloud in base al lavoro che svolgono.

- a Fare clic su **Aggiungi accesso al servizio**.
- b Configurare l'amministratore del catalogo con il valore seguente.

Questo ruolo potrebbe essere l'utente, l'amministratore del cloud o qualcun altro nel team di sviluppo dell'applicazione.

Servizio	Ruolo
Service Broker	Amministratore di Service Broker

- c Configurare i consumatori dei modelli cloud con il valore seguente.

Servizio	Ruolo
Service Broker	Utente di Service Broker

Identity & Access Management

Active Users Enterprise Groups

Edit Roles

You are editing the roles of the user **Gloria Martinez** (gloria@coke.sqa-horizon.local)

Assign Organization Roles Organization Member ▾

Assign Service Roles ⓘ

Service Broker ▾

with roles

Service Broker User ▾

×

[+ ADD SERVICE ACCESS](#)

- d Configurare gli sviluppatori di modelli cloud con il valore seguente.

Servizio	Ruolo
Cloud AssemblyCloud Assembly	Utente di Cloud Assembly

- 7 Creare progetti in Cloud Assembly utilizzati per raggruppare risorse e utenti.

In questo caso d'uso, è possibile creare due progetti. Il primo progetto è PersonnelAppDev e il secondo è PayrollAppDev.

Per istruzioni, vedere il [Caso d'uso ruolo utente 2: configurazione dei ruoli utente di vRealize Automation per supportare team di sviluppo più grandi e il catalogo](#).

- 8 Creare e rilasciare i modelli cloud per ogni team di progetto.

Per istruzioni, vedere il [Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni](#).

- 9 Importare un modello cloud Cloud Assembly in Service Broker.

È necessario accedere come utente con il ruolo di amministratore di Service Broker.

- Accedere come utente con ruolo di amministratore di Service Broker.
- Nella console, fare clic su Service Broker.

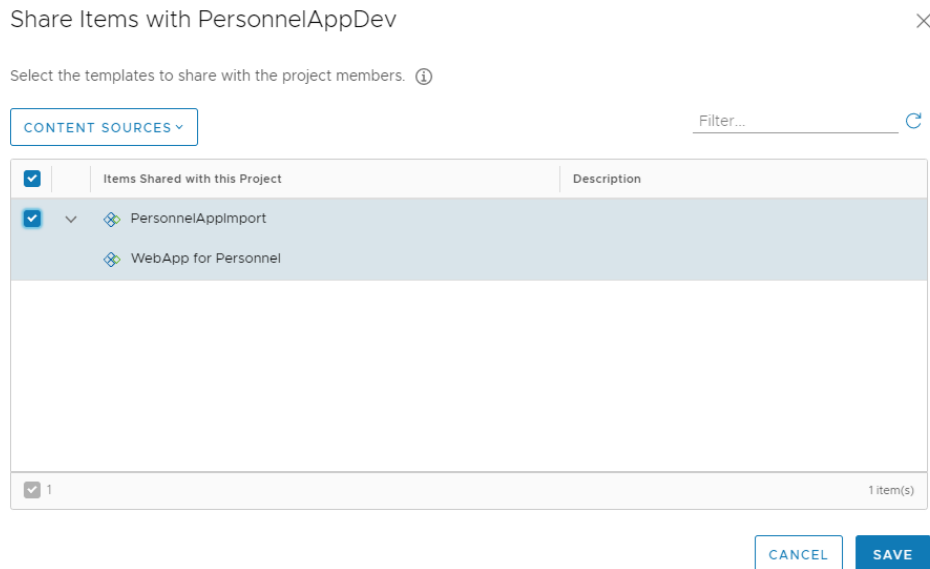
- c Selezionare **Contenuto e criteri > Origini contenuto**, quindi fare clic su **Nuovo**.

- d Selezionare **Modello cloud di Cloud Assembly**.
- e Immettere **PersonnelAppImport** come nome.
- f Nel menu a discesa **Progetto di origine**, selezionare PersonnelAppDev e fare clic su **Convalida**.
- g Quando l'origine viene convalidata, fare clic su **Crea e importa**.
- h Ripetere la procedura per PayrollAppDev utilizzando PayrollAppImport come nome dell'origine del contenuto.
- 10 Condividere un modello cloud importato con un progetto.

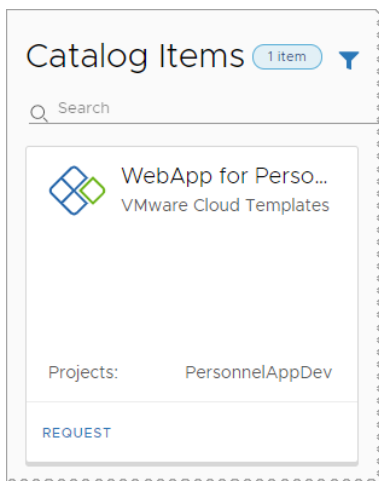
Anche se il modello cloud è già associato a un progetto, viene condiviso in Service Broker per renderlo disponibile nel catalogo.

- a Continuare come utente con il ruolo di amministratore di Service Broker.
- b In Service Broker, selezionare **Contenuto e criteri > Condivisione contenuto**.
- c Selezionare il progetto **PersonnelAppDev**, che include gli utenti che devono essere in grado di distribuire il modello cloud dal catalogo.

- d Fare clic su **Aggiungi elementi**, quindi selezionare il modello cloud PersonnelApp da condividere con i membri del progetto.



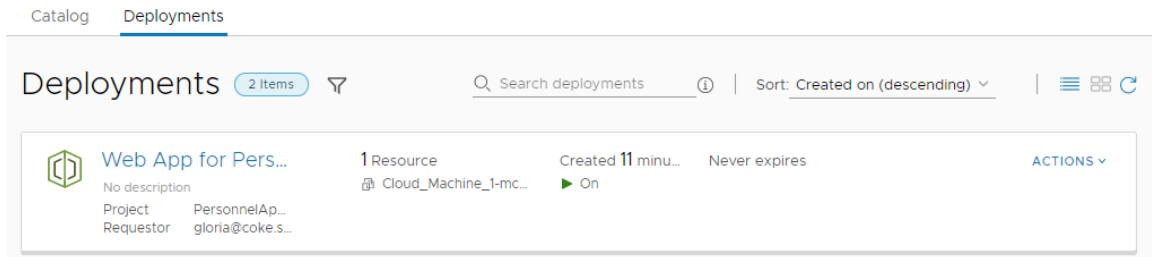
- e Fare clic su **Salva**.
- 11 Verificare che il modello cloud sia disponibile nel catalogo di Service Broker ai membri del progetto.
- a Richiedere che un membro del progetto abbia effettuato l'accesso e fare clic sulla scheda **Catalogo**.



- b Fare clic su Richiedi nella scheda del modello cloud PersonnelApp.
- c Compilare il modulo e fare clic su **Invia**.

12 Verificare che il membro del progetto possa monitorare il processo di distribuzione.

- a Richiedere al membro del progetto di selezionare **Risorse > Distribuzioni** e individuare la richiesta di provisioning.



- b Quando il modello cloud viene distribuito, verificare che l'utente richiedente possa accedere all'applicazione.

13 Ripetere il processo per i progetti aggiuntivi.

Risultati

In questo caso d'uso, riconoscendo che è necessario delegare lo sviluppo dei modelli cloud agli sviluppatori, è possibile aggiungere altri membri dell'organizzazione, per renderli utenti di Cloud Assembly e poi renderli membri dei progetti pertinenti affinché possano creare e distribuire i modelli cloud. Come membri del progetto, non possono visualizzare o alterare l'infrastruttura che si continua a gestire, ma sono state concesse loro autorizzazioni di visualizzatore del servizio complete affinché possano comprendere i vincoli dell'infrastruttura per cui stanno progettando.

In questo caso d'uso, si configurano gli utenti con diversi ruoli, tra cui l'amministratore e gli utenti di Service Broker. È quindi necessario fornire agli utenti non sviluppatori il catalogo di Service Broker.

Operazioni successive

Per informazioni su come definire e assegnare ruoli personalizzati all'utente, vedere [Caso d'uso ruolo utente 3: configurazione dei ruoli utente personalizzati di vRealize Automation per perfezionare i ruoli di sistema](#).

Caso d'uso ruolo utente 3: configurazione dei ruoli utente personalizzati di vRealize Automation per perfezionare i ruoli di sistema

Il proprietario dell'organizzazione o l'amministratore del servizio di vRealize Automation può gestire l'accesso degli utenti utilizzando i ruoli del sistema di organizzazione e servizio. Si desidera però creare anche ruoli personalizzati per gli utenti selezionati ed eseguire attività o visualizzare contenuti che non rientrano nei rispettivi ruoli di sistema.

In questo scenario, si presupponga di conoscere i ruoli di utente e visualizzatore del servizio e di membro e visualizzatore del progetto, definiti nel caso d'uso 2. Come si può notare, questi sono più restrittivi rispetto ai ruoli di amministratore del servizio e del progetto utilizzati nel caso d'uso 1. Sono quindi stati identificati alcuni casi d'uso locali per cui si desidera che alcuni utenti dispongano di autorizzazioni di gestione complete su alcune funzionalità e autorizzazioni di visualizzazione su altre, mentre al tempo stesso si desidera che non possano visualizzare un determinato altro set di funzionalità. Si utilizzano i ruoli personalizzati per definire tali autorizzazioni.

Questo caso d'uso si basa su tre possibili casi d'uso locali. Questa procedura illustra come creare le autorizzazioni per i seguenti ruoli personalizzati.

- **Amministratore dell'infrastruttura con limitazioni.** Si desidera che alcuni utenti del servizio, che non sono amministratori del servizio, dispongano di autorizzazioni per l'infrastruttura più ampie. In qualità di amministratore, si desidera che questi utenti possano offrire aiuto nella configurazione di zone cloud, immagini e caratteristiche. Si desidera inoltre che siano in grado di effettuare l'onboarding e gestire le risorse rilevate. Si noti che non possono aggiungere account cloud o integrazioni, ma possono solo definire l'infrastruttura per tali endpoint.
- **Sviluppatore di estendibilità.** Si desidera che alcuni utenti del servizio dispongano delle autorizzazioni complete per utilizzare le azioni e le sottoscrizioni di estendibilità come parte dello sviluppo del modello cloud per il proprio team di progetto e per altri progetti. Questi utenti svilupperanno anche tipi di risorse personalizzate e azioni personalizzate per più progetti.
- **Sviluppatore XaaS.** Si desidera che alcuni utenti del servizio dispongano delle autorizzazioni complete per sviluppare tipi di risorse personalizzate e azioni personalizzate per più progetti.
- **Risolutore problemi distribuzione.** Si desidera che gli amministratori del progetto dispongano delle autorizzazioni necessarie per risolvere i problemi ed eseguire l'analisi della causa radice nelle distribuzioni non riuscite. Agli utenti vengono assegnate autorizzazioni di gestione per le categorie non distruttive o meno costose, come le mappature di immagini e caratteristiche. Si desidera anche che gli amministratori del progetto dispongano dell'autorizzazione per impostare approvazioni e criteri del giorno 2 come parte del ruolo di risoluzione dei problemi delle distribuzioni non riuscite.

Prerequisiti

- Rivedere le tabelle di ruoli del progetto e ruoli di servizio di Cloud Assembly e Service Broker in [Che cosa sono i ruoli utente di vRealize Automation](#). È necessario conoscere ciò che ciascun ruolo utente del servizio può vedere e fare in tali servizi.
- Rivedere le descrizioni dei [Ruoli utente personalizzati in vRealize Automation](#) per individuare in che modo è possibile perfezionare le autorizzazioni per gli utenti.
- Rivedere il primo caso d'uso in modo da conoscere i ruoli dell'organizzazione e i ruoli di amministratore del servizio. Vedere [Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni](#).

- Rivedere il secondo caso d'uso in modo da comprendere i ruoli dell'utente del servizio e dei membri del progetto. Vedere [Caso d'uso ruolo utente 2: configurazione dei ruoli utente di vRealize Automation per supportare team di sviluppo più grandi e il catalogo](#).
- Acquisire familiarità con Service Broker. Vedere [Aggiunta di contenuti al catalogo](#).

Procedura

- 1 Assegnare i ruoli dei membri dell'organizzazione agli utenti sviluppatori di modelli cloud.

Per istruzioni, vedere il [Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni](#).

- 2 Assegnare i ruoli di servizio Cloud Assembly e Service Broker per gli sviluppatori di modelli cloud e i clienti del catalogo.

Per conoscere le istruzioni, vedere il [Caso d'uso ruolo utente 2: configurazione dei ruoli utente di vRealize Automation per supportare team di sviluppo più grandi e il catalogo](#).

- 3 Creare progetti in Cloud Assembly utilizzati per raggruppare risorse e utenti.

I passaggi seguenti per i ruoli personalizzati includono anche i ruoli del progetto.

Per conoscere le istruzioni per la creazione di progetti, vedere il [Caso d'uso ruolo utente 2: configurazione dei ruoli utente di vRealize Automation per supportare team di sviluppo più grandi e il catalogo](#).

- 4 Creare e rilasciare i modelli cloud per ogni team di progetto.

Per istruzioni, vedere il [Caso d'uso dei ruoli utente 1: configurazione dei ruoli utente di vRealize Automation per supportare un team di sviluppo di applicazioni di piccole dimensioni](#).

- 5 Accedere a Cloud Assembly come amministratore del servizio e selezionare **Infrastruttura > Amministrazione > Ruoli personalizzati**.

- 6 Creare un ruolo di amministratore dell'infrastruttura con limitazioni.

In questo esempio è presente l'utente Tony, esperto nella configurazione dell'infrastruttura per vari progetti, a cui non si desidera concedere le autorizzazioni di servizio complete. Tony tuttavia costruisce l'infrastruttura principale e supporta il lavoro di tutti i progetti. All'utente vengono concesse autorizzazioni di gestione dell'infrastruttura limitate. Tony, o un appaltatore esterno, potrebbe anche disporre di autorizzazioni simili per eseguire l'onboarding delle macchine rilevate e portarle nell'ambito della gestione di vRealize Automation.

- a Aggiungere Tony a Cloud Assembly come utente e visualizzatore del servizio.

Grazie alle autorizzazioni di visualizzatore può vedere gli account cloud e le integrazioni sottostanti se deve risolvere problemi relativi al proprio lavoro, ma non può apportare modifiche.

- b Creare un progetto e aggiungere Tony come membro del progetto.

- c Per creare il ruolo personalizzato, selezionare **Infrastruttura > Amministrazione > Ruoli personalizzati** e fare clic su **Nuovo ruolo personalizzato**.

- d Immettere il nome dell'**Amministratore infrastruttura con limitazioni** e selezionare le autorizzazioni seguenti.

Autorizzazione selezionabile	Operazioni che possono essere eseguite dall'utente
Infrastruttura > Gestisci zone cloud	Creare, aggiornare ed eliminare zone cloud.
Infrastruttura > Gestisci mappature delle caratteristiche	Creare, aggiornare ed eliminare le mappature di caratteristiche.
Infrastruttura > Gestisci mappature delle immagini	Creare, aggiornare ed eliminare mappature di immagini.

- e Fare clic su **Crea**.
- f Nella pagina Ruoli personalizzati, selezionare il ruolo Amministratore infrastruttura con limitazioni e fare clic su **Assegna**.
- g Immettere l'account email di Tony e fare clic su **Aggiungi**.
Immettere ad esempio Tony@yourcompany.com.
È inoltre possibile immettere tutti i gruppi di utenti di Active Directory definiti.
- h Fare in modo che Tony verifichi che, quando accede, possa aggiungere, modificare ed eliminare valori nelle aree definite dal ruolo personalizzato.

7 Creare un ruolo Sviluppatore di estendibilità.

In questo esempio, sono presenti gli sviluppatori di modelli cloud Sylvia e Igor, già formati su come utilizzare azioni e sottoscrizioni di estendibilità per gestire quotidianamente le attività di sviluppo. Essi inoltre sono competenti di vRealize Orchestrator, viene pertanto affidato loro il compito di fornire risorse personalizzate e azioni per vari progetti. Gli vengono concesse autorizzazioni aggiuntive per gestire l'estendibilità tramite la gestione di azioni e risorse personalizzate e la gestione di azioni e sottoscrizioni di estendibilità.

- a Aggiungere Sylvia e Igor come utenti di Cloud Assembly.
- b Aggiungerli come membri dei progetti a cui contribuiscono grazie alle loro capacità di estendibilità.
- c Creare un ruolo utente personalizzato denominato **Sviluppatore di estendibilità** e selezionare le autorizzazioni seguenti.

Autorizzazione selezionabile	Operazioni che possono essere eseguite dall'utente
XaaS > Gestisci Risorse personalizzate	Creare, aggiornare ed eliminare risorse personalizzate.
XaaS > Gestisci Azioni risorsa	Creare, aggiornare ed eliminare azioni personalizzate.
Estendibilità > Gestisci risorse di estendibilità	Creare, aggiornare ed eliminare le azioni e le sottoscrizioni di estendibilità. Disabilitare le sottoscrizioni. Annullare ed eliminare le esecuzioni delle azioni.

- d Fare clic su **Crea**.

- e Assegnare a Sylvia e Igor il ruolo di Sviluppatore di estendibilità.
- f Verificare che Sylvia e Igor possano gestire le risorse e le azioni personalizzate e che possano gestire le varie opzioni nella scheda Estendibilità.

8 Creare un ruolo Risolutore problemi distribuzione.

In questo esempio si assegnano ai propri amministratori di progetto più autorizzazioni di gestione in modo che possano rimediare a errori di distribuzione per i propri team.

- a Aggiungere i propri amministratori di progetto, Shauna, Pratap e Wei, come utenti del servizio di Cloud Assembly e Service Broker.
- b Aggiungerli nei loro progetti come amministratori di progetto.
- c Creare un ruolo utente personalizzato denominato **Risolutore problemi distribuzione** e selezionare le autorizzazioni seguenti.

Autorizzazione selezionabile	Operazioni che possono essere eseguite dall'utente
Infrastruttura > Gestisci mappature delle caratteristiche	Creare, aggiornare ed eliminare le mappature di caratteristiche.
Infrastruttura > Gestisci mappature delle immagini	Creare, aggiornare ed eliminare mappature di immagini.
Distribuzioni > Gestisci distribuzioni	Cisualizzare tutte le distribuzioni dei progetti ed eseguire tutte le azioni del giorno 2 su distribuzioni e componenti delle distribuzioni.
Criterio > Gestisci criteri	Creare, aggiornare ed eliminare le definizioni dei criteri.

- d Fare clic su **Crea**.
- e Assegnare Shauna, Pratap e Wei al ruolo Risolutore problemi distribuzione.
- f Verificare che possano gestire le mappature delle caratteristiche, le mappature delle immagini e i criteri in Service Broker.

Risultati

In questo caso d'uso vengono configurati svariati utenti con ruoli diversi, inclusi i ruoli personalizzati che ne estendono i ruoli di servizio e di progetto.

Operazioni successive

Creare ruoli personalizzati che consentono di affrontare le esigenze dei propri casi d'uso locali.

Modalità di assegnazione del ruolo integrato di Amministratore dell'infrastruttura Cloud Assembly a un utente

Il ruolo di Amministratore dell'infrastruttura è un ruolo integrato che è possibile assegnare agli utenti selezionati. Non è possibile assegnare il ruolo nell'interfaccia utente.

Quando è necessario assegnare questo ruolo utente

È possibile duplicare le autorizzazioni utilizzando le opzioni del ruolo utente personalizzato. Tuttavia, è possibile assegnare questo ruolo integrato agli utenti che sono amministratori limitati.

Autorizzazioni per il ruolo di Amministratore dell'infrastruttura

La seguente tabella include l'elenco delle autorizzazioni di gestione e delle altre autorizzazioni necessarie per gli amministratori dell'infrastruttura. Queste autorizzazioni non possono essere modificate. Se si desidera che un utente disponga di autorizzazioni più limitate, utilizzare i ruoli personalizzati per creare un ruolo utente che soddisfi le esigenze specifiche dell'utente.

Tabella 3-15. Autorizzazioni fornite per il ruolo integrato Amministratore dell'infrastruttura

Autorizzazione per creare, modificare, aggiornare o eliminare	Altre autorizzazioni
<ul style="list-style-type: none"> ■ Account cloud ■ Integrazioni ■ Zone cloud ■ Mappature caratteristiche ■ Mappature immagini ■ Profili di rete ■ Profili di storage ■ Tag ■ Onboarding 	<ul style="list-style-type: none"> ■ Visualizzazione e assegnazione di tag alle risorse rilevate ■ Visualizzazione delle risorse di elaborazione ■ Gestione degli indirizzi IP ■ Visualizzazione e assegnazione di tag ai bilanciamenti del carico ■ Visualizzazione dei di rete ■ Visualizzazione sicurezza ■ Visualizzare lo storage ■ Visualizzazione e rimozione delle richieste

Modalità di assegnazione del ruolo integrato di Amministratore dell'infrastruttura

Questo ruolo integrato viene assegnato utilizzando l'API RBAC. Si ottiene innanzitutto il ruolo e quindi si assegna il ruolo a un utente.

Prima di iniziare:

- Familiarizzare con l'API. Consultare la [Guida alla programmazione delle API di vRealize Automation](#).
 - Familiarizzare con l'API. Consultare la [Guida alla programmazione delle API di vRealize Automation 8.6](#).
 - Ottenere un token bearer dell'API. Consultare l'articolo Get Your Access Token nella [Guida alla programmazione delle API di vRealize Automation](#).
 - Ottenere un token bearer dell'API. Consultare l'articolo Get Your Access Token nella [Guida alla programmazione delle API di vRealize Automation 8.6](#)
- 1 Andare in `$vra/project/api/swagger/swagger-ui.html?urls.primaryName=rba` in cui `$vra` è l'URL di base per l'istanza.
 - 2 Nell'angolo superiore destro della pagina, nell'elenco a discesa **Seleziona una definizione**, selezionare **rbac: 2020-08-10**.

- 3 Per recuperare il ruolo utente, aprire la sezione **Ruolo**, eseguire `GET /rbac-service/api/roles`.

Il risultato deve essere simile all'esempio seguente.

```
"content": [
  {
    "description": "Infrastructure Administrator",
    "hidden": false,
    "id": "infrastructure_administrator",
    "name": "Infrastructure Administrator",
    "orgId": "string",
    "permissions": [
      "string"
    ],
    "projectScope": true
  }
]
```

- 4 Per aggiungere un utente al ruolo, aprire la sezione **Assegnazione ruolo**, aprire e modificare il comando `PUT /rbac-service/api/role-assignments` con il nome utente incluso.

Ad esempio,

```
{
  "orgId": "string",
  "principalId": "Username@domain",
  "principalType": "user",
  "projectId": "string",
  "rolesToAdd": [
    "infrastructure_administrator"
  ],
  "rolesToRemove": [
    "string"
  ]
}
```

- 5 Eseguire il comando `PUT` modificato.
- 6 Per verificare i risultati, chiedere all'utente assegnato di accedere e assicurarsi che disponga delle autorizzazioni definite in precedenza.

Aggiunta di account cloud a Cloud Assembly

Gli account cloud sono le autorizzazioni configurate che Cloud Assembly utilizza per raccogliere i dati dalle regioni o dai data center e per distribuire i modelli cloud in tali regioni.

I dati raccolti includono le regioni che successivamente vengono associate alle zone cloud.

Quando in un secondo momento si configurano le zone cloud, le mappature e i profili, è possibile selezionare l'account cloud a cui sono associati.

L'amministratore del cloud può creare account cloud per i progetti in cui operano i membri del team. Dagli account cloud vengono raccolti i dati delle informazioni sulle risorse, come la rete e la sicurezza, le risorse di elaborazione, lo storage e il contenuto dei tag.

Nota Se all'account cloud sono associate macchine che sono già state distribuite nella regione, è possibile fare in modo che tali macchine rientrino nella gestione di Cloud Assembly utilizzando un piano di onboarding. Vedere [Che cosa sono i piani di onboarding in Cloud Assembly](#).

Se si rimuove un account cloud utilizzato in una distribuzione, le risorse che fanno parte di tale distribuzione diventano non gestite.

Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation

Per configurare e utilizzare gli account cloud in vRealize Automation, verificare di disporre delle credenziali seguenti.

Credenziali account cloud richieste

Operazione da eseguire	Requisiti
Registrarsi e accedere a Cloud Assembly	Un ID VMware. ■ Configurare un account My VMware utilizzando il proprio indirizzo email aziendale.
Stabilire una connessione a vRealize Automation Services	Porta HTTPS 443 aperta per il traffico in uscita con accesso attraverso il firewall a: <ul style="list-style-type: none"> ■ *.vmwareidentity.com ■ gaz.csp-vidm-prod.com ■ *.vmware.com Per ulteriori informazioni sulle porte e sui protocolli, vedere VMware Ports and Protocols . Per ulteriori informazioni sulle porte e sui protocolli, vedere <i>Requisiti delle porte</i> nella guida Architettura di riferimento .

Operazione da eseguire	Requisiti
Aggiungere un account cloud di vCenter	<p data-bbox="432 258 1410 344">L'agente di vSphere deve disporre dei privilegi necessari per gestire l'istanza di vCenter Server. Fornire un account con i seguenti privilegi di lettura e scrittura:</p> <ul style="list-style-type: none"> <li data-bbox="432 357 863 382">■ Indirizzo IP o FQDN di vCenter <p data-bbox="432 394 1398 516">Sono elencate le autorizzazioni necessarie per gestire gli account cloud VMware Cloud on AWS e vCenter. Le autorizzazioni devono essere abilitate per tutti i cluster in vCenter Server, non solo per quelli che ospitano gli endpoint.</p> <p data-bbox="432 529 1382 680">Per tutti gli account cloud basati su vCenter Server, inclusi NSX-V, NSX-T, vCenter e VMware Cloud on AWS, l'amministratore deve disporre delle credenziali dell'endpoint vSphere o delle credenziali utilizzate per eseguire il servizio dell'agente in vCenter, che forniscono l'accesso amministrativo a vCenter Server host.</p> <p data-bbox="432 693 1340 749">Per ulteriori informazioni sui requisiti dell'agente vSphere, consultare la documentazione di prodotto di VMware vSphere.</p> <ul style="list-style-type: none"> <li data-bbox="432 762 596 787">■ Datastore <ul style="list-style-type: none"> <li data-bbox="472 800 676 825">■ Alloca spazio <li data-bbox="472 837 724 863">■ Sfoglia datastore <li data-bbox="472 875 916 900">■ Operazioni di livello base sui file <li data-bbox="432 913 724 938">■ Cluster archivio dati <ul style="list-style-type: none"> <li data-bbox="472 951 887 976">■ Configura cluster di datastore <li data-bbox="432 989 568 1014">■ Cartella <ul style="list-style-type: none"> <li data-bbox="472 1026 671 1052">■ Crea cartella <li data-bbox="472 1064 703 1089">■ Elimina cartella <li data-bbox="432 1102 568 1127">■ Globale <ul style="list-style-type: none"> <li data-bbox="472 1140 895 1165">■ Gestisci attributi personalizzati <li data-bbox="472 1178 919 1203">■ Imposta attributo personalizzato <li data-bbox="432 1215 533 1241">■ Rete <ul style="list-style-type: none"> <li data-bbox="472 1253 676 1278">■ Assegna rete <li data-bbox="432 1291 647 1316">■ Autorizzazioni <ul style="list-style-type: none"> <li data-bbox="472 1329 807 1354">■ Modifica autorizzazione <li data-bbox="432 1367 564 1392">■ Risorsa <ul style="list-style-type: none"> <li data-bbox="472 1404 879 1430">■ Assegna VM a pool di risorse <li data-bbox="472 1442 903 1467">■ Migra macchina virtuale spenta <li data-bbox="472 1480 903 1505">■ Migra macchina virtuale accesa <li data-bbox="432 1518 798 1543">■ Storage basato sul profilo <ul style="list-style-type: none"> <li data-bbox="472 1556 1102 1581">■ Visualizzazione dello storage basato sul profilo <p data-bbox="512 1593 1382 1715">Per restituire un elenco di criteri di storage che è possibile mappare a un profilo di storage, concedere il privilegio StorageProfile.View a tutti gli account che si connettono da vRealize Automation a vCenter Server.</p> <li data-bbox="432 1728 743 1753">■ Libreria dei contenuti

Operazione da eseguire	Requisiti
	<p>Per assegnare un privilegio per una libreria di contenuti, un amministratore deve concedere il privilegio all'utente come privilegio globale. Per informazioni correlate, vedere Ereditarietà gerarchica delle autorizzazioni per le librerie di contenuti in <i>Amministrazione delle macchine virtuali di vSphere</i> nella documentazione di VMware vSphere.</p> <ul style="list-style-type: none"> ■ Aggiungi elemento libreria ■ Crea libreria locale ■ Crea libreria con sottoscrizione ■ Elimina elemento libreria ■ Elimina libreria locale ■ Elimina libreria con sottoscrizione ■ Scarica file ■ Rimuovi elemento libreria ■ Sonda informazioni sottoscrizione ■ Leggi storage ■ Sincronizza elemento libreria ■ Sincronizza libreria con sottoscrizione ■ Rappresenta introspezione ■ Aggiorna impostazioni di configurazione ■ Aggiorna file ■ Aggiorna libreria ■ Aggiorna elemento libreria ■ Aggiorna libreria locale ■ Aggiorna libreria con sottoscrizione ■ Visualizza impostazioni di configurazione ■ Assegnazione di tag di vSphere <ul style="list-style-type: none"> ■ Assegna o annulla assegnazione del tag di vSphere ■ Assegna o annulla l'assegnazione del tag di vSphere sull'oggetto ■ Crea un tag di vSphere ■ Crea categoria di tag di vSphere ■ Elimina il tag di vSphere ■ Elimina la categoria di tag di vSphere ■ Modifica il tag di vSphere ■ Modifica la categoria di tag di vSphere ■ Modifica il campo o la categoria UsedBy ■ Modifica campo UsedBy per tag ■ vApp <ul style="list-style-type: none"> ■ Importazione ■ Configurazione dell'applicazione vApp <p>La configurazione dell'applicazione vApp.Import è necessaria per i modelli OVF e per eseguire il provisioning delle macchine virtuali dalla libreria dei contenuti.</p>

Operazione da eseguire	Requisiti
	<p>La configurazione dell'applicazione vApp.vApp è necessaria quando si utilizza cloud-init per lo scripting di configurazione del cloud. Questa impostazione consente di modificare la struttura interna di una vApp, ad esempio le informazioni e le proprietà del prodotto.</p> <ul style="list-style-type: none"> ■ Macchina virtuale - Inventario <ul style="list-style-type: none"> ■ Crea da esistente ■ Crea nuovo ■ Sposta ■ Rimuovi ■ Macchina virtuale - Interazione <ul style="list-style-type: none"> ■ Configura supporto CD ■ Interazione console ■ Connessione dispositivo ■ Spegni ■ Accendi ■ Reimposta ■ Sospendi ■ Installazione strumenti ■ Macchina virtuale - Configurazione <ul style="list-style-type: none"> ■ Aggiungi disco esistente ■ Aggiungi nuovo ■ Rimuovi disco ■ Avanzate ■ Cambia numero CPU ■ Cambia risorsa ■ Estendi disco virtuale ■ Traccia cambiamenti disco ■ Memoria ■ Modifica impostazioni dispositivo ■ Rinomina ■ Imposta annotazione ■ Impostazioni ■ Posizionamento file di swap ■ Macchina virtuale - Provisioning <ul style="list-style-type: none"> ■ Personalizza ■ Clona modello ■ Clona macchina virtuale ■ Distribuisci modello ■ Leggi specifiche di personalizzazione ■ Macchina virtuale - Stato <ul style="list-style-type: none"> ■ Crea snapshot ■ Rimuovi snapshot ■ Ripristina snapshot

Operazione da eseguire	Requisiti
Aggiungere un account cloud di Amazon Web Services (AWS)	<p>Fornire un account Power User con privilegi di lettura e scrittura. L'account utente deve essere un membro del criterio di accesso Power User (PowerUserAccess) nel sistema Identity and Access Management (IAM) di AWS.</p> <ul style="list-style-type: none"> ■ ID della chiave di accesso a 20 cifre e chiave di accesso segreta corrispondente <p>Se si utilizza un proxy Internet HTTP esterno, è necessario configurarlo per IPv4.</p> <p>L'estendibilità basata su azioni (ABX) di vRealize Automation e l'integrazione IPAM esterna potrebbero richiedere autorizzazioni aggiuntive.</p> <p>Per consentire le funzioni di ridimensionamento automatico sono consigliate le seguenti autorizzazioni di AWS:</p> <ul style="list-style-type: none"> ■ Azioni di ridimensionamento automatico: <ul style="list-style-type: none"> ■ autoscaling:DescribeAutoScalingInstances ■ autoscaling:AttachInstances ■ autoscaling>DeleteLaunchConfiguration ■ autoscaling:DescribeAutoScalingGroups ■ autoscaling>CreateAutoScalingGroup ■ autoscaling:UpdateAutoScalingGroup ■ autoscaling>DeleteAutoScalingGroup ■ autoscaling:DescribeLoadBalancers ■ Risorse di ridimensionamento automatico: <ul style="list-style-type: none"> ■ * <p>Fornire tutte le autorizzazioni delle risorse di ridimensionamento automatico.</p> <p>Sono necessarie le seguenti autorizzazioni per consentire alle funzioni di AWS Security Token Service (AWS STS) di supportare le credenziali temporanee e con privilegi limitati per l'identità e l'accesso di AWS:</p> ■ Risorse AWS STS: <ul style="list-style-type: none"> ■ * <p>Fornire tutte le autorizzazioni delle risorse di STS.</p> <p>Per consentire le funzioni EC2, sono necessarie le seguenti autorizzazioni di AWS:</p> ■ Azioni EC2: <ul style="list-style-type: none"> ■ ec2:AttachVolume ■ ec2:AuthorizeSecurityGroupIngress ■ ec2>DeleteSubnet ■ ec2>DeleteSnapshot ■ ec2:DescribeInstances ■ ec2>DeleteTags ■ ec2:DescribeRegions ■ ec2:DescribeVolumesModifications ■ ec2>CreateVpc ■ ec2:DescribeSnapshots ■ ec2:DescribeInternetGateways

Operazione da eseguire	Requisiti
	<ul style="list-style-type: none"> ■ ec2:DeleteVolume ■ ec2:DescribeNetworkInterfaces ■ ec2:StartInstances ■ ec2:DescribeAvailabilityZones ■ ec2:CreateInternetGateway ■ ec2:CreateSecurityGroup ■ ec2:DescribeVolumes ■ ec2:CreateSnapshot ■ ec2:ModifyInstanceAttribute ■ ec2:DescribeRouteTables ■ ec2:DescribeInstanceTypes ■ ec2:DescribeInstanceTypeOfferings ■ ec2:DescribeInstanceStatus ■ ec2:DetachVolume ■ ec2:RebootInstances ■ ec2:AuthorizeSecurityGroupEgress ■ ec2:ModifyVolume ■ ec2:TerminateInstances ■ ec2:DescribeSpotFleetRequestHistory ■ ec2:DescribeTags ■ ec2:CreateTags ■ ec2:RunInstances ■ ec2:DescribeNatGateways ■ ec2:StopInstances ■ ec2:DescribeSecurityGroups ■ ec2:CreateVolume ■ ec2:DescribeSpotFleetRequests ■ ec2:DescribeImages ■ ec2:DescribeVpcs ■ ec2>DeleteSecurityGroup ■ ec2>DeleteVpc ■ ec2:CreateSubnet ■ ec2:DescribeSubnets ■ ec2:RequestSpotFleet
	<p>Nota L'autorizzazione di richiesta di SpotFleet non è necessaria per l'estendibilità basata su azioni (ABX) di vRealize Automation e le integrazioni IPAM esterne.</p>
	<ul style="list-style-type: none"> ■ Risorse EC2: <ul style="list-style-type: none"> ■ * <p>Fornire tutte le autorizzazioni delle risorse di EC2.</p> <p>Per consentire le funzioni di bilanciamento del carico elastico, sono necessarie le seguenti autorizzazioni di AWS:</p> <ul style="list-style-type: none"> ■ Azioni di bilanciamento del carico: <ul style="list-style-type: none"> ■ elasticloadbalancing>DeleteLoadBalancer

Operazione da eseguire	Requisiti
	<ul style="list-style-type: none"> ■ elasticloadbalancing:DescribeLoadBalancers ■ elasticloadbalancing:RemoveTags ■ elasticloadbalancing:CreateLoadBalancer ■ elasticloadbalancing:DescribeTags ■ elasticloadbalancing:ConfigureHealthCheck ■ elasticloadbalancing:AddTags ■ elasticloadbalancing:CreateTargetGroup ■ elasticloadbalancing>DeleteLoadBalancerListeners ■ elasticloadbalancing:DeregisterInstancesFromLoadBalancer ■ elasticloadbalancing:RegisterInstancesWithLoadBalancer ■ elasticloadbalancing:CreateLoadBalancerListeners ■ Risorse di bilanciamento del carico: <ul style="list-style-type: none"> ■ * <p>Fornire tutte le autorizzazioni delle risorse di bilanciamento del carico. Le seguenti autorizzazioni di AWS Identity and Access Management (IAM) possono essere abilitate, tuttavia non sono obbligatorie:</p> <ul style="list-style-type: none"> ■ iam:SimulateCustomPolicy ■ iam:GetUser ■ iam:ListUserPolicies ■ iam:GetUserPolicy ■ iam:ListAttachedUserPolicies ■ iam:GetPolicyVersion ■ iam:ListGroupsForUser ■ iam:ListGroupPolicies ■ iam:GetGroupPolicy ■ iam:ListAttachedGroupPolicies ■ iam:ListPolicyVersions

Operazione da eseguire	Requisiti
Aggiungere un account cloud di Microsoft Azure	<p>Configurare un'istanza di Microsoft Azure e ottenere una sottoscrizione valida per Microsoft Azure dalla quale sia possibile utilizzare l'ID sottoscrizione.</p> <p>Creare un'applicazione di Active Directory come descritto in Procedura: Usare il portale per creare un'applicazione Azure Active Directory (Azure AD) e un'entità servizio che possano accedere alle risorse nella documentazione del prodotto Microsoft Azure.</p> <p>Se si utilizza un proxy Internet HTTP esterno, è necessario configurarlo per IPv4.</p> <p>Prendere nota delle seguenti informazioni:</p> <ul style="list-style-type: none"> ■ ID sottoscrizione <p>Consente di accedere alle proprie sottoscrizioni di Microsoft Azure.</p> ■ ID tenant <p>Endpoint di autorizzazione per le applicazioni di Active Directory create nell'account Microsoft Azure.</p> ■ ID applicazione client <p>Consente di accedere a Microsoft Active Directory nell'account individuale di Microsoft Azure.</p> ■ Chiave privata applicazione client <p>Chiave privata univoca generata per eseguire l'associazione con il proprio ID applicazione client.</p> <p>La creazione e la convalida degli account cloud di Microsoft Azure richiedono le autorizzazioni seguenti:</p> <ul style="list-style-type: none"> ■ Microsoft Compute <ul style="list-style-type: none"> ■ Microsoft.Compute/virtualMachines/extensions/write ■ Microsoft.Compute/virtualMachines/extensions/read ■ Microsoft.Compute/virtualMachines/extensions/delete ■ Microsoft.Compute/virtualMachines/deallocate/action ■ Microsoft.Compute/virtualMachines/delete ■ Microsoft.Compute/virtualMachines/powerOff/action ■ Microsoft.Compute/virtualMachines/read ■ Microsoft.Compute/virtualMachines/restart/action ■ Microsoft.Compute/virtualMachines/start/action ■ Microsoft.Compute/virtualMachines/write ■ Microsoft.Compute/availabilitySets/write ■ Microsoft.Compute/availabilitySets/read ■ Microsoft.Compute/availabilitySets/delete ■ Microsoft.Compute/disks/delete ■ Microsoft.Compute/disks/read ■ Microsoft.Compute/disks/write ■ Microsoft Network <ul style="list-style-type: none"> ■ Microsoft.Network/loadBalancers/backendAddressPools/join/action ■ Microsoft.Network/loadBalancers/delete ■ Microsoft.Network/loadBalancers/read

Operazione da eseguire	Requisiti
	<ul style="list-style-type: none"> ■ Microsoft.Network/loadBalancers/write ■ Microsoft.Network/networkInterfaces/join/action ■ Microsoft.Network/networkInterfaces/read ■ Microsoft.Network/networkInterfaces/write ■ Microsoft.Network/networkInterfaces/delete ■ Microsoft.Network/networkSecurityGroups/join/action ■ Microsoft.Network/networkSecurityGroups/read ■ Microsoft.Network/networkSecurityGroups/write ■ Microsoft.Network/networkSecurityGroups/delete ■ Microsoft.Network/publicIPAddresses/delete ■ Microsoft.Network/publicIPAddresses/join/action ■ Microsoft.Network/publicIPAddresses/read ■ Microsoft.Network/publicIPAddresses/write ■ Microsoft.Network/virtualNetworks/read ■ Microsoft.Network/virtualNetworks/subnets/delete ■ Microsoft.Network/virtualNetworks/subnets/join/action ■ Microsoft.Network/virtualNetworks/subnets/read ■ Microsoft.Network/virtualNetworks/subnets/write ■ Microsoft.Network/virtualNetworks/write ■ Microsoft Resources <ul style="list-style-type: none"> ■ Microsoft.Resources/subscriptions/resourcegroups/delete ■ Microsoft.Resources/subscriptions/resourcegroups/read ■ Microsoft.Resources/subscriptions/resourcegroups/write ■ Microsoft Storage <ul style="list-style-type: none"> ■ Microsoft.Storage/storageAccounts/delete ■ Microsoft.Storage/storageAccounts/listKeys/action ■ Microsoft.Storage/storageAccounts/read ■ Microsoft.Storage/storageAccounts/write ■ Microsoft Web <ul style="list-style-type: none"> ■ Microsoft.Web/sites/read ■ Microsoft.Web/sites/write ■ Microsoft.Web/sites/delete ■ Microsoft.Web/sites/config/read ■ Microsoft.Web/sites/config/write ■ Microsoft.Web/sites/config/list/action ■ Microsoft.Web/sites/publishxml/action ■ Microsoft.Web/serverfarms/write ■ Microsoft.Web/serverfarms/delete ■ Microsoft.Web/sites/hostruntime/functions/keys/read ■ Microsoft.Web/sites/hostruntime/host/read ■ Microsoft.web/sites/functions/masterkey/read <p>Se si utilizza Microsoft Azure con l'estendibilità basata sulle azioni, oltre alle autorizzazioni minime sono necessarie anche le autorizzazioni seguenti:</p> <ul style="list-style-type: none"> ■ Microsoft.Web/sites/read

Operazione da eseguire	Requisiti
	<ul style="list-style-type: none"> ■ Microsoft.Web/sites/write ■ Microsoft.Web/sites/delete ■ Microsoft.Web/sites/*/action ■ Microsoft.Web/sites/config/read ■ Microsoft.Web/sites/config/write ■ Microsoft.Web/sites/config/list/action ■ Microsoft.Web/sites/publishxml/action ■ Microsoft.Web/serverfarms/write ■ Microsoft.Web/serverfarms/delete ■ Microsoft.Web/sites/hostruntime/functions/keys/read ■ Microsoft.Web/sites/hostruntime/host/read ■ Microsoft.Web/sites/functions/masterkey/read ■ Microsoft.Web/apimanagementaccounts/apis/read ■ Microsoft.Authorization/roleAssignments/read ■ Microsoft.Authorization/roleAssignments/write ■ Microsoft.Authorization/roleAssignments/delete ■ Microsoft.Insights/Components/Read ■ Microsoft.Insights/Components/Write ■ Microsoft.Insights/Components/Query/Read <p>Se si utilizza Microsoft Azure con l'estendibilità basata sulle azioni con estensioni, sono necessarie anche le autorizzazioni seguenti:</p> <ul style="list-style-type: none"> ■ Microsoft.Compute/virtualMachines/extensions/write ■ Microsoft.Compute/virtualMachines/extensions/read ■ Microsoft.Compute/virtualMachines/extensions/delete <p>Per informazioni correlate alla creazione di un account cloud Microsoft Azure, vedere Configurazione di Microsoft Azure.</p>

Operazione da eseguire	Requisiti
Aggiunta di un account cloud Google Cloud Platform (GCP)	<p>L'account cloud di Google Cloud Platform interagisce con il motore di elaborazione di Google Cloud Platform.</p> <p>Le credenziali di amministratore e proprietario del progetto sono necessarie per la creazione e la convalida degli account cloud di Google Cloud Platform.</p> <p>Se si utilizza un proxy Internet HTTP esterno, è necessario configurarlo per IPv4.</p> <p>Il servizio del motore di elaborazione deve essere abilitato. Quando si crea l'account cloud in vRealize Automation, utilizzare l'account del servizio che è stato creato quando il motore di elaborazione è stato inizializzato.</p> <p>Sono necessarie anche le autorizzazioni del motore di elaborazione seguenti, in base alle azioni che l'utente può eseguire:</p> <ul style="list-style-type: none"> ■ <code>roles/compute.admin</code> <p>Offre il controllo completo di tutte le risorse del motore di elaborazione.</p> ■ <code>roles/iam.serviceAccountUser</code> <p>Fornisce l'accesso agli utenti che gestiscono le istanze di macchine virtuali configurate per essere eseguite come account di servizio. Concedere l'accesso alle seguenti risorse e servizi:</p> <ul style="list-style-type: none"> ■ <code>compute.*</code> ■ <code>resourcemanager.projects.get</code> ■ <code>resourcemanager.projects.list</code> ■ <code>serviceusage.quotas.get</code> ■ <code>serviceusage.services.get</code> ■ <code>serviceusage.services.list</code> ■ <code>roles/compute.imageUser</code> <p>Fornisce l'autorizzazione a elencare e leggere le immagini senza dover disporre di altre autorizzazioni per l'immagine. La concessione del ruolo <code>compute.imageUser</code> a livello di progetto offre agli utenti la possibilità di elencare tutte le immagini nel progetto. Consente inoltre agli utenti di creare risorse, ad esempio istanze e dischi persistenti, in base alle immagini nel progetto.</p> <ul style="list-style-type: none"> ■ <code>compute.images.get</code> ■ <code>compute.images.getFromFamily</code> ■ <code>compute.images.list</code> ■ <code>compute.images.useReadOnly</code> ■ <code>resourcemanager.projects.get</code> ■ <code>resourcemanager.projects.list</code> ■ <code>serviceusage.quotas.get</code> ■ <code>serviceusage.services.get</code> ■ <code>serviceusage.services.list</code> ■ <code>roles/compute.instanceAdmin</code> <p>Fornisce le autorizzazioni per creare, modificare ed eliminare istanze di macchine virtuali. Sono incluse le autorizzazioni per creare, modificare ed eliminare i dischi, nonché per configurare le impostazioni VMBETA schermate.</p>

Operazione da eseguire	Requisiti
	<p>Per gli utenti che gestiscono istanze di macchine virtuali (ma non le impostazioni di rete o di sicurezza o le istanze eseguite come account di servizio), concedere questo ruolo all'organizzazione, alla cartella o al progetto che contiene le istanze o alle singole istanze.</p> <p>Gli utenti che gestiscono le istanze di macchine virtuali configurate per l'uso come account di servizio richiedono anche il ruolo roles/iam.serviceAccountUser.</p> <ul style="list-style-type: none"> ■ compute.acceleratorTypes ■ compute.addresses.get ■ compute.addresses.list ■ compute.addresses.use ■ compute.autoscalers ■ compute.diskTypes ■ compute.disks.create ■ compute.disks.createSnapshot ■ compute.disks.delete ■ compute.disks.get ■ compute.disks.list ■ compute.disks.resize ■ compute.disks.setLabels ■ compute.disks.update ■ compute.disks.use ■ compute.disks.useReadOnly ■ compute.globalAddresses.get ■ compute.globalAddresses.list ■ compute.globalAddresses.use ■ compute.globalOperations.get ■ compute.globalOperations.list ■ compute.images.get ■ compute.images.getFromFamily ■ compute.images.list ■ compute.images.useReadOnly ■ compute.instanceGroupManagers ■ compute.instanceGroups ■ compute.instanceTemplates ■ compute.instances ■ compute.licenses.get ■ compute.licenses.list ■ compute.machineTypes ■ compute.networkEndpointGroups ■ compute.networks.get ■ compute.networks.list ■ compute.networks.use ■ compute.networks.useExternalIp

Operazione da eseguire	Requisiti
	<ul style="list-style-type: none"> ■ compute.projects.get ■ compute.regionOperations.get ■ compute.regionOperations.list ■ compute.regions ■ compute.reservations.get ■ compute.reservations.list ■ compute.subnetworks.get ■ compute.subnetworks.list ■ compute.subnetworks.use ■ compute.subnetworks.useExternalIp ■ compute.targetPools.get ■ compute.targetPools.list ■ compute.zoneOperations.get ■ compute.zoneOperations.list ■ compute.zones ■ resourceManager.projects.get ■ resourceManager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list ■ roles/compute.instanceAdmin.v1 <p>Offre il controllo completo delle istanze del motore di elaborazione, dei gruppi di istanze, dei dischi, degli snapshot e delle immagini. Fornisce inoltre l'accesso in lettura a tutte le risorse di rete del motore di elaborazione.</p> <hr/> <p>Nota Se si concede a un utente questo ruolo a livello di istanza, tale utente non può creare nuove istanze.</p> <hr/> <ul style="list-style-type: none"> ■ compute.acceleratorTypes ■ compute.addresses.get ■ compute.addresses.list ■ compute.addresses.use ■ compute.autoscalers ■ compute.backendBuckets.get ■ compute.backendBuckets.list ■ compute.backendServices.get ■ compute.backendServices.list ■ compute.diskTypes ■ compute.disks ■ compute.firewalls.get ■ compute.firewalls.list ■ compute.forwardingRules.get ■ compute.forwardingRules.list ■ compute.globalAddresses.get ■ compute.globalAddresses.list

Operazione da eseguire	Requisiti
	<ul style="list-style-type: none"> ■ compute.globalAddresses.use ■ compute.globalForwardingRules.get ■ compute.globalForwardingRules.list ■ compute.globalOperations.get ■ compute.globalOperations.list ■ compute.healthChecks.get ■ compute.healthChecks.list ■ compute.httpHealthChecks.get ■ compute.httpHealthChecks.list ■ compute.httpsHealthChecks.get ■ compute.httpsHealthChecks.list ■ compute.images ■ compute.instanceGroupManagers ■ compute.instanceGroups ■ compute.instanceTemplates ■ compute.instances ■ compute.interconnectAttachments.get ■ compute.interconnectAttachments.list ■ compute.interconnectLocations ■ compute.interconnects.get ■ compute.interconnects.list ■ compute.licenseCodes ■ compute.licenses ■ compute.machineTypes ■ compute.networkEndpointGroups ■ compute.networks.get ■ compute.networks.list ■ compute.networks.use ■ compute.networks.useExternalIp ■ compute.projects.get ■ compute.projects.setCommonInstanceMetadata ■ compute.regionBackendServices.get ■ compute.regionBackendServices.list ■ compute.regionOperations.get ■ compute.regionOperations.list ■ compute.regions ■ compute.reservations.get ■ compute.reservations.list ■ compute.resourcePolicies ■ compute.routers.get ■ compute.routers.list ■ compute.routes.get ■ compute.routes.list ■ compute.snapshots

Operazione da eseguire	Requisiti
	<ul style="list-style-type: none"> ■ compute.sslCertificates.get ■ compute.sslCertificates.list ■ compute.sslPolicies.get ■ compute.sslPolicies.list ■ compute.sslPolicies.listAvailableFeatures ■ compute.subnetworks.get ■ compute.subnetworks.list ■ compute.subnetworks.use ■ compute.subnetworks.useExternalIp ■ compute.targetHttpProxies.get ■ compute.targetHttpProxies.list ■ compute.targetHttpsProxies.get ■ compute.targetHttpsProxies.list ■ compute.targetInstances.get ■ compute.targetInstances.list ■ compute.targetPools.get ■ compute.targetPools.list ■ compute.targetSslProxies.get ■ compute.targetSslProxies.list ■ compute.targetTcpProxies.get ■ compute.targetTcpProxies.list ■ compute.targetVpnGateways.get ■ compute.targetVpnGateways.list ■ compute.urlMaps.get ■ compute.urlMaps.list ■ compute.vpnTunnels.get ■ compute.vpnTunnels.list ■ compute.zoneOperations.get ■ compute.zoneOperations.list ■ compute.zones ■ resourcemanager.projects.get ■ resourcemanager.projects.list ■ serviceusage.quotas.get ■ serviceusage.services.get ■ serviceusage.services.list
Aggiungere un account cloud di NSX-T	<p data-bbox="432 1570 1230 1598">Fornire un account con i seguenti privilegi di lettura e scrittura:</p> <ul style="list-style-type: none"> ■ Indirizzo IP o FQDN di NSX-T ■ NSX-T Data Center - Ruolo e credenziali di accesso di amministratore aziendale <p data-bbox="432 1713 1362 1803">Gli amministratori richiedono l'accesso a <i>anche</i> a vCenter Server come descritto nella sezione <i>Aggiungere un account cloud di vCenter</i> di questa tabella.</p>

Operazione da eseguire	Requisiti
Aggiungere un account cloud di NSX-V	<p>Fornire un account con i seguenti privilegi di lettura e scrittura:</p> <ul style="list-style-type: none"> ■ Ruolo di amministratore di NSX-V Enterprise e credenziali di accesso ■ Indirizzo IP o FQDN di NSX-V <p>Gli amministratori richiedono l'accesso a <i>anche</i> a vCenter Server come descritto nella sezione <i>Aggiungere un account cloud di vCenter</i> di questa tabella.</p>
Aggiunta di un account cloud VMware Cloud on AWS (VMC)	<p>Fornire un account con i seguenti privilegi di lettura e scrittura:</p> <ul style="list-style-type: none"> ■ Account cloudadmin@vmc.local o qualsiasi altro account utente nel gruppo CloudAdmin ■ Ruolo di amministratore di NSX Enterprise e credenziali di accesso ■ Accesso da amministratore di NSX Cloud all'ambiente SDDC di VMware Cloud on AWS dell'organizzazione ■ Accesso da amministratore all'ambiente SDDC di VMware Cloud on AWS dell'organizzazione ■ Token API di VMware Cloud on AWS per l'ambiente VMware Cloud on AWS nel servizio VMware Cloud on AWS dell'organizzazione ■ Indirizzo IP o FQDN di vCenter <p>Gli amministratori richiedono l'accesso a <i>anche</i> a vCenter Server come descritto nella sezione <i>Aggiungere un account cloud di vCenter</i> di questa tabella.</p> <p>Per ulteriori informazioni sulle autorizzazioni necessarie per creare e utilizzare account cloud di VMware Cloud on AWS, vedere <i>Gestione del data center di VMware Cloud on AWS</i> nella documentazione di prodotto di VMware Cloud on AWS.</p>
Integrazione con vRealize Operations Manager	<p>Fornire un account di accesso locale o non locale a vRealize Operations Manager con i privilegi di lettura seguenti.</p> <ul style="list-style-type: none"> ■ Istanza adattatore vCenter Adattatore > Adattatore istanza VC per <i>vCenter-FQDN</i> <p>Potrebbe essere necessario importare prima un account non locale, prima di poterne assegnare il ruolo di sola lettura.</p>

Configurazione di Microsoft Azure per l'utilizzo con Cloud Assembly

Per creare un account cloud di Microsoft Azure in Cloud Assembly, è necessario raccogliere alcune informazioni ed eseguire alcune configurazioni.

Procedura

- 1 Individuare e registrare la sottoscrizione a Microsoft Azure e gli ID dei tenant.
 - ID sottoscrizione: fare clic sull'icona Sottoscrizioni sulla barra degli strumenti a sinistra nel portale di Azure per visualizzare l'ID della sottoscrizione.
 - ID tenant: fare clic sull'icona ? e selezionare Visualizza diagnostica nel portale di Azure. Cercare il tenant e registrare l'ID una volta individuato.

- 2 È possibile creare un nuovo account di storage e un gruppo di risorse per iniziare. In alternativa, è possibile crearli nei blueprint in un secondo momento.
 - Account di storage: per configurare un account, utilizzare la procedura seguente.
 - 1 Nel portale di Azure, individuare l'icona Account di archiviazione nella barra laterale. Assicurarsi che sia selezionata la sottoscrizione corretta e fare clic su **Aggiungi**. È inoltre possibile cercare l'account di storage nel campo di ricerca di Azure.
 - 2 Immettere le informazioni richieste per l'account di storage. Sarà necessario l'ID della sottoscrizione.
 - 3 Scegliere se utilizzare un gruppo di risorse esistente o crearne uno nuovo. Prendere nota del nome del gruppo di risorse, poiché sarà necessario in un secondo momento.

Nota Salvare la posizione dell'account di storage perché sarà necessaria in un secondo momento.

- 3 Creare una rete virtuale. In alternativa, se si dispone di una rete esistente idonea, è possibile selezionarla.

Se si sta creando una rete, è necessario selezionare Usa un gruppo di risorse esistente e specificare il gruppo creato nel passaggio precedente. Selezionare inoltre la stessa posizione specificata in precedenza. Microsoft Azure non distribuirà macchine virtuali o altri oggetti se la posizione non coincide in tutti i componenti applicabili che l'oggetto utilizzerà.

 - a Individuare l'icona Rete virtuale nel pannello sinistro e fare clic su tale icona oppure cercare una rete virtuale. Assicurarsi di selezionare la sottoscrizione corretta e fare clic su **Aggiungi**.
 - b Immettere un nome univoco per la nuova rete virtuale e registrarlo per farvi riferimento in seguito.
 - c Immettere l'indirizzo IP appropriato per la rete virtuale nel campo **Spazio indirizzi**.
 - d Assicurarsi che sia selezionata la sottoscrizione corretta e fare clic su **Aggiungi**.
 - e Immettere le informazioni di configurazione di base rimanenti.
 - f È possibile modificare le altre opzioni in base alle necessità, ma per la maggior parte delle configurazioni è consigliabile lasciare le impostazioni predefinite.
 - g Fare clic su **Crea**.
- 4 Configurare un'applicazione Azure Active Directory in modo che vRA possa eseguire l'autenticazione.
 - a Individuare l'icona di Active Directory nel menu a sinistra di Azure e fare clic su tale icona.
 - b Fare clic su **Registrazioni app** e selezionare **Aggiungi**.
 - c Digitare un nome per l'applicazione conforme alla convalida dei nomi di Azure.
 - d Lasciare App Web/API come tipo di applicazione.

- e L'URL di accesso può essere qualsiasi URL appropriato per l'utilizzo.
 - f Fare clic su **Crea**.
- 5** Creare una chiave segreta per eseguire l'autenticazione dell'applicazione in Cloud Assembly.
- a Fare clic sul nome dell'applicazione in Azure.
Prendere nota dell'ID dell'applicazione per poterlo utilizzare in seguito.
 - b Fare clic su **Tutte le impostazioni** nel riquadro successivo e selezionare Chiavi nell'elenco delle impostazioni.
 - c Immettere una descrizione per la nuova chiave e scegliere una durata.
 - d Fare clic su **Salva** e assicurarsi di copiare il valore della chiave in una posizione sicura, poiché non sarà possibile recuperarlo in un secondo momento.
 - e Nel menu a sinistra, selezionare **Autorizzazioni API** per l'applicazione e fare clic su **Aggiungi un'autorizzazione** per creare una nuova autorizzazione.
 - f Selezionare Gestione servizio Azure nella pagina Selezionare un'API.
 - g Fare clic su **Autorizzazioni delegate**.
 - h In Seleziona autorizzazioni, selezionare user_impersonation, quindi fare clic su **Aggiungi autorizzazioni**.
- 6** Autorizzare l'applicazione Active Directory a connettersi alla sottoscrizione di Azure in modo da poter distribuire e gestire le macchine virtuali.
- a Nel menu a sinistra, fare clic sull'icona Sottoscrizioni e selezionare la nuova sottoscrizione.
Potrebbe essere necessario fare clic sul testo del nome per far scorrere il pannello.
 - b Selezionare l'opzione Controllo di accesso (IAM) per visualizzare le autorizzazioni per la sottoscrizione.
 - c Fare clic su **Aggiungi** sotto l'intestazione Aggiungi assegnazione ruolo.
 - d Scegliere Collaboratore dal menu a discesa Ruolo.
 - e Lasciare la selezione predefinita nel menu a discesa Assegna accesso a.
 - f Digitare il nome dell'applicazione nella casella Seleziona.
 - g Fare clic su **Salva**.
 - h Aggiungere ulteriori ruoli in modo che la nuova applicazione disponga dei ruoli Proprietario, Collaboratore e Lettore.
 - i Fare clic su **Salva**.

Operazioni successive

È necessario installare gli strumenti dell'interfaccia della riga di comando di Microsoft Azure. Questi strumenti sono disponibili gratuitamente per i sistemi operativi Windows e Mac. Per ulteriori informazioni sul download e l'installazione di questi strumenti, vedere la documentazione di Microsoft.

Una volta installata l'interfaccia della riga di comando, è necessario eseguire l'autenticazione nella nuova sottoscrizione.

- 1 Aprire una finestra del terminale e digitare le credenziali di accesso di Microsoft Azure. Si riceveranno un URL e un codice breve che consentiranno di eseguire l'autenticazione.

- 2 In un browser, immettere il codice ricevuto dall'applicazione sul dispositivo.

- 3 Immettere il codice di autenticazione e fare clic su **Continua**.

- 4 Selezionare l'account e le credenziali di accesso di Azure.

Se si dispone di più sottoscrizioni, assicurarsi che sia selezionata quella corretta utilizzando il comando `azure account set <subscription-name>`.

- 5 Prima di procedere, è necessario registrare il provider Microsoft.Compute nella nuova sottoscrizione di Azure utilizzando il comando `azure provider register microsoft.compute`.

Se si verifica il timeout del comando e viene generato un errore la prima volta che il comando viene eseguito, eseguirlo di nuovo.

Una volta completata la configurazione, è possibile utilizzare il comando `azure vm image list` per recuperare i nomi delle immagini delle macchine virtuali disponibili. È possibile scegliere l'immagine desiderata e registrare l'URN fornito per utilizzarlo successivamente nei blueprint.

Creazione di un account cloud di Microsoft Azure in vRealize Automation

L'amministratore del cloud può creare un account cloud di Microsoft Azure per le regioni dell'account in cui il suo team distribuirà i modelli cloud di vRealize Automation.

Per visualizzare un caso d'uso di esempio sul funzionamento di un account cloud di Microsoft Azure in vRealize Automation, vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).

Prerequisiti

- Verificare di disporre delle credenziali di amministratore necessarie e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente necessario. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Configurare un account Microsoft Azure per l'uso con vRealize Automation. Vedere [Configurazione di Microsoft Azure per l'utilizzo con Cloud Assembly](#).

- Se non si dispone di accesso a Internet esterno, configurare un server proxy Internet. Vedere [Come configurare un server proxy Internet per vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account Microsoft Azure e immettere le credenziali e gli altri valori.
- 3 Fare clic su **Convalida**.
Vengono raccolte le regioni dell'account associate all'account.
- 4 Selezionare le regioni in cui si desidera eseguire il provisioning della risorsa.
- 5 Per migliorare l'efficienza, fare clic su **Creare una zona cloud per le regioni selezionate**.
- 6 Se è necessario aggiungere tag per supportare una strategia di assegnazione dei tag, immettere tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).



Per ulteriori informazioni su come i tag di funzionalità e di vincolo consentono di controllare i posizionamenti delle distribuzioni, vedere il tutorial video [Constraint Tags and Placement](#).

- 7 Fare clic su **Salva**.

Risultati

L'account viene aggiunto a vRealize Automation e le regioni selezionate sono disponibili per la zona cloud specificata.

Operazioni successive

Creare risorse dell'infrastruttura per questo account cloud.

Quando si aggiunge un account cloud di Azure a un modello cloud, è possibile scegliere di riutilizzare i set di disponibilità se lo si desidera. Poiché le sottoscrizioni hanno un limite di 2.000 set di disponibilità e 25.000 macchine virtuali, è opportuno riutilizzare i set di disponibilità quando possibile. Esistono due proprietà YAML che è possibile utilizzare per controllare in che modo le distribuzioni utilizzano i set di disponibilità. La proprietà `availabilitySetName` consente di specificare un set di disponibilità da utilizzare. La seconda proprietà è `doNotAttachAvailabilitySet`, impostata su `false` per impostazione predefinita. Se questa proprietà è impostata su `true`, vRealize Automation crea la distribuzione senza set di disponibilità.

Non è possibile creare una distribuzione senza un set di disponibilità se si utilizza un bilanciamento del carico collegato alla macchina virtuale.

La seguente tabella descrive il comportamento di vRealize Automation in base al fatto che nel modello cloud siano specificati un gruppo di risorse e un set di disponibilità.

Un set di disponibilità non può esistere senza far parte di un gruppo di risorse. I set di disponibilità in un determinato gruppo di risorse devono avere nomi univoci. I set di disponibilità possono avere lo stesso nome solo se fanno parte di gruppi di risorse diversi.

Se non si specifica il nome di un gruppo di risorse, vRealize Automation creerà un nuovo gruppo di risorse. Ciò significa che è necessario creare anche un nuovo set di disponibilità anche se viene passato un nome. Il nuovo set utilizzerà il nome passato.

Tabella 3-16.

Gruppo di risorse specificato	Set di disponibilità specificato	Risultato
No	No	vRealize Automation crea un nuovo gruppo di risorse e un nuovo set di disponibilità per la macchina virtuale.
Sì	No	vRealize Automation riutilizza il gruppo di risorse esistente e crea un nuovo set di disponibilità per la macchina virtuale.
No	Sì	vRealize Automation crea un nuovo gruppo di risorse e un nuovo set di disponibilità con il nome specificato.
Sì	Sì	vRealize Automation riutilizza il gruppo di risorse esistente. Se in tale gruppo esiste già un set di disponibilità con il nome specificato, verrà riutilizzato. Se nel gruppo non è presente alcun set di disponibilità con il nome specificato, ne verrà creato uno nuovo con lo stesso nome.

Cloud Assembly supporta gli snapshot dei dischi di Azure per le macchine virtuali distribuite. Vedere [Utilizzo degli snapshot per i dischi delle macchine virtuali di Microsoft Azure in vRealize Operations Manager](#) per ulteriori informazioni.

Cloud Assembly supporta diverse opzioni di diagnostica all'avvio per le distribuzioni di Azure. La diagnostica all'avvio supporta il debug delle macchine virtuali Azure e include la raccolta di informazioni di registro e le screenshot pertinenti. Vedere [Utilizzo della diagnostica all'avvio e dell'analisi dei registri con una macchina virtuale Microsoft Azure](#) per ulteriori informazioni.

Utilizzo della diagnostica all'avvio e dell'analisi dei registri con una macchina virtuale Microsoft Azure

È possibile richiamare e configurare la diagnostica all'avvio di Microsoft Azure da un'istanza di Azure in un modello cloud. È inoltre possibile configurare l'analisi dei registri per un'istanza della macchina virtuale Azure. La diagnostica all'avvio è una funzionalità di debug per le macchine virtuali Azure che facilita la diagnostica degli errori di avvio delle macchine virtuali. Utilizzando la diagnostica all'avvio, l'utente può monitorare lo stato della macchina virtuale mentre viene avviata, raccogliendo screenshot e informazioni sul registro in serie.

Diagnostica all'avvio

La diagnostica all'avvio acquisisce gli screenshot e le informazioni del registro in serie, che devono essere salvati nel disco. Il disco può essere di due tipi; Disco gestito o Disco non gestito di Azure.

La proprietà YAML `bootDiagnostics` è supportata nei modelli cloud di Azure. Quando questa proprietà è impostata su `true`, la diagnostica all'avvio è abilitata nella distribuzione della macchina virtuale Azure applicabile.

Il seguente frammento di codice YAML mostra un esempio di come viene utilizzata la proprietà `bootDiagnostics`.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Azure_Machine_1:
    type: Cloud.Azure.Machine
    metadata:
      layoutPosition:
        - 0
        - 0
    properties:
      image: ubuntu
      flavor: small
      bootDiagnostics: true
```

La diagnostica all'avvio può essere richiamata anche in una macchina virtuale Azure distribuita come operazione giorno 2. Passare alla pagina Distribuzioni in Cloud Assembly e selezionare la distribuzione Azure. Il menu Azioni in questa pagina consente di alternare tra Abilita diagnostica all'avvio e Disabilita diagnostica all'avvio.

Dopo aver distribuito un modello cloud con la diagnostica all'avvio abilitata, la pagina Cloud Assembly distribuzione iniziale per la distribuzione indicherà che la diagnostica di avvio è abilitata. Se si desidera disabilitare la diagnostica all'avvio, fare clic sul menu Azioni nella pagina Distribuzioni e selezionare Disabilita diagnostica all'avvio.

Log Analytics

Log Analytics consente di modificare ed eseguire query dei registri dai dati raccolti da Azure Monitor Logs e quindi di analizzare i risultati in modo interattivo. È possibile utilizzare le query di Log Analytics per recuperare i record che corrispondono a specifici criteri per consentire di identificare tendenze e modelli e quindi fornire una varietà di dettagli sui dati. Abilitando Log Analytics su una macchina virtuale Azure, tale macchina fungerà da origine dati.

Prima di poter configurare le analisi dei registri in un modello cloud di Cloud Assembly, è necessario creare e configurare un'area di lavoro Log Analytics di Azure. È possibile eseguire questa operazione utilizzando l'opzione Macchine virtuali nel menu Monitor di Azure. Per ulteriori informazioni, consultare la documentazione di Azure.

Per configurare le analisi dei registri, è necessario disporre dell'ID dell'area di lavoro di Azure e della chiave dell'area di lavoro. È possibile trovarli nella scheda Gestione agenti in Azure nell'area di lavoro Log Analytics.

Il seguente esempio di modello cloud mostra in che modo è possibile configurare le analisi dei registri utilizzando le estensioni.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Azure_Machine_1:
    type: Cloud.Azure.Machine
    properties:
      image: ubuntu
      flavor: small
    extensions:
      - autoUpgradeMinorVersion: true
        name: test-loga
        protectedSettings:
          workspaceKey: xxxxxxxxxx
        publisher: Microsoft.EnterpriseCloud.Monitoring
        settings:
          workspaceId: aaaaaaaaaa
          type: OmsAgentForLinux
          typeHandlerVersion: '1.0'
```

Dopo aver distribuito un modello cloud con Log Analytics abilitato, è possibile abilitarlo o disabilitarlo utilizzando le opzioni del menu Azioni nella pagina Distribuzioni di Cloud Assembly per la distribuzione.

Utilizzo degli snapshot per i dischi delle macchine virtuali di Microsoft Azure in vRealize Operations Manager

È possibile creare snapshot completi o incrementali di dischi gestiti di Microsoft Azure.

La pagina Distribuzioni di Cloud Assembly per una distribuzione Azure contiene un menu Azioni che offre diverse opzioni per la creazione e l'eliminazione di snapshot dalle distribuzioni Azure in dischi gestiti di macchine virtuali e in dischi gestiti indipendenti. L'elenco seguente illustra le funzionalità di snapshot specifiche supportate.

- Creazione di uno snapshot del disco: supportato sia per i dischi esterni che per quelli di elaborazione. È inoltre possibile creare snapshot per un disco in un gruppo di risorse diverso.
- Eliminazione di uno snapshot del disco: supportato solo per i dischi esterni
- Crittografia degli snapshot utilizzando un set di crittografia del disco di Azure.
- È possibile fornire coppie chiave-valore come tag durante la creazione dello snapshot.

Gli snapshot sui dischi non gestiti non sono attualmente supportati.

Se si utilizza la crittografia, l'implementazione dello snapshot corrente supporta la crittografia con chiave gestita dalla piattaforma. Per impostazione predefinita, il criterio di rete consente l'accesso da qualsiasi punto, pertanto non è possibile limitare l'accesso agli snapshot utilizzando il criterio di rete.

Per ulteriori informazioni sull'utilizzo della pagina Azioni e della pagina Distribuzioni di Cloud Assembly, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Per ulteriori informazioni sul supporto degli snapshot di Microsoft Azure, vedere [Creazione di uno snapshot di un disco rigido virtuale](#) nella documentazione del prodotto Microsoft.

Creazione di un account cloud di Amazon Web Services in vRealize Automation

L'amministratore del cloud può creare un account cloud di Amazon Web Services (AWS) per le regioni dell'account in cui il suo team distribuirà i modelli cloud di vRealize Automation.

La seguente procedura illustra come configurare un account cloud di AWS.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore necessarie e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente necessario. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre delle credenziali di amministratore AWS necessarie.
- Se non si dispone di accesso a Internet esterno, configurare un server proxy Internet. Vedere [Come configurare un server proxy Internet per vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account AWS e immettere le credenziali e altri valori.
- 3 Fare clic su **Convalida**.

Vengono raccolte le regioni dell'account associate all'account.

- 4 Selezionare le regioni in cui si desidera eseguire il provisioning della risorsa.
- 5 Per migliorare l'efficienza, fare clic su **Creare una zona cloud per le regioni selezionate**.
- 6 Se è necessario aggiungere tag per supportare una strategia di assegnazione dei tag, immettere tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).



Per ulteriori informazioni su come i tag di funzionalità e di vincolo consentono di controllare i posizionamenti delle distribuzioni, vedere il tutorial video [Constraint Tags and Placement](#).

- 7 Fare clic su **Aggiungi**.

Risultati

L'account viene aggiunto a vRealize Automation e le regioni selezionate sono disponibili per la zona cloud specificata.

Operazioni successive

Configurare le risorse dell'infrastruttura per questo account cloud.

Creazione di un account cloud di Google Cloud Platform in vRealize Automation

L'amministratore del cloud può creare un account cloud di Google Cloud Platform (GCP) per le regioni dell'account in cui il suo team distribuirà i modelli cloud di vRealize Automation.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore necessarie e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente necessario. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di poter accedere alla chiave di sicurezza JSON di Google Cloud Platform.
- Verificare di disporre delle informazioni di sicurezza necessarie per l'istanza di Google Cloud Platform. È possibile ottenere la maggior parte di queste informazioni dall'istanza o dalla documentazione di Google.
- Se non si dispone di accesso a Internet esterno, configurare un server proxy Internet. Vedere [Come configurare un server proxy Internet per vRealize Automation](#).

Procedura

- 1 In Cloud Assembly, selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account di Google Cloud Platform e immettere le credenziali appropriate e le informazioni correlate. Utilizzare l'account del servizio creato quando è stato inizializzato il motore di elaborazione dell'account GCP di origine.

Come indicato nella sezione **Prerequisiti** precedente, i requisiti delle credenziali sono disponibili in [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#). Per creare l'account cloud in vRealize Automation, nell'account GCP di origine deve essere abilitato il servizio del motore di elaborazione.

In vRealize Automation, l'ID del progetto fa parte dell'endpoint di Google Cloud Platform. È possibile specificarlo quando si crea l'account cloud. Durante la raccolta dei dati delle immagini private specifiche del progetto, l'adattatore GCP di vRealize Automation esegue una query nell'API di Google Cloud Platform.

3 Fare clic su Convalida.

Vengono raccolte le regioni dell'account associate all'account.

4 Selezionare le regioni in cui si desidera eseguire il provisioning della risorsa.**5 Per migliorare l'efficienza, fare clic su Creare una zona cloud per le regioni selezionate.****6 Se sono necessari tag per supportare una strategia di assegnazione dei tag, immettere i tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).**

Per ulteriori informazioni su come i tag di funzionalità e di vincolo consentono di controllare i posizionamenti delle distribuzioni, vedere il tutorial video [Constraint Tags and Placement](#).

7 Fare clic su Aggiungi.**Risultati**

L'account viene aggiunto a vRealize Automation e le regioni selezionate sono disponibili per la zona cloud specificata.

Operazioni successive

Creare risorse dell'infrastruttura per questo account cloud.

I seguenti paragrafi forniscono alcune informazioni sulla distribuzione di una macchina virtuale di Google Cloud Platform da Cloud Assembly.

Quando si aggiunge un account cloud di Google Cloud Platform a un modello cloud di Cloud Assembly, è possibile utilizzare la proprietà YAML di `useSoleTenant` per indicare che si desidera distribuire una macchina virtuale in un unico nodo tenant. Questa configurazione consente di isolare le macchine virtuali per motivi di sicurezza, privacy o altri problemi.

Per facilitare questa funzionalità, le etichette di affinità dei nodi di Google Cloud Platform vengono convertite in tag in Cloud Assembly, i quali vengono applicati nelle zone di disponibilità di vRealize Automation pertinenti in cui risiedono i gruppi di nodi. Quando la proprietà `useSoleTenant` è impostata su `true`, i tag di vincolo devono essere una delle etichette di affinità dei nodi. Inoltre, per distribuire una macchina in modalità tenant unica, è necessario includere la proprietà `useSoleTenant` personalizzata nel modello cloud, nonché i tag di vincolo.

Prima di utilizzare questa funzionalità, è necessario creare il modello di nodo e le etichette di affinità dei nodi appropriati in Google Cloud Platform, quindi creare un gruppo di nodi.

Il seguente esempio di codice YAML mostra in che modo è possibile utilizzare la proprietà `useSoleTenant` nei modelli cloud di Cloud Assembly. I tag di vincolo sono le etichette di affinità dei nodi che sono state raccolte automaticamente dal server di Google Cloud Platform.

```
resources:
  Cloud_GCP_Machine_1:
    type: Cloud.GCP.Machine
```

```
properties:
  image: ubuntu
  flavor: c2-family
  name: demo-vm
  useSoleTenant: true
  constraints:
    -tag: 'env:prod'
    -tag: 'region:asia-east1'
```

Creazione di un account cloud di vCenter in vRealize Automation

È possibile aggiungere un account cloud vCenter per le regioni dell'account in cui si desidera distribuire modelli cloud di vRealize Automation.

Per motivi di sicurezza e di rete, è possibile associare un account cloud di vCenter a un account cloud di NSX-T o NSX-V.

Un account cloud di NSX-T può essere associato a uno o più account cloud di vCenter. Tuttavia, un account cloud di NSX-V può essere associato a un solo account cloud di vCenter.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore necessarie e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di aver configurato correttamente le porte e i protocolli per supportare l'account cloud. Vedere l'argomento *Porte e protocolli per vRealize Automation* in *Installazione di vRealize Automation con vRealize Easy Installer* e l'argomento *Requisiti delle porte* in *Guida all'architettura di riferimento di vRealize Automation* nella [documentazione di prodotto di vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account vCenter e immettere l'indirizzo IP dell'host vCenter Server.
- 3 Immettere le credenziali di amministratore di vCenter Server e fare clic su **Convalida**.

Vengono raccolti i dati di tutti i data center associati all'account. Vengono raccolti i dati e tutti i tag vSphere dei seguenti elementi:

- Macchine
- Cluster e host
- Gruppi di porte
- Datastore

- 4 Selezionare almeno uno dei data center disponibili nell'istanza di vCenter Server specificata per consentire il provisioning per questo account cloud.

- 5 Per l'efficienza, creare una zona cloud per il provisioning nei data center selezionati.

È inoltre possibile creare zone cloud in un passaggio separato in base alla strategia cloud dell'organizzazione.

Per informazioni sulle zone cloud, vedere [Ulteriori informazioni sulle zone cloud di Cloud Assembly](#).

- 6 Selezionare un account cloud di NSX esistente.

L'account di NSX può essere selezionato ora o in un secondo momento quando si modifica l'account cloud.

Per informazioni sugli account cloud di NSX-V, vedere [Creazione di un account cloud di NSX-V in vRealize Automation](#).

Per informazioni sugli account cloud di NSX-T, vedere [Creazione di un account cloud di NSX-T in vRealize Automation](#).

Per informazioni su come apportare modifiche all'associazione dopo aver distribuito un modello cloud, vedere [Che cosa accade se si rimuove un'associazione di account cloud di NSX in vRealize Automation](#).

- 7 Se si desidera aggiungere tag per supportare una strategia di assegnazione dei tag, immettere tag di funzionalità.

È possibile aggiungere tag ora o in un secondo momento quando si modifica l'account cloud. Per informazioni sull'assegnazione dei tag, vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#).



Per ulteriori informazioni su come i tag di funzionalità e di vincolo consentono di controllare i posizionamenti delle distribuzioni, vedere il tutorial video [Constraint Tags and Placement](#).

- 8 Fare clic su **Salva**.

Risultati

L'account cloud viene aggiunto e i data center selezionati sono disponibili per la zona cloud specificata. I dati raccolti, come macchine, reti, storage e volumi, sono elencati nella sezione **Risorse** della scheda **Infrastruttura**.

Operazioni successive

Configurare le risorse dell'infrastruttura rimanenti per questo account cloud. Vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).

Creazione di un account cloud di NSX-V in vRealize Automation

Per motivi di sicurezza e di rete, è possibile creare e associare un account cloud di NSX-V a un account cloud di vCenter.

Un account cloud di NSX-V può essere associato a un solo account cloud di vCenter.

L'associazione tra NSX-V e un account cloud di vCenter deve essere configurata all'esterno di vRealize Automation, in particolare nell'applicazione NSX. vRealize Automation non crea l'associazione tra NSX e vCenter. In vRealize Automation, è possibile specificare un'associazione già esistente in NSX.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore necessarie e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre di un account cloud vCenter da utilizzare con questo account cloud NSX. Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).
- Verificare di aver configurato correttamente le porte e i protocolli per supportare l'account cloud. Vedere l'argomento *Porte e protocolli per vRealize Automation* in *Installazione di vRealize Automation con vRealize Easy Installer* e l'argomento *Requisiti delle porte* in *Guida all'architettura di riferimento di vRealize Automation* nella [documentazione di prodotto di vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account NSX-V e immettere l'indirizzo IP dell'host NSX-V.
- 3 Immettere le credenziali di amministratore di NSX e fare clic su **Convalida**.
Vengono raccolte le risorse associate all'account.
Se l'indirizzo IP dell'host di NSX non è disponibile, la convalida non riesce.
- 4 Se disponibile, selezionare l'endpoint vCenter che rappresenta l'account cloud vCenter che si sta associando a questo account NSX-V.

Solo gli account cloud di vCenter che non sono attualmente associati a un account cloud di NSX-T o NSX-V sono disponibili per la selezione.

Per informazioni su come apportare modifiche all'associazione dopo aver distribuito un modello cloud, vedere [Che cosa accade se si rimuove un'associazione di account cloud di NSX in vRealize Automation](#).

- 5 Se si desidera aggiungere tag per supportare una strategia di assegnazione dei tag, immettere tag di funzionalità.

È possibile aggiungere o rimuovere tag di funzionalità in un secondo momento. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#).



Per informazioni su come i tag di funzionalità e di vincolo consentono di controllare i posizionamenti delle distribuzioni, vedere il tutorial video [Constraint Tags and Placement](#).

- 6 Fare clic su **Salva**.

Operazioni successive

È possibile creare o modificare un account cloud di vCenter da associare a questo account cloud di NSX. Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).

Creare e configurare una o più zone cloud da utilizzare con i data center usati da questo account cloud. Vedere [Ulteriori informazioni sulle zone cloud di Cloud Assembly](#).

Configurare le risorse dell'infrastruttura per questo account cloud. Vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).

Creazione di un account cloud di NSX-T in vRealize Automation

Per motivi di rete e sicurezza, è possibile creare un account cloud di NSX-T e associarlo a uno o più account cloud di vCenter.

Un account cloud di NSX-T può essere associato a uno o più account cloud di vCenter. Tuttavia, un account cloud di NSX-V può essere associato a un solo account cloud di vCenter.

L'associazione tra NSX-T e uno o più account cloud di vCenter deve essere configurata all'esterno di vRealize Automation, in particolare nell'applicazione NSX. vRealize Automation non crea l'associazione tra NSX e vCenter. In vRealize Automation, è possibile specificare una o più associazioni di configurazione già esistenti in NSX.

Quando si crea un account cloud di NSX-T in vRealize Automation, è necessario specificare un tipo di gestione e una modalità NSX. Queste selezioni non possono essere modificate dopo la creazione dell'account cloud.

È possibile connettersi a un Manager globale di NSX-T e configurare un'associazione tra un Manager globale di NSX-T e manager locali nel contesto della federazione di NSX-T.

Per informazioni correlate sulle opzioni e sulle funzionalità in generale di NSX-T, vedere la [documentazione di prodotto di NSX-T Data Center](#).

Per semplificare la tolleranza agli errori e l'alta disponibilità nelle distribuzioni, ogni endpoint del data center di NSX-T rappresenta un cluster di tre NSX Manager.

- vRealize Automation può puntare a una delle istanze di NSX Manager. Utilizzando questa opzione, un NSX Manager riceve le chiamate API da vRealize Automation.

- vRealize Automation può puntare all'IP virtuale del cluster. Utilizzando questa opzione, un NSX Manager assume il controllo del VIP. Tale istanza di NSX Manager riceve le chiamate API da vRealize Automation. In caso di errore, un altro nodo del cluster assume il controllo del VIP e riceve le chiamate API da vRealize Automation.

Per ulteriori informazioni sulla configurazione di VIP per NSX, vedere l'argomento relativo alla *configurazione di un indirizzo IP virtuale (VIP) per un cluster* nella *guida all'installazione di NSX-T Data Center* all'interno della [documentazione di VMware NSX-T Data Center](#).

- vRealize Automation può puntare a un VIP del bilanciamento del carico per bilanciare il carico delle chiamate ai tre NSX Manager. Utilizzando questa opzione, tutti e tre le istanze di NSX Manager ricevono chiamate API da vRealize Automation.

È possibile configurare il VIP in un bilanciamento del carico di terze parti o in un bilanciamento del carico di NSX-T.

Per gli ambienti su larga scala, è consigliabile utilizzare questa opzione per suddividere le chiamate API di vRealize Automation fra le tre istanze di NSX Manager.

Per un'analisi dettagliata sull'utilizzo di NSX-T 3.2 con vRealize Automation, vedere il post del blog [VMware Network Automation con NSX-T 3.2 e vRealize Automation](#).

Prerequisiti

- Verificare di disporre delle credenziali di amministratore necessarie e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre di un account cloud vCenter da utilizzare con questo account cloud NSX. Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).
- Verificare di aver configurato correttamente le porte e i protocolli per supportare l'account cloud. Vedere l'argomento *Porte e protocolli per vRealize Automation* in *Installazione di vRealize Automation con vRealize Easy Installer* e l'argomento *Requisiti delle porte* in *Guida all'architettura di riferimento di vRealize Automation* nella [documentazione di prodotto di vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account di NSX-T e specificare un nome e una descrizione dell'account cloud.
- 3 Immettere l'indirizzo IP dell'host per il VIP o l'istanza di NSX-T Manager (vedere sopra per informazioni sul comportamento previsto per le opzioni di NSX Manager e VIP).
- 4 Immettere le proprie credenziali di nome utente e password da amministratore di NSX.

5 In **Tipo di manager**, selezionare **Globale** o **Locale** (predefinito).

■ Manager globale

L'impostazione Manager globale è disponibile per l'utilizzo solo con l'impostazione **Modalità NSX** di Criterio. Non è disponibile quando si utilizza l'impostazione **Modalità NSX** di Manager.

L'impostazione Globale fa riferimento alle funzionalità della federazione di NSX-T, inclusi i segmenti della rete globale. Solo gli account cloud di NSX-T con l'impostazione Globale supportano la federazione di NSX-T.

Quando si utilizza l'impostazione Manager globale, viene richiesto di identificare un account cloud di NSX-T del Manager locale e un account cloud di vCenter Server associato.

Non è possibile associare un account cloud di NSX-T del Manager globale all'account cloud di vCenter come invece è possibile fare con un account cloud di NSX-T del Manager locale. Analogamente alla modalità con cui è possibile associare un account cloud di NSX-T del Manager locale a più account cloud di vCenter, un account cloud di NSX-T del Manager globale può essere associato a più account cloud di NSX-T del Manager locale.

■ Manager locale

Utilizzare l'impostazione Locale per definire un account cloud di NSX-T tradizionale, che può essere associato a uno o più account cloud di vSphere. È possibile associare un account cloud di NSX-T del Manager globale agli account cloud di NSX-T del Manager locale. Si tenga presente che questa è l'impostazione da utilizzare anche quando si crea un account cloud di NSX-T di destinazione nuovo e vuoto per la migrazione da NSX-V a NSX-T.

Non è possibile modificare l'impostazione **Tipo di manager** dopo aver creato l'account cloud.

6 Per **Modalità NSX**, selezionare **Policy** o **Manager**.

■ Modalità Policy (predefinita)

La modalità Policy è disponibile per NSX-T 3.0 e NSX-T 3.1 e versioni successive. Questa opzione consente a vRealize Automation di utilizzare le funzionalità aggiuntive disponibili nell'API Policy di NSX-T.

Se si utilizza NSX-T con un account cloud di VMware Cloud on AWS in un modello cloud, l'account cloud di NSX-T deve utilizzare la **Modalità NSX** di Policy.

L'impostazione Policy si riferisce al modulo dell'API NSX-T Policy di NSX-T.

■ Modalità Manager

Gli endpoint o gli account cloud esistenti di NSX-T che vengono aggiornati da una versione precedente di vRealize Automation che non hanno fornito un'opzione Policy vengono trattati come modalità Manager per gli account cloud di NSX-T.

La modalità Manager è supportata per NSX-T 2.4, NSX-T 3.0, NSX-T 3.1 e versioni successive.

Se si specifica la modalità Manager, utilizzare l'opzione Modalità Manager per gli altri account cloud di NSX-T finché vRealize Automation non introduce una modalità Manager al percorso di migrazione verso la modalità Policy.

Alcune opzioni di vRealize Automation per NSX-T, tra cui l'aggiunta di tag ai componenti NIC della macchina virtuale nel modello cloud, richiedono NSX-T 3.0 o versione successiva.

L'impostazione Manager fa riferimento al modulo dell'API NSX-T Manager di NSX-T.

Eventuali account cloud di NSX-T esistenti, creati prima dell'introduzione della modalità Policy in vRealize Automation 8.2 utilizzano il metodo API Manager. È consigliabile attendere che venga reso disponibile in vRealize Automation lo strumento di migrazione da API Manager ad API Policy. Se si preferisce non attendere, è necessario sostituire gli account cloud di NSX-T esistenti con nuovi account cloud di NSX-T in cui venga specificato il metodo API Policy.

Non è possibile modificare il valore **Modalità NSX** dopo aver creato l'account cloud.

- 7 Fare clic su **Convalida** per confermare le credenziali in relazione al tipo di NSX Manager e alla modalità NSX selezionati.

Vengono raccolte le risorse associate all'account.

Se l'indirizzo IP dell'host di NSX non è disponibile, la convalida non riesce.

- 8 In **Associazioni**, aggiungere uno o più account cloud di vCenter da associare a questo account cloud di NSX-T. È inoltre possibile rimuovere le associazioni di account cloud di vCenter esistenti.

Solo gli account cloud di vCenter che non sono associati a un account cloud di NSX-T o NSX-V in vRealize Automation sono disponibili per la selezione.

Vedere [Quali operazioni è possibile eseguire con la mappatura di NSX-T a più vCenter in vRealize Automation](#).

Per informazioni su come apportare modifiche all'associazione dopo aver distribuito un modello cloud o su come eliminare l'account cloud dopo aver distribuito un modello cloud, vedere [Che cosa accade se si rimuove un'associazione di account cloud di NSX in vRealize Automation](#).

- 9 Se si desidera aggiungere tag per supportare una strategia di assegnazione dei tag, immettere tag di funzionalità.

È possibile aggiungere o rimuovere tag di funzionalità in un secondo momento. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#).



Per ulteriori informazioni su come i tag di funzionalità e di vincolo consentono di controllare i posizionamenti delle distribuzioni, vedere il tutorial video [Constraint Tags and Placement](#).

- 10 Fare clic su **Salva**.

Operazioni successive

È possibile creare o modificare un account cloud di vCenter da associare a questo account cloud di NSX. Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).

Creare e configurare una o più zone cloud da utilizzare con i data center usati da questo account cloud. Vedere [Ulteriori informazioni sulle zone cloud di Cloud Assembly](#).

Configurare le risorse dell'infrastruttura per questo account cloud. Vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).

Per esempi di utilizzo delle opzioni di NSX-T nei modelli cloud di vRealize Automation, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation

L'amministratore del cloud può creare un account cloud di VMware Cloud on AWS per le regioni dell'account in cui il suo team distribuirà i modelli cloud di vRealize Automation.

VMware Cloud on AWS richiede alcune procedure di configurazione specifiche in vRealize Automation. Per configurare correttamente vRealize Automation per VMware Cloud on AWS, inclusa l'impostazione dei valori di un token API per l'account cloud e l'impostazione delle regole del firewall del gateway per il proxy cloud, vedere il workflow [Tutorial: configurazione di VMware Cloud on AWS per vRealize Automation](#).

Prerequisiti

- Verificare di disporre delle credenziali di amministratore di VMware Cloud on AWS necessarie, incluse le credenziali CloudAdmin di VMware Cloud on AWS per l'SDDC di destinazione in vCenter e che sia stato abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Se non si dispone di accesso a Internet esterno, configurare un server proxy Internet. Vedere [Come configurare un server proxy Internet per vRealize Automation](#).
- Verificare di aver configurato le regole di accesso e del firewall necessarie in SDDC. Vedere [Preparazione dell'SDDC di VMware Cloud on AWS per la connessione con gli account cloud di VMware Cloud on AWS in vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud**, fare clic su **Aggiungi account cloud** e selezionare il tipo di account VMware Cloud on AWS.

- 2 Aggiungere il **token dell'API VMC** affinché l'organizzazione acceda agli SDDC disponibili.

È possibile creare un nuovo token o utilizzare un token esistente per l'organizzazione nella pagina **Token API** collegata. Per i dettagli, vedere [Creazione di un account cloud di VMware Cloud on AWS in vRealize Automation all'interno di un workflow di esempio](#).

- 3 Selezionare l'SDDC che deve essere disponibile per le distribuzioni.

Gli SDDC di NSX-V non sono supportati e non sono presenti nell'elenco.

I valori dell'indirizzo IP o del nome di dominio completo di vCenter e NSX-T Manager vengono automaticamente compilati in base all'SDDC.

- 4 Immettere il nome utente e la password di vCenter per l'SDDC specificato, se diversi dal valore predefinito di cloudadmin@vmc.local.

- 5 Fare clic su **Convalida** per verificare i diritti di accesso all'istanza di vCenter specificata e controllare che vCenter sia in esecuzione.

Vengono raccolti i data center associati all'account.

- 6 Per l'efficienza, creare una zona cloud per il provisioning negli SDDC selezionati.

È inoltre possibile creare zone cloud in un passaggio separato in base alla strategia cloud dell'organizzazione.

- 7 Se si desidera aggiungere tag per supportare una strategia di assegnazione dei tag, immettere tag di funzionalità.

È possibile aggiungere o rimuovere tag di funzionalità in un secondo momento. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#).



Per ulteriori informazioni su come i tag di funzionalità e di vincolo consentono di controllare i posizionamenti delle distribuzioni, vedere il tutorial video [Constraint Tags and Placement](#).

Come per le macchine virtuali distribuite in vSphere, è possibile configurare i tag delle macchine per una macchina virtuale da distribuire in VMware Cloud on AWS. È inoltre possibile aggiornare il tag della macchina dopo la distribuzione iniziale. Questi tag della macchina consentono a vRealize Automation di assegnare dinamicamente una macchina virtuale a un gruppo di sicurezza di NSX-T appropriato durante la distribuzione. Per informazioni correlate, vedere [Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation](#).

- 8 Fare clic su **Salva**.

Risultati

L'account cloud viene aggiunto e l'SDDC selezionato è disponibile per la zona cloud specificata.

Operazioni successive

Per configurare correttamente vRealize Automation per VMware Cloud on AWS, vedere [Tutorial: configurazione di VMware Cloud on AWS per vRealize Automation](#).

Per informazioni relative a VMware Cloud on AWS all'esterno di vRealize Automation, vedere [Documentazione di VMware Cloud on AWS](#).

Creazione di un account cloud di VMware Cloud Foundation

È possibile configurare un'istanza di VMware Cloud Foundation (VCF) come account cloud all'interno di Cloud Assembly per utilizzare i domini del carico di lavoro.

Un account cloud di VCF consente di incorporare un carico di lavoro di VCF in Cloud Assembly per agevolare una soluzione di gestione del cloud ibrido completa. Cloud Assembly offre diversi punti di ingresso da cui è possibile attivare la pagina di configurazione dell'account cloud di VCF. Se si accede a questa pagina utilizzando il pulsante **Aggiungi account cloud** nella scheda Dominio carico di lavoro dell'integrazione di SDDC, il carico di lavoro è preselezionato, così come le informazioni di base per vCenter e NSX Manager.

Prerequisiti

È necessario disporre di un'istanza di VMware SDDC Manager 4.1 o versione successiva configurata come integrazione di Cloud Assembly da utilizzare con questo account cloud. Per ulteriori informazioni, vedere [Configurazione di un'integrazione di VMware SDDC Manager](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account cloud di VCF, quindi immettere un **Nome** e una **Descrizione**.
- 3 Immettere il nome di dominio completo e le credenziali per l'istanza di SDDC Manager utilizzata con questo account cloud.

È possibile ignorare questo passaggio se è già stata configurata l'istanza di SDDC Manager che verrà utilizzata con questo account.

- 4 Selezionare uno o più domini del carico di lavoro che si desidera utilizzare con questo account cloud di VCF.
- 5 Se si desidera che Cloud Assembly utilizzi le credenziali del servizio gestito di Cloud Foundation per vCenter e NSX, selezionare **Crea automaticamente credenziali del servizio**. In un secondo momento, se si desidera modificare queste credenziali, è necessario utilizzare il meccanismo VCF per la gestione delle password.

Se si seleziona questa opzione, è possibile ignorare i passaggi 7 e 8.

- 6 Immettere le credenziali necessarie per accedere al vCenter associato a questo account cloud.

- 7 Nell'installazione NSX Manager, immettere le credenziali di NSX se si desidera inserire manualmente le credenziali per l'account cloud VCF oppure fare clic su **Crea** e convalida credenziali del servizio se si desidera che Cloud Assembly crei e convalidi le credenziali di NSX.
- 8 Immettere le credenziali necessarie per accedere alla rete NSX-T associata a questo account cloud.
- 9 Se applicabile, selezionare la modalità NSX.
- 10 Fare clic su **Convalida** per confermare una connessione a SDDC Manager.
- 11 Se applicabile, selezionare i data center in cui si desidera eseguire il provisioning sotto l'installazione Configurazione. Fare clic sulla casella di controllo se si desidera creare una zona cloud per i data center selezionati.
- 12 Se si utilizzano tag per supportare una strategia di assegnazione dei tag, immettere i tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).
- 13 Fare clic su **Salva**.

Risultati

Questo account cloud consente di utilizzare il dominio del carico di lavoro selezionato associandolo all'SDDC Manager specificato in Cloud Assembly.

Se si desidera gestire ulteriori domini del carico di lavoro utilizzando vRealize Automation, è necessario ripetere questo processo per ciascun dominio.

Operazioni successive

Dopo aver configurato l'account cloud di VCF, è possibile selezionare l'account nella pagina dell'account cloud principale e fare clic su **Configura cloud** per avviare la procedura guidata Avvio rapido di VMware Cloud Foundation che configurerà il cloud.

Per ulteriori informazioni sulla procedura guidata Avvio rapido, vedere [Come iniziare a utilizzare vRealize Automation utilizzando Avvio rapido di VMware Cloud Foundation](#) nella Guida introduttiva.

Creazione di un account cloud di VMware Cloud Director in vRealize Automation

È possibile creare un account cloud di VMware Cloud Director in vRealize Automation per distribuire le macchine virtuali di Cloud Director utilizzando oggetti indipendenti dal cloud. Cloud Director supporta il provisioning flessibile delle risorse di rete, storage ed elaborazione e offre un'esperienza basata su portale per gestire i vCenter e le relative appliance di rete NSX-T e NSX-V, nonché i virtual data center associati tramite un catalogo.

L'account cloud di VMware Cloud Director supporta la creazione di macchine virtuali Cloud Director standalone senza vApp. Sono supportati tre scenari per il provisioning delle macchine virtuali di Cloud Director tramite i modelli cloud di Cloud Assembly:

- Macchine virtuali
- Reti collegate alle macchine virtuali
- Macchine virtuali con dischi aggiuntivi

Per ulteriori informazioni sull'utilizzo di VMware Cloud Director, incluse le informazioni sulla configurazione di più server per l'alta disponibilità, consultare la documentazione ufficiale all'indirizzo <https://docs.vmware.com/it/VMware-Cloud-Director/index.html>.

L'account cloud di VMware Cloud Director supporta fino a 1000 macchine virtuali con vRealize Automation in modalità di supporto.

La procedura seguente illustra come configurare un account cloud di VMware Cloud Director in vRealize Automation Cloud Assembly.

Prerequisiti

- Configurare una distribuzione di VMware Cloud Director 10.2.0, 10.2.1, 10.2.2, 10.3 o 10.3.1 con una o più organizzazioni appropriate.
- Gli utenti specificati per questa integrazione devono disporre dei privilegi di amministratore dell'organizzazione per leggere i modelli applicabili e creare macchine virtuali, nonché per visualizzare altre risorse come i criteri di calcolo, i dischi, i virtual data center e così via.
L'account cloud VCD per vRealize Automation funziona all'interno di un contesto tenant in Cloud Director, pertanto è possibile connettersi a una singola organizzazione in Cloud Director con le credenziali del tenant. Per ulteriori informazioni sulle credenziali necessarie, vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- È necessario configurare il criterio di storage, rete, immagine e caratteristiche o dimensionamento appropriato nell'istanza di VMware Cloud Director e mappare questi oggetti in vRealize Automation Cloud Assembly prima o dopo aver configurato l'integrazione. L'elenco seguente illustra come mappare gli oggetti virtuali di VMware Cloud Director a oggetti di vRealize Automation in Cloud Assembly.
 - Reti di organizzazione di VMware Cloud Director (isolate, dirette, instradate): mappare alle reti di vRealize Automation. Non è possibile impostare pool di IP statici per la scheda di rete.
 - Criteri di dimensionamento delle macchine virtuali di VMware Cloud Director: mappare alle caratteristiche di vRealize Automation.
 - Criteri di storage di VMware Cloud Director: mappare ai profili di storage di vRealize Automation.

- Immagini di VMware Cloud Director (OVF, supporto di avvio ISO): mappare alle immagini di vRealize Automation. Le immagini possono essere un modello di vApp o un file multimediale come i file ISO. Se si utilizza ISO, viene creata una macchina virtuale "vuota" e il supporto viene collegato come supporto di avvio.
- Macchine virtuali di VMware Cloud Director: mappare alle risorse di elaborazione di vRealize Automation.
- Dischi delle macchine virtuali di VMware Cloud Director: mappare ai volumi cloud di vRealize Automation.

È possibile mappare questi oggetti di VMware Cloud Director a oggetti di vRealize Automation utilizzando le opzioni delle pagine **Infrastruttura > Configura >** in Cloud Assembly. Per informazioni dettagliate sulla mappatura degli oggetti in vRealize Automation, vedere gli argomenti pertinenti in [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Account cloud** e fare clic su **Aggiungi account cloud**.
- 2 Selezionare il tipo di account cloud di VMware Cloud Director, quindi immettere un **Nome** e una **Descrizione**.
- 3 Immettere le informazioni dell'account appropriate necessarie per accedere al server VMware Cloud Director.
- 4 Immettere l'URL di base da utilizzare per connettersi al server VMware Cloud Director.
- 5 Immettere un **Nome utente** e una **Password** per un account valido che possa accedere all'istanza di Cloud Director specificata.
- 6 Immettere il nome **Organizzazione** desiderato da utilizzare con questa integrazione.
In vCloud Director, un'organizzazione contiene gli utenti, le vApp che creano e le risorse utilizzate dalle vApp.
- 7 Fare clic su **Convalida**.
Durante la convalida, potrebbe essere necessario accettare un certificato. Quando la connessione viene convalidata, è possibile selezionare impostazioni aggiuntive.
- 8 Se si utilizzano tag per supportare una strategia di assegnazione dei tag, immettere i tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).
- 9 Dopo la convalida, nella pagina viene visualizzato un elenco di virtual data center di Cloud Director che è possibile selezionare. Selezionare il data center appropriato. Questa selezione determina le regioni di Director in cui è possibile distribuire.
- 10 Fare clic su **Aggiungi** per aggiungere l'account cloud di VMware Cloud Director a vRealize Automation.

Risultati

L'account cloud di VMware Cloud Director è disponibile per la configurazione in vRealize Automation. Le reti associate all'istanza di Cloud Director sono disponibili per la configurazione nella pagina Cloud Assembly **Risorse > Reti**. È possibile configurare i profili di storage appropriati e quindi utilizzare l'account cloud per creare distribuzioni nei modelli cloud. Assicurarsi inoltre che in Cloud Assembly sia configurato un progetto appropriato da utilizzare con l'istanza di Cloud Director.

Operazioni successive

L'account cloud di VMware Cloud Director è pronto per l'uso nei modelli cloud di Cloud Assembly.

Di seguito è riportato un modello cloud di esempio per una distribuzione di VMware Cloud Director di base.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: existing
      constraints:
        - tag: net1:isolated
  Cloud_Volume_1:
    type: Cloud.Volume
    properties:
      capacityGb: 2
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: image1
      flavor: small
      storage:
        constraints:
          - tag: storage:development
      attachedDisks:
        - source: '${resource.Cloud_Volume_1.id}'
      networks:
        - network: '${resource.Cloud_Network_1.id}'
```

Nelle macchine virtuali di VMware Cloud Director distribuite sono supportate le seguenti azioni del giorno 2:

- Accendi
- Spegni
- Sospendi
- Crea snapshot
- Ripristina snapshot

- Rimuovi snapshot
- Aggiungi disco
- Rimuovi disco
- Ridimensiona disco (nota: è supportato solo l'aumento della dimensione del disco)
- Ridimensiona disco di avvio

Dopo la distribuzione di un blueprint, gli utenti possono applicare tag alle macchine di cui è stato appena eseguito il provisioning in vRealize Automation. Questi tag vRealize Automation vengono mappati ai metadati di VMware Cloud Director che possono essere recuperati utilizzando l'API di VMware Cloud Director. Gli utenti possono anche contrassegnare altre risorse vRealize Automation, ma solo le macchine sul lato VMware Cloud Director vengono aggiornate perché è l'unico tipo di risorsa supportato di questa funzionalità.

Dopo la distribuzione di un blueprint, gli utenti possono ridimensionare il disco di avvio di una macchina virtuale. Sono supportati anche i dischi normali; in questo caso, i clienti devono solo collegare una risorsa disco a una risorsa macchina. Quando viene effettuata la distribuzione, è possibile utilizzare l'opzione per "aggiorna il disco di avvio" o "aggiorna il disco" per aumentare, ma non diminuire, le dimensioni del disco desiderato.

Dopo aver distribuito un blueprint, gli utenti possono modificare un criterio di dimensionamento della macchina virtuale utilizzando l'opzione di ridimensionamento della configurazione delle caratteristiche di vRealize Automation. Una volta selezionato, la macchina virtuale di VMware Cloud Director utilizzerà il criterio di dimensionamento fornito.

Questa funzionalità richiede che il **Bundle dei diritti predefinito** assegnato al ruolo Amministratore dell'organizzazione contenga il diritto "Modifica criteri di calcolo" per il quale il codice interno è `VAPP_EDIT_VM_COMPUTE_POLICY`. Questo diritto deve essere attivato per l'amministratore dell'organizzazione. In caso contrario l'operazione di ridimensionamento non riuscirà e verrà visualizzato un errore 403: `Either you need some or all of the following rights [VAPP_EDIT_VM_COMPUTE_POLICY] to perform operations.`

È possibile ridimensionare il disco di avvio di una macchina virtuale VMware Cloud Director come operazione giorno 2, selezionando la macchina virtuale nella pagina Distribuzioni. Tuttavia, è necessario disabilitare il provisioning rapido prima di tentare di ridimensionare il disco di avvio o potrebbe verificarsi il seguente errore:

```
Request timed out after 120 minutes. Please configure project request timeout
parameter for long running resource requests.
```

Si noti che questo requisito si applica solo alle macchine virtuali create dai dischi del modello di vApp. Non si applica alle macchine virtuali create dai file ISO.

La procedura seguente illustra come disabilitare il provisioning rapido.

- 1 Accedere a VMware Cloud Director come amministratore di sistema: `https://vcd_url/provider` con l'utente di sistema
- 2 Fare clic sui VDC dell'organizzazione.

- 3 Selezionare l'organizzazione di destinazione.
- 4 Fare clic su Storage (in Criteri).
- 5 Disabilitare **Provisioning rapido**.

Utilizzo dei registri e di altre risorse per risolvere i problemi degli account cloud di VMware Cloud Director in vRealize Automation

Se si verificano problemi durante la configurazione o l'utilizzo di un account cloud di VMware Cloud Director in vRealize Automation, è possibile consultare i registri e le altre risorse come descritto di seguito.

Risoluzione dei problemi di connessione dell'account cloud di VMware Cloud Director

Se l'adattatore di VMware Cloud Director non è elencato nella schermata di creazione dell'account cloud o non risponde, è possibile utilizzare il comando seguente per verificare lo stato accedendo all'host kubernetes di vRealize Automation e controllando lo stato del pod dell'adattatore:

```
root@host [ ~ ]# kubectl -n prelude get pods | grep adapter-host-service-app
adapter-host-service-app-65f5c945bb-p6hpn      1/1      Running    0          4dlh
```

Se l'adattatore VMware Cloud Director non è in grado di comunicare con la macchina fisica Cloud Director, nella schermata dell'account cloud viene visualizzato un errore con istruzioni sulle eccezioni di connessione ed elaborazione. L'errore viene visualizzato anche nei registri.

Utilizzo dei registri di VMware Cloud Director

Il file di registro principale dell'adattatore VMware Cloud Director si trova nella `directory locale /var/log/adapter-host-service-app.log` (pod) e, nel caso in cui l'adattatore venga eseguito all'interno dell'host dell'appliance vRealize Automation, questo registro viene copiato anche in `/services-logs/prelude/adapter-host-service-app/file-logs/`. Per impostazione predefinita, la maggior parte della registrazione è limitata ai livelli DEBUG o INFO. È possibile modificare la configurazione dei seguenti logger per abilitare una registrazione più dettagliata a scopo di debug:

- `org.apache.cxf.services=INFO`: questo logger fornisce informazioni dettagliate per la comunicazione tra l'adattatore e VMware Cloud Director.
- `com.vmware.vra.vcloud.director.adapter=TRACE`: questo logger fornisce informazioni dettagliate per la comunicazione tra l'adattatore e vRealize Automation.

Esistono tre modi per accedere ai registri:

- accesso al registro tramite login al pod dell'adattatore

```
root@host [ ~ ]# kubectl -n prelude exec -ti adapter-host-service-app-65f5c945bb-p6hpn --
bash
root [ / ]# less /var/log/adapter-host-service-app.log
```

- accesso al registro tramite kubectl

```
root@host [ ~ ]# kubectl -n prelude get logs adapter-host-service-app-65f5c945bb-p6hpn
```

- accesso al registro utilizzando la copia locale dell'host kubernetes dell'adattatore

```
root@host [ ~ ]# less /services-logs/prelude/adapter-host-service-app/file-logs/adapter-host-service-app.log
```

È possibile eseguire una query o modificare la configurazione dei logger tramite l'endpoint REST API /actuator/loggers.

- Esempio di abilitazione dell'analisi della comunicazione del client VMware Cloud Director tramite curl:

```
curl -i -X POST -H 'Content-Type: application/json' -d '{"configuredLevel": "INFO"}'
http://{adapter-url}/actuator/loggers/org.apache.cxf.services
```

- Esempio di disabilitazione dell'analisi della comunicazione del client VMware Cloud Director tramite curl:

```
curl -i -X POST -H 'Content-Type: application/json' -d '{"configuredLevel": "OFF"}'
http://{adapter-url}/actuator/loggers/org.apache.cxf.services
```

- Esempio di recupero della configurazione corrente per la comunicazione del client VMware Cloud Director tramite curl:

```
curl http://{adapter-url}/actuator/loggers/org.apache.cxf.services
...
{"configuredLevel":"OFF","effectiveLevel":"INFO"}
```

Esistono altri parametri che possono essere regolati per alterare le prestazioni di VMware Cloud Director.

- `vcd.max.thread.count`: questo parametro determina il massimo grado di parallelismo durante l'esecuzione delle chiamate API di VMware Cloud Director. Il valore predefinito è 128.

Nota La riduzione del valore di questo parametro ridurrà la pressione sul back-end di VMware Cloud Director durante l'esecuzione dell'enumerazione, ma potrebbe ridurre le prestazioni dell'enumerazione.

- `VCD_ADAPTER_PAGINATION_SIZE_IMAGES`: questo parametro determina le dimensioni della pagina durante l'esecuzione dell'enumerazione delle immagini. Il valore predefinito è 50.

Nota Diminuire questo parametro se si verificano errori di timeout dell'adattatore durante l'enumerazione dell'immagine.

Integrazione di vRealize Automation con altre applicazioni

Le integrazioni consentono di aggiungere sistemi esterni a vRealize Automation.

Le integrazioni includono vRealize Orchestrator, la gestione della configurazione e altri sistemi esterni, come GitHub, Ansible, Puppet e i provider IPAM esterni, tra cui Infoblox.

Nota Se non si dispone di accesso a Internet esterno e l'integrazione lo richiede, è possibile configurare un server proxy Internet. Vedere [Come configurare un server proxy Internet per vRealize Automation](#).

Come utilizzare l'integrazione di Git in Cloud Assembly

Cloud Assembly supporta l'integrazione con varie caratteristiche dei repository Git, consentendo in tal modo di gestire VMware Cloud Templates e gli script di azione nell'ambito del controllo dell'origine. Questa funzionalità facilita il controllo e la responsabilità relativa ai processi correlati alla distribuzione.

Cloud Assembly supporta diverse caratteristiche dell'integrazione Git, come descritto nell'elenco seguente. Ognuna di queste opzioni è un'integrazione separata.

- Cloud GitHub, GitHub Enterprise locale
- Cloud GitLab, GitLab Enterprise locale
- BitBucket locale

È necessario disporre di un repository Git locale appropriato configurato con l'accesso per tutti gli utenti designati per configurare l'integrazione di Git con Cloud Assembly. È inoltre necessario salvare i modelli cloud in una struttura specifica affinché vengano rilevati da Git. Per creare un'integrazione con GitLab o GitHub, selezionare **Infrastruttura > Connessioni > Integrazioni** in Cloud Assembly e quindi effettuare la selezione appropriata. Sono necessari l'URL e il token del repository di destinazione.

Quando l'integrazione di Git è configurata con un repository esistente, tutti i modelli cloud associati ai progetti selezionati diventano disponibili per gli utenti qualificati. È possibile utilizzare questi modelli con una distribuzione esistente o come base di una nuova distribuzione. Quando si aggiunge un progetto, è necessario selezionare alcune proprietà relative a luogo e modalità di archiviazione in Git.

È possibile salvare le azioni in un repository Git direttamente da Cloud Assembly. È possibile creare le versioni degli script di azione direttamente in Git oppure in Cloud Assembly. Se si crea una versione di un'azione in Cloud Assembly, viene salvata automaticamente in Git come versione. I modelli cloud sono un po' più complessi, perché non è possibile aggiungerli direttamente a un'integrazione Git da Cloud Assembly. È necessario salvarli direttamente in un'istanza di Git ed è quindi possibile recuperarli da Git quando si utilizza la pagina di gestione dei modelli cloud in Cloud Assembly.

Prima di iniziare

È necessario creare e salvare i modelli cloud in una struttura specifica affinché vengano rilevati da GitLab o GitHub.

- Configurare e archiviare correttamente i modelli cloud da integrare con GitLab. Solo i modelli validi vengono importati in GitLab.
 - Creare una o più cartelle designate per i modelli cloud.
 - Tutti i modelli cloud devono essere archiviati in file `blueprint.yaml`.
 - Assicurarsi che la parte superiore dei modelli includa le proprietà `name:` e `version:`.
- Estrarre una chiave API per il repository applicabile. Nell'account Git, selezionare l'accesso nell'angolo superiore destro e passare al menu Impostazioni. Selezionare **Token di accesso**, quindi assegnare un nome al token e impostare una data di scadenza. Quindi, selezionare l'API e creare il token. Copiare il valore risultante e salvarlo.

Per tutti i modelli cloud utilizzati con l'integrazione di Git, è necessario attenersi alle seguenti linee guida.

- Ogni modello cloud deve risiedere in una cartella separata.
- Tutti i modelli cloud devono essere denominati `blueprint.yaml`.
- Tutti i file YAML del modello cloud devono utilizzare i campi `name` e `version`.
- Vengono importati solo i modelli cloud validi.
- Se si aggiorna la bozza di un modello cloud importata da Git e il suo contenuto è diverso da quello della versione superiore, la bozza non verrà aggiornata nelle sincronizzazioni successive e verrà creata una nuova versione. Se si desidera aggiornare un modello e consentire anche ulteriori sincronizzazioni da Git, è necessario creare una nuova versione dopo le modifiche finali.
- [Configurazione dell'integrazione dei modelli cloud GitLab in Cloud Assembly](#)
Questa procedura illustra come configurare l'integrazione di GitLab in Cloud Assembly in modo da poter utilizzare i modelli cloud nel repository e scaricare automaticamente i modelli salvati associati ai progetti designati. Per utilizzare i modelli cloud con GitLab, è necessario creare una connessione a un'istanza di GitLab appropriata, quindi salvare i modelli desiderati in tale istanza.
- [Configurazione dell'integrazione di GitHub in Cloud Assembly](#)
È possibile integrare il servizio di hosting del repository basato su cloud di GitHub in Cloud Assembly
- [Configurazione dell'integrazione di Bitbucket in Cloud Assembly](#)
Cloud Assembly supporta l'integrazione con Bitbucket per l'utilizzo come repository basato su Git per gli script di azione ABX e VMware Cloud Templates.

Configurazione dell'integrazione dei modelli cloud GitLab in Cloud Assembly

Questa procedura illustra come configurare l'integrazione di GitLab in Cloud Assembly in modo da poter utilizzare i modelli cloud nel repository e scaricare automaticamente i modelli salvati associati ai progetti designati. Per utilizzare i modelli cloud con GitLab, è necessario creare una connessione a un'istanza di GitLab appropriata, quindi salvare i modelli desiderati in tale istanza.

Quando l'integrazione di GitLab è configurata con un repository esistente, tutti i modelli cloud associati ai progetti selezionati diventano disponibili per gli utenti qualificati. È possibile utilizzare questi modelli con una distribuzione esistente o come base di una nuova distribuzione. Quando si aggiunge un progetto, è necessario selezionare alcune proprietà relative a posizione e modalità di archiviazione in GitLab.

Nota Non è possibile inserire modelli cloud nuovi o aggiornati nel repository Git da Cloud Assembly. Inoltre, non è possibile inserire nuovi modelli nel repository da Cloud Assembly. Per aggiungere modelli cloud a un repository, gli sviluppatori devono utilizzare l'interfaccia Git.

Se si aggiorna la bozza di un modello cloud importata da Git e il suo contenuto è diverso da quello della versione superiore, la bozza non verrà aggiornata nelle sincronizzazioni successive e verrà creata una nuova versione. Se si desidera aggiornare un modello cloud e consentire anche ulteriori sincronizzazioni da Git, è necessario creare una nuova versione dopo le modifiche finali.

Dopo aver configurato i modelli cloud per l'uso con GitLab e aver raccolto le informazioni richieste, è necessario configurare l'integrazione con l'istanza di GitLab. È quindi possibile importare i modelli cloud designati in GitLab. Una dimostrazione video di questa procedura è disponibile presso <https://www.youtube.com/watch?v=h0vqo63Sdgg>.

Prerequisiti

- Estrarre una chiave API per il repository applicabile. Nell'account GitLab, selezionare l'accesso nell'angolo superiore destro e passare al menu Impostazioni. Selezionare Token di accesso, quindi assegnare un nome al token e impostare una data di scadenza. Quindi, selezionare l'API e creare il token. Copiare il valore risultante e salvarlo.

È necessario disporre di un repository Git locale appropriato configurato con l'accesso per tutti gli utenti designati per configurare l'integrazione di Git con Cloud Assembly. È inoltre necessario creare e salvare i modelli cloud in una struttura specifica affinché vengano rilevati da GitLab.

- Configurare e archiviare correttamente i modelli cloud da integrare con GitLab. Solo i modelli validi vengono importati in GitLab. Vedere [Come utilizzare l'integrazione di Git in Cloud Assembly](#).

Procedura

- 1 Configurare l'integrazione con l'ambiente GitLab in Cloud Assembly.
 - a Selezionare **Infrastruttura > Integrazioni > Aggiungi nuovo** e scegliere GitLab.
 - b Immettere l'**URL** dell'istanza di GitLab. Per un'istanza SaaS di GitLab, nella maggior parte dei casi sarà gitlab.com.

- c Immettere il **Token**, noto anche come chiave API, per l'istanza di GitLab specificata. Per informazioni sull'estrazione del token dall'istanza di GitLab, vedere i prerequisiti precedenti.
 - d Aggiungere un nome e una descrizione appropriati.
 - e Fare clic su **Convalida** per verificare la connessione.
 - f Aggiungere i tag di funzionalità, se lo si desidera. Vedere [Utilizzo di tag di funzionalità in Cloud Assembly](#) per ulteriori informazioni.
 - g Fare clic su **Aggiungi**.
- 2** Configurare la connessione di GitLab in modo che accetti i modelli cloud in un repository appropriato.
- a Selezionare **Infrastruttura > Integrazioni** e scegliere l'integrazione di GitLab appropriata.
 - b Selezionare **Progetti**.
 - c Selezionare **Nuovo progetto** e creare un nome per il progetto.
 - d Immettere il percorso del **Repository** all'interno di GitLab. In genere, è il nome utente dell'account principale aggiunto al nome del repository.
 - e Immettere il **Ramo** di GitLab appropriato che si desidera utilizzare.
 - f Se applicabile, immettere il nome della **Cartella**. Se lasciato vuoto, tutte le cartelle saranno disponibili.
 - g Immettere un **Tipo** appropriato. Se applicabile, immettere il nome della cartella. Se lasciato vuoto, tutte le cartelle saranno disponibili.
 - h Fare clic su **Avanti** per completare l'aggiunta del repository.

Quando si fa clic su **Avanti**, viene avviata un'attività di sincronizzazione automatica che consente di importare i modelli cloud nella piattaforma.

Quando le attività di sincronizzazione vengono completate, un messaggio indica che i modelli cloud sono stati importati.

Risultati

È ora possibile recuperare i modelli cloud da GitLab.

Configurazione dell'integrazione di GitHub in Cloud Assembly

È possibile integrare il servizio di hosting del repository basato su cloud di GitHub in Cloud Assembly

Per configurare l'integrazione di GitHub in Cloud Assembly, è necessario un token GitHub valido. Per informazioni sulla creazione e l'individuazione del token, consultare la documentazione di GitHub.

Prerequisiti

- È necessario poter accedere a GitHub.
- Configurare e archiviare correttamente i modelli cloud da integrare con GitHub. Solo i modelli cloud validi vengono importati in GitHub. Vedere [Come utilizzare l'integrazione di Git in Cloud Assembly](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare GitHub.
- 3 Immettere le informazioni richieste nella pagina di configurazione di GitHub.
- 4 Fare clic su **Convalida** per verificare l'integrazione.
- 5 Se è necessario aggiungere tag per supportare una strategia di assegnazione dei tag, immettere tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).
- 6 Fare clic su **Aggiungi**.
- 7 Configurare la connessione di GitHub in modo che accetti i modelli cloud in un repository appropriato.
 - a Selezionare **Infrastruttura > Integrazioni** e scegliere l'integrazione di GitHub appropriata.
 - b Selezionare **Progetti**.
 - c Selezionare **Nuovo progetto** e creare un nome per il progetto.
 - d Immettere il percorso del **Repository** all'interno di GitHub. In genere, è il nome utente dell'account principale aggiunto al nome del repository.
 - e Immettere il **Ramo** di GitHub appropriato che si desidera utilizzare.
 - f Se applicabile, immettere il nome della **Cartella**. Se lasciato vuoto, tutte le cartelle saranno disponibili.
 - g Immettere un **Tipo** appropriato.
 - h Fare clic su **Avanti** per completare l'aggiunta del repository.

Viene avviata un'attività di sincronizzazione automatizzata che importa i modelli cloud nella piattaforma.

Quando le attività di sincronizzazione vengono completate, un messaggio indica che i modelli cloud sono stati importati.

Risultati

GitHub è disponibile per l'uso nei blueprint di Cloud Assembly.

Operazioni successive

È ora possibile recuperare i modelli cloud da GitHub.

Configurazione dell'integrazione di Bitbucket in Cloud Assembly

Cloud Assembly supporta l'integrazione con Bitbucket per l'utilizzo come repository basato su Git per gli script di azione ABX e VMware Cloud Templates.

In Cloud Assembly, è possibile utilizzare due tipi di elementi del repository tramite l'integrazione di Bitbucket, ovvero VMware Cloud Templates e gli script di azione ABX. Prima di usare un'integrazione di Bitbucket, è necessario sincronizzare i progetti che si desidera utilizzare. Le azioni ABX supportano il writeback nel repository Bitbucket, ma non è possibile effettuare il writeback dei modelli cloud dall'integrazione. Se si desidera creare nuove versioni dei file dei modelli cloud, è necessario farlo manualmente.

Prerequisiti

- Configurare una distribuzione Bitbucket Server locale con uno o più progetti ABX o basati su modelli cloud DA utilizzare con le distribuzioni. Bitbucket Cloud non è attualmente supportato.
- Creare o designare un progetto Cloud Assembly per associare l'integrazione di Bitbucket.
- I file dei modelli cloud da sincronizzare con un'integrazione di Bitbucket devono essere denominati `blueprint.yaml`.

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare Bitbucket.
- 3 Immettere le informazioni di riepilogo e le credenziali di Bitbucket nella pagina di riepilogo della nuova integrazione di Bitbucket.
- 4 Per verificare l'integrazione, fare clic su **Convalida**.
- 5 Se si aggiungono tag a supporto di una strategia di assegnazione dei tag, immettere tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).
- 6 Fare clic su **Aggiungi**.
- 7 Selezionare la scheda Progetti nella pagina principale relativa all'integrazione di Bitbucket per associare un progetto all'integrazione di Bitbucket.
- 8 Selezionare il progetto da associare a questa integrazione di Bitbucket.
- 9 Fare clic su **Avanti** per aggiungere un repository al progetto Bitbucket e indicare il tipo di repository che si sta aggiungendo, quindi specificare il nome del **Repository**, il **Ramo** e la **Cartella**.
- 10 Fare clic su **Aggiungi**.

Se si desidera aggiungere uno o più repository a un progetto, fare clic su **Aggiungi repository**.

Risultati

L'integrazione di Bitbucket viene configurata con la configurazione del repository specificato ed è possibile visualizzare e utilizzare le azioni ABX e i modelli cloud contenuti nei repository configurati. Quando si aggiunge un progetto a un'integrazione di Bitbucket, viene eseguita un'operazione di sincronizzazione per ottenere le versioni più recenti degli script di azione ABX e dei file dei modelli cloud del repository designato. La scheda Cronologia della pagina dell'integrazione di Bitbucket mostra i record di tutte le operazioni di sincronizzazione relative all'integrazione. Per impostazione predefinita, i file vengono sincronizzati automaticamente ogni 15 minuti, ma è possibile sincronizzare manualmente un file in qualsiasi momento selezionandolo e facendo clic su **SINCRONIZZA**.

Operazioni successive

È possibile utilizzare le azioni ABX nella pagina Estendibilità di Cloud Assembly e utilizzare i modelli cloud nella pagina Progettazione. Se si salva una versione modificata di un'azione ABX nell'area Estendibilità di Cloud Assembly, la nuova versione dello script viene creata e riscritta nel repository.

Come configurare un'integrazione IPAM esterna in vRealize Automation

È possibile creare un punto di integrazione IPAM esterno specifico del provider per gestire gli indirizzi IP utilizzati nelle distribuzioni dei modelli cloud. Quando si utilizza un punto di integrazione IPAM esterno, gli indirizzi IP vengono ottenuti e gestiti dal provider IPAM designato anziché da vRealize Automation.

È possibile creare un punto di integrazione IPAM specifico del provider per gestire gli indirizzi IP e le impostazioni DNS per le distribuzioni dei modelli cloud e le macchine virtuali in vRealize Automation.

Per informazioni su come configurare i prerequisiti e consultare un esempio su come creare un punto di integrazione IPAM esterno specifico del provider nel contesto di un workflow di esempio, vedere [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#). Si noti che questo workflow è per un'integrazione Infoblox IPAM, ma può essere utilizzato come riferimento per qualsiasi fornitore IPAM esterno.

Per informazioni su come creare le risorse necessarie per consentire a partner e fornitori IPAM esterni di integrare la propria soluzione IPAM con vRealize Automation, vedere [Come utilizzare l'SDK IPAM per creare un pacchetto di integrazione IPAM esterno specifico del provider per vRealize Automation](#).

Prerequisiti

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

- Verificare di disporre di un account con il provider IPAM esterno, ad esempio [Infoblox](#) o [Bluecat](#) e di disporre delle credenziali di accesso corrette per l'account dell'organizzazione con il provider IPAM.
- Verificare di disporre dell'accesso a un pacchetto di integrazione distribuito per il provider IPAM, ad esempio Infoblox o BlueCat. Il pacchetto distribuito viene inizialmente ottenuto come download .zip dal provider IPAM o da [VMware Marketplace](#) e quindi distribuito in vRealize Automation.
- Verificare di disporre dell'accesso a un ambiente in esecuzione configurato per il provider IPAM.
- Se si utilizza un ambiente in esecuzione incorporato locale di estendibilità basata su azioni (ABX), verificare di disporre di un server proxy HTTP nella rete vRealize Automation in grado di far passare il traffico in uscita verso siti esterni, come gcr.io o storage.googleapis.com. Per informazioni dettagliate, vedere [come estrarre immagini Docker dietro il proxy in vRealize Automation 8.x \(75180\)](#).
- Verificare di disporre delle credenziali utente necessarie per accedere e utilizzare il prodotto del fornitore IPAM. Per informazioni sulle autorizzazioni utenti richieste, consultare la documentazione del prodotto del fornitore di integrazione.

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Fare clic su **IPAM**.
- 3 Nel menu a discesa **Provider**, selezionare un pacchetto del provider IPAM configurato nell'elenco.

Se l'elenco è vuoto, fare clic su **Importa pacchetto del provider**, passare a un file ZIP del pacchetto del provider esistente e selezionarlo. Se non si dispone del file .zip, è possibile ottenerlo da [VMware Marketplace](#).

- 4 Immettere il nome utente e la password dell'amministratore per il proprio account con il provider IPAM esterno, insieme a tutti gli altri campi obbligatori (se presenti), ad esempio il nome host del provider.
- 5 Nell'elenco a discesa **Ambiente in esecuzione**, selezionare un ambiente in esecuzione esistente, ad esempio il punto di integrazione locale di estendibilità basata su azioni.

L'ambiente in esecuzione supporta la comunicazione tra vRealize Automation e il provider IPAM.

Il framework IPAM supporta solo un ambiente in esecuzione incorporato locale di estendibilità basata su azioni (ABX).

Nota Se si utilizza un account cloud di Amazon Web Services o Microsoft Azure come ambiente in esecuzione dell'integrazione, assicurarsi che l'appliance del provider IPAM sia accessibile da Internet e non sia protetta da una regola NAT o un firewall e che disponga di un nome DNS risolvibile pubblicamente. Se il provider IPAM non è accessibile, le funzioni di Amazon Web Services Lambda o Microsoft Azure non possono connettersi e l'integrazione non riuscirà.

6 Fare clic su **Convalida**.

7 Quando viene richiesto di considerare attendibile il certificato autofirmato dal provider IPAM esterno, fare clic su **Accetta**.

Dopo aver accettato il certificato autofirmato, l'azione di convalida può continuare fino al completamento.

8 Immettere un nome per questo punto di integrazione IPAM e fare clic su **Aggiungi** per salvare il nuovo punto di integrazione IPAM.

Viene imitata un'azione di raccolta dati. I dati di reti e indirizzi IP vengono raccolti dal provider IPAM esterno.

Come eseguire l'aggiornamento a un pacchetto di integrazione IPAM esterno più recente in vRealize Automation

È possibile aggiornare un punto di integrazione IPAM esterno esistente per sfruttare una versione più recente del pacchetto di integrazione IPAM specifico del fornitore.

Un provider IPAM esterno o VMware possono aggiornare un pacchetto di integrazione IPAM di origine per un fornitore specifico. Ad esempio, il pacchetto di integrazione IPAM esterno per Infoblox è stato aggiornato diverse volte. Per conservare tutte le impostazioni dell'infrastruttura di vRealize Automation esistenti che utilizzano un punto di integrazione IPAM denominato, è possibile modificare un punto di integrazione IPAM per ottenere il pacchetto di integrazione IPAM aggiornato, anziché creare un nuovo punto di integrazione IPAM.

Prerequisiti

Questa procedura presuppone che sia già stato creato un punto di integrazione IPAM esterno e si desideri aggiornare tale punto di integrazione per utilizzare una versione più recente del pacchetto di integrazione IPAM del fornitore.

Per informazioni su come creare un punto di integrazione IPAM esterno, vedere [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#).

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

- Verificare di disporre di un account con il provider IPAM esterno e di disporre delle credenziali di accesso corrette per l'account dell'organizzazione con tale provider IPAM.
- Verificare di poter accedere a un pacchetto di integrazione distribuito per il provider IPAM. Il pacchetto distribuito viene inizialmente ottenuto come download ZIP dal sito Web del provider IPAM o da [VMware Marketplace](#) e quindi distribuito in vRealize Automation.

Per informazioni su come scaricare e distribuire il file ZIP del pacchetto del provider e renderlo disponibile come valore **Provider** nella pagina Integrazione IPAM, vedere [Download e distribuzione di un pacchetto del provider IPAM esterno per l'utilizzo in vRealize Automation](#).

- Verificare di disporre dell'accesso a un ambiente in esecuzione configurato per il provider IPAM. L'ambiente in esecuzione è in genere un punto di integrazione incorporato locale di estendibilità basata su azioni (ABX).

Per informazioni sulle caratteristiche dell'ambiente in esecuzione, vedere [Creazione di un ambiente in esecuzione per un punto di integrazione IPAM in vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni IPAM** e aprire il punto di integrazione IPAM esistente.
- 2 Fare clic su **Gestisci provider**.
- 3 Passare al pacchetto di integrazione IPAM aggiornato e importarlo.
- 4 Fare clic su **Convalida**, quindi fare clic su **Salva**.

Configurazione dell'integrazione di My VMware in Cloud Assembly

È possibile integrare My VMware con Cloud Assembly per supportare le azioni e le capacità relative a VMware associate ai componenti scaricabili che richiedono un account.

È possibile creare una sola integrazione di My VMware per ogni organizzazione.

Prerequisiti

È necessario disporre di un account utente con le autorizzazioni appropriate per My VMware.

- Per informazioni su come invitare un utente a un account My VMware, vedere [KB 2070555](#).
- Per informazioni sull'assegnazione delle autorizzazioni utente in un account My VMware, vedere [KB 2006977](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare My VMware.
- 3 Immettere le informazioni richieste nella pagina di configurazione di My VMware.

- 4 Se sono necessari tag per supportare una strategia di assegnazione dei tag, immettere i tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).
- 5 Fare clic su **Aggiungi**.

Risultati

My VMware è disponibile per l'uso.

Operazioni successive

Accedere ai componenti My VMware in base alle esigenze.

Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly

È possibile configurare una o più integrazioni di vRealize Orchestrator, in modo da poter utilizzare i workflow come parte dell'estendibilità e dei modelli cloud.

vRealize Automation include un'istanza di vRealize Orchestrator incorporata preconfigurata. È possibile accedere al client dell'istanza di vRealize Orchestrator incorporata dalla console di vRealize Automation Cloud Services.

Nota È possibile accedere al Centro di controllo dell'istanza di vRealize Orchestrator incorporata passando a `https://your_vRA_FQDN/VCO-controlcenter` e accedendo come **root**.

È inoltre possibile integrare un'istanza di vRealize Orchestrator esterna da utilizzare nelle sottoscrizioni di estendibilità di vRealize Automation e nelle operazioni XaaS (Anything as a Service) utilizzate per i modelli cloud.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Eseguire l'aggiornamento o la migrazione a vRealize Orchestrator 8.3. Vedere [Aggiornamento e migrazione di VMware vRealize Orchestrator](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni**.
- 2 Fare clic su **Aggiungi integrazione**.
- 3 Selezionare **vRealize Orchestrator**.
- 4 Immettere un nome per l'integrazione di vRealize Orchestrator.
- 5 (Facoltativo) Immettere una descrizione per l'integrazione di vRealize Orchestrator.

- 6 In **URL di vRealize Orchestrator**, immettere il nome di dominio completo dell'istanza di vRealize Orchestrator esterna.

Ad esempio, `https://my_vRO_FQDN.com:443`.

- 7 Per convalidare l'integrazione, fare clic su **Convalida**.
- 8 (Facoltativo) Se richiesto, rivedere le informazioni del certificato e fare clic su **Accetta**.
- 9 (Facoltativo) Aggiungere tag di funzionalità. Per ulteriori informazioni sui tag di funzionalità, vedere [Utilizzo di tag di funzionalità in Cloud Assembly](#).

Nota I tag di funzionalità possono essere utilizzati per gestire più integrazioni di vRealize Orchestrator. Vedere [Gestione di più integrazioni di vRealize Orchestrator con vincoli di progetto](#).

- 10 Fare clic su **Aggiungi**.

L'integrazione di vRealize Orchestrator viene salvata.

- 11 Per verificare che l'integrazione sia configurata e che i workflow siano stati aggiunti, selezionare **Estendibilità > Libreria > Workflow**.

Operazioni successive

Accedere al client di vRealize Orchestrator esterno integrato:

- 1 Passare alla console Cloud Services di vRealize Automation.
- 2 Selezionare **Orchestrator**.
- 3 Selezionare la scheda che corrisponde all'istanza di vRealize Orchestrator integrata.

Nota Gli utenti di Cloud Assembly che non dispongono di credenziali di amministratore del cloud non possono visualizzare la scheda dell'istanza di vRealize Orchestrator integrata.

Disabilitazione o abilitazione delle integrazioni di vRealize Orchestrator

È possibile disabilitare o abilitare manualmente l'integrazione di vRealize Orchestrator in modo da poter eseguire la manutenzione mentre l'integrazione è ancora in esecuzione.

È possibile disabilitare l'integrazione di vRealize Orchestrator per eseguire la manutenzione. Quando disabilitata, l'integrazione di vRealize Orchestrator è ancora in uno stato **ESECUZIONE**, quindi è possibile continuare a eseguire attività come il monitoraggio delle risorse e la raccolta dati.

Nota Oltre alla disabilitazione manuale, il servizio Gateway vRealize Orchestrator esegue controlli periodici dello stato di integrità per verificare se le integrazioni di vRealize Orchestrator sono attive o meno. Tutte le integrazioni di vRealize Orchestrator inattive vengono disabilitate automaticamente e vengono impostate sullo stato **DISCONNESSO**. Non sarà possibile eseguire attività come la raccolta dati o il monitoraggio delle risorse su integrazioni disconnesse.

Dopo aver disabilitato un'integrazione di vRealize Orchestrator o aver eseguito la disconnessione dell'integrazione dal controllo dello stato di integrità, i workflow verranno eseguiti solo sulle integrazioni abilitate. Se l'ambiente include più integrazioni di vRealize Orchestrator abilitate che non sono gestite tramite vincoli di progetto o tag di funzionalità, viene selezionata un'integrazione di vRealize Orchestrator casuale per eseguire il workflow.

Nota Poiché l'integrazione di vRealize Orchestrator viene selezionata in modo casuale, è necessario assicurarsi che le informazioni necessarie per eseguire una determinata operazione siano disponibili in tutte le integrazioni. Per le entità dei contenuti come i workflow, significa che devono essere sincronizzate in tutte le integrazioni. Per gli oggetti dell'inventario non è possibile garantire che abbiano lo stesso identificatore di oggetto in tutte le integrazioni. Il tentativo di eseguire un workflow che include un oggetto di inventario come parametro di input potrebbe non riuscire.

Per informazioni sulla gestione di più integrazioni di vRealize Orchestrator con vincoli di progetto e tag di funzionalità, vedere [Gestione di più integrazioni di vRealize Orchestrator con vincoli di progetto](#) e [Gestione di più integrazioni di vRealize Orchestrator con tag di funzionalità dell'account cloud](#).

Prerequisiti

Configurare una o più integrazioni di vRealize Orchestrator in Cloud Assembly. Vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).

Procedura

- 1 Disabilitare l'integrazione vRealize Orchestrator.
 - a Andare in **Infrastruttura > Connessioni > Integrazioni**.
 - b Selezionare l'integrazione di vRealize Orchestrator da disabilitare.
 - c In **Credenziali del server di vRealize Orchestrator**, disattivare l'opzione **Abilita endpoint**.
 - d Fare clic su **Convalida**.
 - e Dopo la corretta convalida, fare clic su **Salva**.
- 2 Eseguire le attività di manutenzione necessarie sull'integrazione vRealize Orchestrator disabilitata.
- 3 Abilitare l'interazione di vRealize Orchestrator.
 - a Andare in **Infrastruttura > Connessioni > Integrazioni**.
 - b Selezionare l'integrazione di vRealize Orchestrator disabilitata in precedenza.
 - c In **Credenziali server di vRealize Orchestrator**, attivare l'opzione **Abilita endpoint**.
 - d Fare clic su **Convalida**.
 - e Dopo la corretta convalida, fare clic su **Salva**.

Gestione di più integrazioni di vRealize Orchestrator con vincoli di progetto

È possibile utilizzare i vincoli di progetto per gestire le integrazioni di vRealize Orchestrator utilizzate nelle sottoscrizioni ai workflow.

Cloud Assembly supporta l'integrazione di più server di vRealize Orchestrator che possono essere utilizzati nelle sottoscrizioni ai workflow. È possibile gestire quali integrazioni di vRealize Orchestrator sono utilizzate nei modelli cloud di cui è stato eseguito il provisioning dal progetto con vincoli di progetto temporanei e permanenti. Per ulteriori informazioni sui vincoli di progetto, vedere [Utilizzo dei tag di progetto e delle proprietà personalizzate di Cloud Assembly](#).

Prerequisiti

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Configurare due o più integrazioni di vRealize Orchestrator in Cloud Assembly. Vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).
- Aggiungere i tag di funzionalità alle integrazioni di vRealize Orchestrator. Vedere [Utilizzo di tag di funzionalità in Cloud Assembly](#).

Procedura

- 1 Passare a **Infrastruttura > Amministrazione > Progetti** e selezionare il progetto.
- 2 Selezionare la scheda **Provisioning**.
- 3 Immettere i tag di funzionalità delle integrazioni di vRealize Orchestrator nella casella di testo **Vincoli di estendibilità** e impostarlo come vincoli di progetto soft o hard.
- 4 Fare clic su **Salva**.

Risultati

Quando si distribuisce un modello cloud, Cloud Assembly utilizza i vincoli di progetto per gestire quali integrazioni di vRealize Orchestrator sono utilizzate nelle sottoscrizioni ai workflow.

Operazioni successive

In alternativa, è possibile utilizzare i tag di funzionalità per gestire più integrazioni di vRealize Orchestrator in un livello di account cloud. Per ulteriori informazioni, vedere [Gestione di più integrazioni di vRealize Orchestrator con tag di funzionalità dell'account cloud](#).

Gestione di più integrazioni di vRealize Orchestrator con tag di funzionalità dell'account cloud

È possibile utilizzare i tag di funzionalità per gestire le integrazioni di vRealize Orchestrator utilizzate nelle sottoscrizioni ai workflow.

Cloud Assembly supporta l'integrazione di più server di vRealize Orchestrator che possono essere utilizzati nelle sottoscrizioni ai workflow. È possibile gestire le integrazioni di vRealize Orchestrator utilizzate nelle sottoscrizioni ai workflow aggiungendo tag di funzionalità all'account cloud personale.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Configurare due o più integrazioni di vRealize Orchestrator in Cloud Assembly. Per ulteriori informazioni, vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).
- Aggiungere i tag di funzionalità alle integrazioni di vRealize Orchestrator. Vedere [Utilizzo di tag di funzionalità in Cloud Assembly](#).

Procedura

- 1 Passare a **Infrastruttura > Connessioni > Account cloud**.
- 2 Selezionare l'account cloud personale.
- 3 Immettere i tag di funzionalità delle integrazioni di vRealize Orchestrator che si desidera utilizzare.

I tag di funzionalità vengono convertiti automaticamente in vincoli soft. Per utilizzare vincoli hard nella gestione delle integrazioni, è necessario utilizzare i vincoli di progetto. Per ulteriori informazioni, vedere [Gestione di più integrazioni di vRealize Orchestrator con vincoli di progetto](#).

- 4 Fare clic su **Salva**.

Risultati

Quando si distribuisce un modello cloud, Cloud Assembly utilizza l'assegnazione tag nell'account cloud associato per gestire quali integrazioni di vRealize Orchestrator sono utilizzate nelle sottoscrizioni ai workflow.

Raccolta dati per le integrazioni di vRealize Orchestrator

vRealize Automation esegue la raccolta dati periodica per le integrazioni di vRealize Orchestrator.

Gli eventi di raccolta dati per le integrazioni di vRealize Orchestrator vengono attivati ogni 10 minuti. La raccolta dati raccoglie i dati relativi ai workflow inclusi nella libreria di ciascuna integrazione di vRealize Orchestrator.

Importante Verificare di aver eseguito la versione di un workflow al termine della modifica. Le modifiche ai workflow senza aver eseguito la versione non vengono raccolte dall'agente di raccolta dati.

È possibile trovare informazioni sull'ultima raccolta dati eseguita in un'integrazione di vRealize Orchestrator passando a **Infrastruttura > Connessioni > Integrazioni** e selezionando l'integrazione specifica. È inoltre possibile attivare un evento di raccolta dati manuale facendo clic su **Avvia raccolta dati**.

Per ulteriori informazioni sulla raccolta dati di vRealize Automation, vedere [Come funziona la raccolta dati in vRealize Automation](#).

Come si utilizza Kubernetes in Cloud Assembly

Cloud Assembly offre diverse opzioni per la configurazione, la gestione e la distribuzione dei carichi di lavoro virtuali Kubernetes.

Sono disponibili due opzioni per utilizzare le risorse Tanzu Kubernetes in Cloud Assembly. È possibile creare una configurazione di vSphere with Tanzu Kubernetes, che richiede solo un account cloud vCenter adatto e un piano cluster per accedere alle funzionalità di vSphere Tanzu Kubernetes native. Con questa opzione, è possibile utilizzare al meglio un account cloud vCenter per accedere agli spazi dei nomi del supervisore per distribuire i carichi di lavoro vSphere basati su Kubernetes. È inoltre possibile integrare le risorse Kubernetes esterne in Cloud Assembly.

In alternativa, è possibile integrare VMware Tanzu Kubernetes Grid Integrated Edition (TKGI), in precedenza denominato PKS. Questo tipo di implementazione Kubernetes richiede un'integrazione PKS in Cloud Assembly. Non richiede un piano del cluster di Cloud Assembly.

Infine, è inoltre possibile creare un'integrazione di Red Hat OpenShift con Cloud Assembly per configurare, gestire e distribuire le risorse Kubernetes.

Utilizzo dei cluster di vSphere with Tanzu Kubernetes

La versione vSphere 7.x contiene miglioramenti significativi che consentono di utilizzare Kubernetes in modo nativo per gestire sia le macchine virtuali che i container da un'unica interfaccia. Cloud Assembly consente agli utenti di utilizzare al meglio le funzionalità di vSphere with Tanzu Kubernetes incorporate in vSphere. È possibile accedere alla funzionalità di vSphere with Tanzu Kubernetes tramite un account cloud vCenter con un'implementazione di vSphere che contenga cluster supervisore. Questa implementazione consente di gestire le macchine virtuali convenzionali e i cluster Kubernetes da vCenter.

Per gli spazi dei nomi supervisore di Tanzu Kubernetes, gli utenti devono poter accedere a un SSO di vSphere applicabile in modo che possano accedere al collegamento fornito ai dettagli dello spazio dei nomi supervisore. Quindi, possono scaricare un Kubectl personalizzato con l'autenticazione di vSphere affinché possano utilizzare lo spazio dei nomi supervisore.

Per utilizzare questa funzionalità, è necessario disporre di un vCenter con un account cloud di vSphere configurato con spazi dei nomi supervisore. Dopo aver eseguito l'accesso, è possibile iniziare a utilizzare gli spazi dei nomi applicabili.

Utilizzo delle integrazioni di VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) oppure OpenShift

Per TKGI, i cluster esterni o le configurazioni OpenShift, Cloud Assembly fornisce l'accesso a un Kubeconfig che consente agli utenti di accedere ai cluster Kubernetes applicabili.

Dopo aver creato un'integrazione con TKGI oppure OpenShift, i cluster Kubernetes applicabili diventano disponibili in Cloud Assembly ed è possibile creare e aggiungere componenti Kubernetes a Cloud Assembly per supportare la gestione delle applicazioni cluster e contenitori. Queste applicazioni costituiscono la base delle distribuzioni self-service disponibili nel catalogo di Service Broker.

- [Configurazione dell'integrazione di VMware Tanzu Kubernetes Grid Integrated Edition in Cloud Assembly](#)

È possibile configurare una connessione di risorse VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) (denominato in precedenza PKS) in locale o nel cloud per supportare le funzionalità di gestione e integrazione di Kubernetes in Cloud Assembly.

- [Provisioning di una distribuzione di vSphere with Tanzu Kubernetes in vRealize Automation](#)

vRealize Automation consente di eseguire il provisioning di una distribuzione di vSphere with Tanzu Kubernetes da Cloud Assembly per utilizzare al meglio le funzionalità native di vSphere 7.x per distribuire e gestire i cluster Tanzu Kubernetes, fornendo un livello indipendente dall'infrastruttura per il provisioning e la gestione dell'infrastruttura virtuale.

- [Configurazione dell'integrazione di Red Hat OpenShift in Cloud Assembly](#)

È possibile configurare una connessione di risorse Red Hat OpenShift in locale e nel cloud per supportare le funzionalità di gestione e integrazione di Kubernetes a livello aziendale in Cloud Assembly.

- [Configurazione di una zona Kubernetes in Cloud Assembly](#)

Le zone Kubernetes consentono agli amministratori del cloud di definire il posizionamento basato su criteri di cluster e spazi dei nomi Kubernetes e gli spazi dei nomi supervisore utilizzati nelle distribuzioni di Cloud Assembly. Un amministratore può utilizzare questa pagina per specificare quali cluster sono disponibili per il provisioning degli spazi dei nomi Kubernetes e quali proprietà sono accettabili per i cluster.

- [Creazione di un piano cluster in vRealize Automation Cloud Assembly per l'utilizzo con una distribuzione di vSphere with Tanzu Kubernetes](#)

È necessario creare un piano cluster da utilizzare con le distribuzioni di vSphere with Tanzu Kubernetes in vRealize Automation. Un piano cluster funge da modello di configurazione per il provisioning delle istanze del cluster Tanzu Kubernetes in una determinata istanza dell'account cloud vSphere.

- [Utilizzo dei cluster e degli spazi dei nomi supervisore di Tanzu in Cloud Assembly](#)

Gli amministratori possono rendere gli spazi dei nomi supervisore in un'integrazione di vSphere abilitata per Tanzu disponibili per gli utenti in modo che possano aggiungere tali spazi dei nomi nelle distribuzioni Kubernetes tramite modelli cloud o richiederli dal catalogo di Service Broker.

- [Utilizzo di spazi dei nomi e cluster Kubernetes in Cloud Assembly](#)

Gli amministratori del cloud possono aggiungere, visualizzare e gestire la configurazione degli spazi dei nomi e dei cluster Kubernetes distribuiti, sia generici che basati su Pacific, in Cloud Assembly.

- [Aggiunta dei componenti Kubernetes ai modelli cloud in Cloud Assembly](#)

Quando si aggiungono componenti Kubernetes a un modello cloud di Cloud Assembly, è possibile scegliere di aggiungere cluster o consentire agli utenti di creare spazi dei nomi in varie configurazioni. Questa scelta dipende in genere dalle esigenze di controllo degli accessi, da come sono stati configurati i componenti Kubernetes e dalle esigenze di distribuzione.

- [Utilizzo dell'estendibilità di Cloud Assembly con Kubernetes](#)

Cloud Assembly fornisce una serie di argomenti degli eventi che corrispondono alle azioni tipiche correlate alla distribuzione dello spazio dei nomi e del cluster Kubernetes. Gli utenti possono iscriversi a questi argomenti in base alle esigenze e questi verranno eseguiti nel momento appropriato. Gli utenti riceveranno la notifica al verificarsi dell'evento correlato all'argomento sottoscritto. È inoltre possibile configurare workflow vRO da eseguire in base alle notifiche degli eventi.

Configurazione dell'integrazione di VMware Tanzu Kubernetes Grid Integrated Edition in Cloud Assembly

È possibile configurare una connessione di risorse VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) (denominato in precedenza PKS) in locale o nel cloud per supportare le funzionalità di gestione e integrazione di Kubernetes in Cloud Assembly.

Le integrazioni di TKGI consentono di gestire le istanze di TKGI in locale e nel cloud e i cluster Kubernetes sottoposti a provisioning in cluster esterni e TKGI. È necessario creare un profilo Kubernetes e associarlo a un progetto per supportare il posizionamento delle risorse basato su criteri.

Prerequisiti

- È necessario disporre di un server TKGI configurato in modo appropriato con autenticazione UAA.
- Verificare di disporre delle credenziali di amministratore del cloud. Per ulteriori informazioni, vedere [Che cosa sono i ruoli utente di vRealize Automation](#).

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare VMware Tanzu Kubernetes Grid Integrated Edition.
- 3 Immettere l'indirizzo IP o il nome di dominio completo e l'indirizzo di TKGI per l'account cloud TKGI che si sta creando.
 - L'indirizzo IP è il nome di dominio completo o l'indirizzo IP del server di autenticazione utente di TKGI.

- L'indirizzo di TKGI è il nome di dominio completo o l'indirizzo IP del server di TKGI principale.
- 4 Selezionare se questo server TKGI è in locale oppure si trova nel cloud pubblico o in un cloud privato.
 - 5 Immettere **Nome utente** e **Password** appropriati per il server di TKGI e altre informazioni correlate.
 - 6 Se si utilizzano tag per supportare una strategia di assegnazione dei tag, immettere i tag di funzionalità. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).
 - 7 Fare clic su **Aggiungi**.

Risultati

È possibile creare zone Kubernetes e assegnarle a un progetto oppure individuare i cluster Kubernetes esterni e assegnare tali cluster ai progetti. È inoltre possibile aggiungere o creare spazi dei nomi Kubernetes che facilitano la gestione dei cluster tra gruppi e organizzazioni di grandi dimensioni.

Operazioni successive

Creare o selezionare le zone Kubernetes appropriate, quindi selezionare uno o più cluster o spazi dei nomi e assegnarli a un progetto. In seguito, è possibile creare e pubblicare modelli cloud per consentire agli utenti di generare distribuzioni self-service che utilizzano Kubernetes.

Provisioning di una distribuzione di vSphere with Tanzu Kubernetes in vRealize Automation

vRealize Automation consente di eseguire il provisioning di una distribuzione di vSphere with Tanzu Kubernetes da Cloud Assembly per utilizzare al meglio le funzionalità native di vSphere 7.x per distribuire e gestire i cluster Tanzu Kubernetes, fornendo un livello indipendente dall'infrastruttura per il provisioning e la gestione dell'infrastruttura virtuale.

La funzionalità di vSphere with Tanzu Kubernetes sfrutta la funzionalità Kubernetes nativa di vSphere 7.x. Per funzionare, non richiede un'integrazione di vRealize Automation PKS.

Prerequisiti

- Per eseguire il provisioning di una distribuzione di vSphere with Tanzu Kubernetes con Cloud Assembly, è necessario disporre dell'accesso a vSphere 7.x. In vRealize Automation, vSphere è disponibile come parte di un account cloud vCenter di Cloud Assembly. Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).
- Tanzu deve essere abilitato nell'account cloud vSphere e deve contenere spazi dei nomi supervisore appropriati.
- È necessario disporre di un piano cluster appropriato da utilizzare con l'integrazione. Vedere [Creazione di un piano cluster in vRealize Automation Cloud Assembly per l'utilizzo con una distribuzione di vSphere with Tanzu Kubernetes](#).

Procedura

- 1 Se in Cloud Assembly non esiste già un account cloud vCenter idoneo, crearne uno.
Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).
- 2 Selezionare **Infrastruttura > Configura > Zona Kubernetes** per creare o selezionare una zona Kubernetes in vRealize Automation Cloud Assembly.

È possibile utilizzare una zona Kubernetes esistente se ne è già stata configurata una appropriata, ma un amministratore deve aggiungere uno o più spazi dei nomi supervisore alla zona. Questi spazi dei nomi fungono da risorse di elaborazione in cui vengono creati i cluster Tanzu Kubernetes sottoposti a provisioning all'interno della zona. Per ulteriori informazioni sulle zone Kubernetes, vedere [Configurazione di una zona Kubernetes in Cloud Assembly](#).
- 3 Passare alla scheda Provisioning Kubernetes nella pagina **Infrastruttura > Amministrazione > Progetti** in Cloud Assembly e associare la zona Kubernetes al progetto appropriato.
- 4 Creare o selezionare un piano cluster per un account cloud vSphere 7.x appropriato.

Vedere [Creazione di un piano cluster in vRealize Automation Cloud Assembly per l'utilizzo con una distribuzione di vSphere with Tanzu Kubernetes](#) per ulteriori informazioni.
- 5 Selezionare **Progettazione > Modelli cloud** e creare un modello cloud per un progetto che abbia accesso a una zona Kubernetes appropriata. Trascinare quindi un componente cluster K8S nello schema del modello cloud e specificarne il nome e il piano cluster.

È possibile specificare anche il numero di nodi worker.
- 6 Eseguire il modello cloud. Al termine, individuare l'indirizzo del cluster Tanzu sottoposto a provisioning nella distribuzione nelle proprietà delle risorse della pagina Distribuzioni di Cloud Assembly.
- 7 Individuare ed esplorare il cluster Tanzu nella pagina **Infrastruttura > Configura > Kubernetes** di Cloud Assembly.

Risultati

Viene eseguito il provisioning del cluster Tanzu Kubernetes come specificato nel modello cloud.

Operazioni successive

Dopo aver distribuito il cluster Tanzu, sono disponibili diverse opzioni per utilizzarlo.

- Passare alla pagina **Risorse > Distribuzioni** in Cloud Assembly, quindi individuare e scaricare il file Kubeconfig correlato per accedere al cluster Tanzu sottoposto a provisioning. È possibile utilizzare il file Kubeconfig per gestire il cluster Tanzu Kubernetes distribuito come qualsiasi altro cluster Kubernetes conforme.
- È possibile individuare ed esplorare il cluster Tanzu nella pagina **Infrastruttura > Risorse > Kubernetes** di Cloud Assembly.

- Per creare un nuovo spazio dei nomi, passare alla scheda Spazi dei nomi nella pagina **Infrastruttura > Risorse > Kubernetes** di Cloud Assembly e fare clic su **Nuovo spazio dei nomi** per creare uno spazio dei nomi nel cluster Tanzu applicabile. È possibile controllare se lo spazio dei nomi è stato creato verificando che sia elencato nella scheda Spazi dei nomi della pagina Kubernetes.

Configurazione dell'integrazione di Red Hat OpenShift in Cloud Assembly

È possibile configurare una connessione di risorse Red Hat OpenShift in locale e nel cloud per supportare le funzionalità di gestione e integrazione di Kubernetes a livello aziendale in Cloud Assembly.

Cloud Assembly supporta l'integrazione con OpenShift versioni 3.x.

Prerequisiti

- È necessario disporre di un'implementazione di Red Hat OpenShift configurata in modo appropriato.
- Verificare di disporre delle credenziali di amministratore del cloud. Per ulteriori informazioni, vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- VMware fornisce risorse che è possibile utilizzare per creare un cluster OpenShift con un modello cloud nella seguente posizione: <https://flings.vmware.com/enterprise-openshift-as-a-service-on-cloud-automation-services>. È possibile utilizzare i cluster creati con queste risorse come cluster globali nelle zone Kubernetes per creare spazi dei nomi self-service.

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare Red Hat OpenShift.
- 3 Immettere **Indirizzo** e **Posizione** per il server OpenShift.
- 4 Selezionare il tipo appropriato in **Tipo di credenziali** e immettere le credenziali di appropriate. L'integrazione di OpenShift supporta il nome utente/password OAuth, la chiave pubblica o l'autenticazione con il token di connessione.
- 5 Immettere **Nome** e **Descrizione** appropriati per l'integrazione di OpenShift.
- 6 Se si utilizzano tag per supportare una strategia di assegnazione dei tag, immettere i tag di funzionalità appropriati. Vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#) e [Creazione di una strategia di assegnazione dei tag](#).
- 7 Fare clic su **Aggiungi**.

Risultati

Quando viene creata un'integrazione, i nuovi cluster Kubernetes vengono visualizzati nella sezione pertinente della pagina Kubernetes. È possibile creare zone Kubernetes e assegnarle a un progetto. È inoltre possibile configurare spazi dei nomi Kubernetes che facilitano la gestione dei cluster tra gruppi e organizzazioni di grandi dimensioni.

Operazioni successive

Creare o selezionare le zone Kubernetes appropriate, quindi selezionare uno o più cluster o spazi dei nomi e assegnarli a un progetto. In seguito, è possibile creare e pubblicare modelli cloud per consentire agli utenti di generare distribuzioni self-service che utilizzano Kubernetes.

Configurazione di una zona Kubernetes in Cloud Assembly

Le zone Kubernetes consentono agli amministratori del cloud di definire il posizionamento basato su criteri di cluster e spazi dei nomi Kubernetes e gli spazi dei nomi supervisore utilizzati nelle distribuzioni di Cloud Assembly. Un amministratore può utilizzare questa pagina per specificare quali cluster sono disponibili per il provisioning degli spazi dei nomi Kubernetes e quali proprietà sono accettabili per i cluster.

Gli amministratori del cloud possono associare le zone Kubernetes agli account cloud TKGI configurati per Cloud Assembly oppure a cluster Kubernetes esterni non associati a un progetto.

Quando si crea una zona Kubernetes, è possibile assegnare più risorse specifiche del provider alla zona e queste risorse indicheranno le proprietà che possono essere impostate per i cluster appena sottoposti a provisioning in termini di numero di worker, master, CPU disponibile, memoria e altre impostazioni di configurazione. Per i provider TKGI, queste corrispondono ai piani TKGI. Un amministratore può anche assegnare più cluster a una zona Kubernetes che verrà utilizzata per il posizionamento degli spazi dei nomi Kubernetes appena sottoposti a provisioning. L'amministratore può assegnare solo i cluster non sottoposti a onboarding o non gestiti da CMX e che sono stati sottoposti a provisioning tramite il provider di cluster preselezionato. L'amministratore può assegnare più zone Kubernetes a un singolo progetto, rendendole quindi tutte disponibili per le operazioni di posizionamento che si verificano all'interno del progetto.

Un amministratore del cloud può assegnare le priorità in più livelli.

- Priorità della zona Kubernetes all'interno di un progetto.
- Priorità della risorsa all'interno di una zona Kubernetes.
- Priorità del cluster all'interno di una zona Kubernetes.

L'amministratore del cloud può anche assegnare tag a più livelli:

- Tag di funzionalità per zona Kubernetes.
- Tag per assegnazione risorsa.
- Tag per assegnazione cluster.

È possibile creare zone Kubernetes con spazi dei nomi supervisore in vSphere nello stesso modo in cui si utilizzano spazi dei nomi Kubernetes generici. Per aggiungere uno spazio dei nomi supervisore a una zona Kubernetes, è necessario associare la zona a un endpoint vSphere 7 che contenga le risorse dello spazio dei nomi Pacific desiderate.

Service Broker contiene una versione della pagina Zona Kubernetes per consentire agli amministratori di Service Broker di accedere alle zone Kubernetes esistenti affinché possano creare criteri di posizionamento per gli spazi dei nomi Kubernetes e i cluster sottoposti a provisioning dal catalogo.

Prerequisiti

Configurare l'integrazione con una distribuzione di VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) appropriata. Vedere [Configurazione dell'integrazione di VMware Tanzu Kubernetes Grid Integrated Edition in Cloud Assembly](#).

Procedura

- 1 Selezionare **Infrastruttura > Configura > Zona Kubernetes** e fare clic su **Nuova zona Kubernetes**.
- 2 Immettere il nome dell'**Account** dell'integrazione TKGI a cui si desidera applicare questa zona.
Definisce l'account cloud o l'endpoint associato alla zona. È possibile assegnare un solo endpoint a ciascuna zona. Se si sta utilizzando lo spazio dei nomi supervisore in vSphere, qui è possibile selezionare solo istanze di vSphere che contengono spazi dei nomi supervisore.
- 3 Aggiungere un **Nome** e una **Descrizione** per la zona Kubernetes.
- 4 Aggiungere i tag di funzionalità, se pertinenti. Vedere [Utilizzo di tag di funzionalità in Cloud Assembly](#) per ulteriori informazioni.
- 5 Fare clic su **Salva**.
- 6 Fare clic sulla scheda Su richiesta e aggiungere i piani TKGI appropriati per la zona da utilizzare per il provisioning del cluster.
È possibile selezionare uno o più piani e assegnare priorità a tali piani. Ai numeri più bassi corrispondono priorità più alte. Le assegnazioni di priorità sono secondarie alla selezione basata su tag.
- 7 Fare clic sulla scheda Cluster e quindi sul pulsante **Aggiungi elaborazione** per aggiungere cluster Kubernetes o supervisore alla zona. Se si utilizza un cluster esterno, viene automaticamente sottoposto a onboarding in Cloud Assembly quando lo si seleziona.
È possibile aggiungere spazi dei nomi Kubernetes al cluster nella pagina Cluster Kubernetes in Cloud Assembly.

Risultati

Le zone Kubernetes sono configurate per l'utilizzo con le distribuzioni di Cloud Assembly.

Operazioni successive

Assegnare la zona Kubernetes a un progetto.

- 1 Scegliere **Infrastruttura > Amministrazione > Progetti** e quindi selezionare il progetto da associare alla zona Kubernetes.
- 2 Fare clic sulla scheda Provisioning Kubernetes nella pagina Progetto.
- 3 Fare clic su **Aggiungi zona Kubernetes** e aggiungere la zona appena creata. Se applicabile, è possibile specificare più zone e impostare la loro priorità.
- 4 Fare clic su **Salva**.

La scheda Provisioning Kubernetes della pagina Progetto di Cloud Assembly consente di impostare limiti al tipo e al numero di spazi dei nomi di cui gli utenti possono eseguire il provisioning in una zona Kubernetes. È inoltre possibile selezionare il tipo di spazi dei nomi di cui è possibile eseguire il provisioning in una zona, ovvero spazi dei nomi regolari o spazi dei nomi supervisore. La tabella Zone Kubernetes nella scheda Provisioning Kubernetes contiene colonne che mostrano le impostazioni dei limiti correnti. Per impostare i limiti, fare clic sulla zona applicabile nella tabella per aprire una finestra di dialogo che consenta di scegliere i limiti dello spazio dei nomi e dello spazio dei nomi supervisore.

Fare clic nella colonna Supporti nella tabella Zone Kubernetes per selezionare il tipo di spazio dei nomi di cui è possibile eseguire il provisioning per la zona.

Dopo aver assegnato una zona Kubernetes a un progetto, è possibile utilizzare la pagina Modelli cloud nella scheda Progettazione di Cloud Assembly per eseguire il provisioning di una distribuzione in base alla zona Kubernetes e alla configurazione del progetto. Nella pagina Modelli cloud sono presenti opzioni per aggiungere un cluster K8S, uno spazio dei nomi K8S e uno spazio dei nomi supervisore. Selezionare l'opzione appropriata per la risorsa Kubernetes che si sta utilizzando.

Creazione di un piano cluster in vRealize Automation Cloud Assembly per l'utilizzo con una distribuzione di vSphere with Tanzu Kubernetes

È necessario creare un piano cluster da utilizzare con le distribuzioni di vSphere with Tanzu Kubernetes in vRealize Automation. Un piano cluster funge da modello di configurazione per il provisioning delle istanze del cluster Tanzu Kubernetes in una determinata istanza dell'account cloud vSphere.

Un piano di cluster definisce una mappatura della configurazione, simile a una mappatura delle caratteristiche, per un set di istanze dell'account cloud di vSphere. In genere, il piano del cluster codifica un set significativo di proprietà di configurazione, ad esempio classi di macchine virtuali, classi di storage e così via, utilizzate durante il provisioning dei cluster Tanzu Kubernetes in un particolare account cloud di vSphere Server.

Si tenga presente che un singolo piano cluster potrebbe avere una determinata mappatura delle proprietà di configurazione in un account cloud vSphere e un'altra mappatura di configurazione in un'altra istanza di vSphere. Ad esempio, se si dispone di due account cloud vSphere idonei, uno con risorse elevate e un altro con risorse limitate, il piano cluster `large` potrebbe specificare `guaranteed-xlarge` per il server vSphere di alto profilo e `best-effort-medium` per l'istanza di vSphere limitata. In generale, la specifica `large` mappa un set di proprietà di configurazione diverso a ogni istanza del server vSphere idonea.

Dopo aver creato un piano cluster per una o più istanze di vSphere, tutti gli spazi dei nomi supervisore idonei, che un amministratore assegna per ospitare un cluster Tanzu Kubernetes utilizzando l'assegnazione di una zona Kubernetes, devono essere allineati rispetto alla configurazione definita nella specifica del piano cluster. Ad esempio, il criterio di storage specificato nel piano cluster deve essere aggiunto come classe di storage a tutti gli spazi dei nomi supervisore vSphere dedicati per il provisioning dei cluster Tanzu.

Prerequisiti

- Per creare una distribuzione di vSphere with Tanzu Kubernetes in Cloud Assembly, è necessario disporre dell'accesso a vSphere 7.x, disponibile come parte di un account cloud vCenter. Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).
- Tanzu deve essere abilitato nell'account cloud vSphere con uno o più spazi dei nomi supervisore.
- Tutti i cluster supervisore nell'account cloud di vSphere registrato che sono idonei per il provisioning dei cluster Tanzu devono essere aggiunti come entità gestite nella pagina Cloud Assembly **Infrastruttura > Kubernetes > Cluster supervisore** utilizzando l'opzione **Aggiungi cluster supervisore**.

Procedura

- 1 Selezionare **Infrastruttura > Configura > Piano cluster** e fare clic su **Nuovo piano cluster**.
- 2 Immettere un **Account**, un **Nome** e una **Descrizione** per il piano cluster. L'account definisce l'account cloud a cui il piano cluster viene applicato.
- 3 Immettere i dettagli delle informazioni sul cluster, tra cui **Versioni Kubernetes** e **Piano di controllo**. Queste informazioni includono le allocazioni per i nodi, la classe della macchina e la classe di storage.
 - Immettere la versione di Kubernetes applicabile a questo piano cluster. Si tratta della versione di Kubernetes dei cluster Tanzu Kubernetes sottoposti a provisioning, ad esempio 1.19 o 1.20.
 - Il conteggio del piano di controllo definisce la specifica per i nodi del server dell'API Kubernetes.
 - La classe di una macchina virtuale è una richiesta di prenotazioni sulla macchina virtuale per la potenza di elaborazione. Esistono numerose classi di macchina predefinite, che rappresentano diversi livelli di potenza di elaborazione. Per ulteriori informazioni, vedere [Classi di macchine virtuali per i cluster Tanzu Kubernetes](#).
 - I worker specificano i nodi worker di Tanzu Kubernetes da distribuire con questo piano.
- 4 Immettere e selezionare le impostazioni aggiuntive per il piano cluster.
 - Immettere la **Classe di storage PVC predefinita** da utilizzare con questo cluster.
 - Utilizzare i pulsanti di opzione per indicare il comportamento relativo all'utilizzo delle classi di storage e delle impostazioni di rete.
- 5 Fare clic su **Crea**.

Risultati

Il piano cluster viene creato ed è disponibile per l'uso nei modelli cloud di Cloud Assembly.

Operazioni successive

Dopo aver creato un piano cluster, è possibile utilizzarlo per creare una distribuzione di vSphere with Tanzu Kubernetes in Cloud Assembly. Vedere [Provisioning di una distribuzione di vSphere with Tanzu Kubernetes in vRealize Automation](#).

Utilizzo dei cluster e degli spazi dei nomi supervisore di Tanzu in Cloud Assembly

Gli amministratori possono rendere gli spazi dei nomi supervisore in un'integrazione di vSphere abilitata per Tanzu disponibili per gli utenti in modo che possano aggiungere tali spazi dei nomi nelle distribuzioni Kubernetes tramite modelli cloud o richiederli dal catalogo di Service Broker.

Questa attività descrive come aggiungere cluster supervisore Tanzu con Cloud Assembly per l'utilizzo nelle distribuzioni e come creare o aggiungere spazi dei nomi che definiscano le risorse Kubernetes specifiche a cui i progetti e gli utenti di Cloud Assembly possono accedere. Questa funzionalità si basa su un account cloud di vSphere adatto anziché su un'integrazione come VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) oppure OpenShift. I cluster supervisore sono cluster Kubernetes personalizzati associati a vSphere. Espongono le API di Kubernetes agli utenti finali e utilizzano ESXi come piattaforma per i nodi worker anziché Linux. Gli spazi dei nomi supervisore facilitano il controllo dell'accesso alle risorse Kubernetes, perché in genere è più semplice applicare i criteri agli spazi dei nomi anziché alle singole macchine virtuali. È possibile creare più spazi dei nomi per ogni cluster supervisore.

Le distribuzioni abilitate per Tanzu possono utilizzare anche cluster guest generati da vSphere. Un cluster guest è un cluster Kubernetes che viene eseguito nelle macchine virtuali nel cluster supervisore. Un cluster guest è completamente conforme a monte a Kubernetes, quindi è garantito il funzionamento con tutte le applicazioni Kubernetes. I cluster guest in vSphere utilizzano il progetto Cluster API open source per gestire il ciclo di vita dei cluster Kubernetes, che a loro volta utilizzano l'operatore della macchina virtuale per gestire le macchine virtuali che costituiscono un guest.

Quando vengono utilizzate con istanze di vSphere abilitate per Tanzu, le zone Kubernetes definiscono quali cluster supervisore sono disponibili per il provisioning di uno spazio dei nomi supervisore. Gli spazi dei nomi supervisore sono specifici delle istanze di vSphere abilitate per Tanzu. Non è possibile eseguire il provisioning di una risorsa Kubernetes generica in un'istanza di vSphere abilitata per Tanzu.

Gli utenti di Cloud Assembly designati come visualizzatori del progetto possono accedere agli spazi dei nomi in sola visualizzazione, mentre i membri del progetto possono modificarli.

Se lo si desidera, è possibile configurare i cluster supervisore associati agli spazi dei nomi.

Prerequisiti

- Per utilizzare i cluster e gli spazi dei nomi supervisore con Cloud Assembly, è necessario che sia configurato un endpoint di vSphere 7.x. In vRealize Automation, vSphere è installato come parte di un account cloud di vCenter. Vedere [Creazione di un account cloud di vCenter in vRealize Automation](#).

- Tanzu deve essere abilitato nell'account cloud di vSphere e deve contenere spazi dei nomi supervisore appropriati.
- Per fare in modo che gli utenti siano sincronizzati, vCenter e la distribuzione di vRealize Automation devono utilizzare la stessa istanza di Active Directory. In caso contrario, anche se il provisioning continuerà a funzionare, gli utenti di vRealize Automation non potranno accedere automaticamente allo spazio dei nomi.

Procedura

- 1 Selezionare **Infrastruttura > Configura > Zona Kubernetes** in Cloud Assembly.

In questa pagina sono visualizzati i cluster gestiti disponibili per l'uso ed è possibile aggiungere altri cluster. È possibile fare clic su uno dei cluster per visualizzarne i dettagli.

- 2 Selezionare **Nuova zona Kubernetes**.
- 3 In **Account** specificare i dettagli dell'account cloud di vSphere di destinazione.
- 4 Fare clic sull'icona di ricerca nella casella di testo per visualizzare tutti gli account di vSphere o cercare un account in base al nome.
- 5 Digitare un **Nome** e una **Descrizione** per la nuova zona.
- 6 Aggiungere i tag di funzionalità, se pertinenti. Vedere [Utilizzo di tag di funzionalità in Cloud Assembly](#) per ulteriori informazioni.
- 7 Fare clic sulla scheda Provisioning per selezionare il cluster supervisore che verrà associato agli spazi dei nomi.
- 8 Fare clic su **Aggiungi elaborazione** per visualizzare e selezionare i cluster supervisione disponibili.
- 9 Fare clic su **Aggiungi**.
- 10 Scegliere **Infrastruttura > Amministrazione > Progetti** e quindi selezionare il progetto da associare alla zona Kubernetes.
- 11 Fare clic sulla scheda Provisioning Kubernetes nella pagina Progetto.
- 12 Fare clic su **Aggiungi zona Kubernetes** e aggiungere la zona appena creata. Se applicabile, è possibile specificare più zone e impostare la loro priorità.
- 13 Fare clic su **Salva**.

Operazioni successive

Dopo aver configurato uno spazio dei nomi, nella pagina **Infrastruttura > Risorse > Kubernetes** in Cloud Assembly per gli utenti applicabili viene visualizzato lo spazio dei nomi. Gli utenti possono fare clic sul collegamento Indirizzo nella scheda Riepilogo per aprire gli strumenti della CLI di Kubernetes di vSphere per gestire lo spazio dei nomi. Per accedere a un collegamento dei dettagli dello spazio dei nomi supervisore, gli utenti devono essere amministratori del cloud o membri

dello spazio dei nomi per il progetto designato. Gli utenti possono inoltre scaricare un Kubectl personalizzato per utilizzare lo spazio dei nomi supervisore. Gli utenti possono accedere allo spazio dei nomi supervisore e utilizzarlo come qualsiasi altro spazio dei nomi, quindi creare modelli cloud distribuire applicazioni.

Per aggiungere lo spazio dei nomi a un modello cloud, scegliere **Progettazione > Modello cloud** e selezionare un modello cloud esistente o crearne uno nuovo. È quindi possibile selezionare la voce dello spazio dei nomi supervisore nel menu a sinistra e trascinarla nella tela.

È possibile assegnare criteri di storage a uno spazio dei nomi supervisore utilizzando i tag. È possibile aggiungere tag, ad esempio `location:local` per specificare la zona Kubernetes che si desidera utilizzare con la distribuzione e altri tag nei profili di storage, ad esempio `speed:fast` e `speed:slow`.

```
formatVersion: 1
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: 'a'
      storage:
        -profile:
          constraints:
            - tag: 'speed:fast'
        -profile:
          limitMB:1000
          constraints:
            -tag: 'speed:slow'
```

Questo modello cloud richiede uno spazio dei nomi supervisore senza limiti e specifica due profili di storage con tale spazio dei nomi.

Dopo aver distribuito modelli cloud contenenti uno spazio dei nomi supervisore, gli utenti possono richiedere spazi dei nomi supervisore anche dal catalogo di Service Broker. È inoltre possibile fare clic sulla pagina Distribuzioni in Cloud Assembly per visualizzare le informazioni sulla distribuzione e accedere a un collegamento contenente il comando per eseguire kubectl per lo spazio dei nomi in vSphere.

È possibile specificare classi di macchine virtuali per gli spazi dei nomi supervisore in un modello cloud utilizzando la proprietà `vmclasses` che consente di specificare un nome di classe. Vedere il seguente esempio di modello cloud.

```
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: demo-vmclass1
      vmclasses:
        - name: vmclass1
```

Utilizzo di spazi dei nomi e cluster Kubernetes in Cloud Assembly

Gli amministratori del cloud possono aggiungere, visualizzare e gestire la configurazione degli spazi dei nomi e dei cluster Kubernetes distribuiti, sia generici che basati su Pacific, in Cloud Assembly.

Gli utenti dotati di privilegi amministrativi possono visualizzare, aggiungere e gestire gli spazi dei nomi e i cluster Kubernetes per cui si dispone di accesso autorizzato nella pagina **Infrastruttura > Risorse > Kubernetes**. Questa pagina contiene le schede per cluster, spazi dei nomi, cluster supervisore e spazi dei nomi supervisore. È possibile selezionare una di queste schede per visualizzare e gestire le risorse analoghe. In genere, questa pagina semplifica la gestione degli spazi dei nomi e dei cluster distribuiti.

- **Cluster:** un cluster è un gruppo di nodi Kubernetes distribuiti in una o più macchine fisiche. Questa pagina mostra i cluster sottoposti a provisioning e non distribuiti che sono stati configurati per l'utilizzo nell'istanza di Cloud Assembly. È possibile fare clic su un cluster per visualizzare le informazioni sullo stato corrente. Quando si distribuisce un cluster, include un collegamento a un file Kubconfig accessibile solo per gli amministratori del cloud. Questo file concede privilegi di amministratore completi sul cluster, incluso un elenco di spazi dei nomi.

I cluster supervisore sono univoci per le istanze di vSphere e utilizzano ESXi come nodi di lavoro anziché Linux.

- **Spazi dei nomi:** gli spazi dei nomi sono cluster virtuali che forniscono agli amministratori un modo per raggruppare o separare le risorse del cluster. Facilitano la gestione delle risorse tra grandi gruppi di utenti e organizzazioni. Come forma di controllo degli accessi in base al ruolo, un amministratore del cloud può consentire agli utenti di aggiungere spazi dei nomi a un progetto quando richiedono una distribuzione e successivamente gestiscono gli spazi dei nomi dalla pagina Cluster Kubernetes. Quando si distribuisce uno spazio dei nomi, include un collegamento a un file kubeconfig che consente agli utenti validi, ad esempio gli sviluppatori, di visualizzare e gestire alcuni aspetti di tale spazio dei nomi.

I cluster supervisore e gli spazi dei nomi supervisore esistono solo per le istanze di vSphere e forniscono un accesso simile a Kubernetes agli oggetti vSphere.

Un amministratore del cloud può modificare il progetto associato a uno spazio dei nomi o a un cluster Kubernetes in questa pagina, in modo che l'amministratore possa eseguire il provisioning di risorse Kubernetes da modelli cloud e Service Broker e quindi assegnarli a progetti specifici per il consumo. L'amministratore di può modificare l'ambito di un cluster per renderlo specifico del progetto o globale. I cluster globali vengono visualizzati nella scheda Cluster per tutte le zone Kubernetes e sono disponibili per la selezione e il provisioning. Se un cluster è globale, può essere aggiunto a una zona Kubernetes e quindi utilizzato per eseguire il provisioning degli spazi dei nomi dal catalogo.

Se si configura un cluster nuovo o esistente, è necessario scegliere se connettersi con un indirizzo IP primario o un nome host primario.

Utilizzo dei cluster Kubernetes generici in Cloud Assembly

È possibile aggiungere nuovi cluster, esistenti o esterni a Cloud Assembly utilizzando le opzioni in questa pagina.

- 1 Selezionare **Infrastruttura > Risorse > Kubernetes** e verificare che la scheda Cluster sia attiva.

Se sono presenti cluster attualmente configurati per l'istanza di Cloud Assembly, vengono visualizzati in questa pagina.

- 2 Se si aggiunge un cluster nuovo o esistente o se ne distribuisce uno, selezionare l'opzione appropriata in base alla tabella seguente.

Opzione	Descrizione	Dettagli
Distribuisci	Aggiunge nuovi cluster a Cloud Assembly	È necessario specificare l'account cloud TKGI in cui verrà distribuito il cluster, nonché il piano e il numero di nodi desiderati.
Aggiungi esistente	Configura un cluster esistente in modo che funzioni con il progetto.	È necessario specificare l'account cloud TKGI, il cluster da utilizzare e il progetto appropriato per lo sviluppatore di destinazione. Inoltre, è necessario specificare l'ambito di condivisione. Se si desidera condividere globalmente, è necessario configurare le zone e gli spazi dei nomi Kubernetes in modo appropriato.
Aggiungi esterno	Aggiunge un cluster Kubernetes vanilla, che potrebbe non essere associato a TKGI, per Cloud Assembly.	È necessario designare un progetto a cui il cluster è associato, immettere l'indirizzo IP del cluster desiderato e selezionare un proxy cloud e le informazioni del certificato necessarie per connettersi a questo cluster.

- 3 Fare clic su **Aggiungi** per rendere il cluster disponibile in Cloud Assembly.

Utilizzo degli spazi dei nomi Kubernetes in Cloud Assembly

Se si è un amministratore del cloud, gli spazi dei nomi consentono di raggruppare e gestire le risorse del cluster Kubernetes. Se si è un utente, gli spazi dei nomi sono l'area nei cluster Kubernetes per le distribuzioni. Gli amministratori e gli utenti possono accedere agli spazi dei nomi utilizzando la scheda Spazi dei nomi disponibile nella pagina **Infrastruttura > Risorse > Kubernetes**.

Esistono diversi modi per aggiungere spazi dei nomi Kubernetes alle risorse in Cloud Assembly. La seguente procedura illustra un metodo tipico.

- 1 Selezionare **Infrastruttura > Risorse > Kubernetes** e fare clic sulla scheda Spazi dei nomi.
- 2 Per aggiungere un nuovo spazio dei nomi, fare clic su **Nuovo spazio dei nomi**. Per aggiungere uno spazio dei nomi esistente, fare clic su **Aggiungi spazio dei nomi**.
- 3 Immettere un **nome** e una **descrizione** per l'integrazione.

A questo punto è stato aggiunto uno spazio dei nomi da utilizzare con le risorse Kubernetes, ma non è associato a nulla in particolare.

- 4 Specificare il **cluster** che si desidera associare a questo spazio dei nomi.
- 5 Fare clic su **Crea** per aggiungere lo spazio dei nomi a Cloud Assembly.

È possibile aggiungere proprietà personalizzate negli spazi dei nomi Kubernetes per supportare l'estendibilità in diversi modi. È possibile aggiungere proprietà personalizzate quando si esegue il provisioning di uno spazio dei nomi creando un modello cloud di Cloud Assembly. Quando si specifica uno spazio dei nomi Kubernetes in un modello cloud, è possibile aggiungere proprietà allo spazio dei nomi. Innanzitutto, è possibile fare clic con il pulsante destro del mouse sulle proprietà nel modello per accedere alle proprietà predefinite che fanno parte dello schema del modello cloud. Come seconda opzione, è possibile aggiungere proprietà definite dall'utente nella sezione delle proprietà dello spazio nomi nel modello cloud.

Dopo la distribuzione, queste proprietà personalizzate vengono visualizzate nella pagina Distribuzioni in Cloud Assembly per la distribuzione applicabile.

Infine, è possibile aggiungere proprietà personalizzate a uno spazio dei nomi utilizzando le azioni configurate nella pagina **Estendibilità > Azioni** in Cloud Assembly.

Utilizzo di cluster supervisore e spazi dei nomi supervisore

Gli amministratori del cloud possono visualizzare e modificare la configurazione dei cluster e degli spazi dei nomi supervisore nella pagina Kubernetes in Cloud Assembly.

- 1 Selezionare **Infrastruttura > Risorse > Kubernetes** in Cloud Assembly.
- 2 Selezionare **Aggiungi cluster supervisore**.
- 3 In Account specificare i dettagli dell'account cloud di vSphere di destinazione.
- 4 Fare clic sull'icona di ricerca nella casella di testo Cluster supervisore per visualizzare tutti i cluster supervisore oppure cercare un cluster in base al nome.
- 5 Selezionare il cluster desiderato e fare clic su **Aggiungi**.
- 6 Selezionare la scheda Spazi dei nomi supervisore e fare clic sul pulsante **Nuovo spazio dei nomi supervisore** per aggiungere un nuovo spazio dei nomi.
- 7 Selezionare la scheda Spazi dei nomi supervisore e fare clic sul pulsante **Nuovo spazio dei nomi supervisore** per aggiungere un nuovo spazio dei nomi.
 - a Se si sta creando un nuovo spazio dei nomi, aggiungere un **Nome** e una **Descrizione**.
 - b Selezionare l'**Account** cloud appropriato da associare allo spazio dei nomi.
 - c Selezionare il **Cluster supervisore** da associare a questo spazio dei nomi.
 - d Selezionare il **Progetto** da associare allo spazio dei nomi.
 - e Utilizzare la selezione **Criteri di storage disponibili** per aggiungere criteri di storage da utilizzare con lo spazio dei nomi.

È possibile aggiungere tutti i criteri di storage disponibili o selezionare criteri specifici da utilizzare con lo spazio dei nomi supervisore. Inoltre, facoltativamente, è possibile impostare un limite per le dimensioni di storage disponibili con ogni criterio di storage disponibile.

f Fare clic su **Crea**.

- 8 Rivedere i dettagli pertinenti per il nuovo spazio dei nomi. È necessario modificare la configurazione del criterio di storage.

Gli utenti e i gruppi che al momento possono accedere allo spazio dei nomi in vSphere sono elencati nella scheda Utenti. Se vengono aggiunti nuovi utenti o gruppi al progetto, fare clic sul pulsante **Aggiorna utenti** in questa scheda per aggiornare l'elenco. L'elenco non viene aggiornato automaticamente, pertanto è necessario utilizzare il pulsante per aggiornarlo.

Nota La sincronizzazione degli utenti ha senso solo se Cloud Assembly e vCenter sono configurati con un servizio Active Directory/LDAP comune.

Dopo aver configurato un cluster o uno spazio dei nomi, la pagina **Infrastruttura > Risorse > Kubernetes** in Cloud Assembly visualizza i cluster e gli spazi dei nomi disponibili per l'utente. È possibile fare clic su un singolo spazio dei nomi o cluster per aprire una pagina contenente diverse schede che mostrano statistiche e altre informazioni per la risorsa e consentono di configurare varie opzioni.

La scheda Riepilogo per i cluster nella pagina Kubernetes consente agli amministratori di visualizzare e, in alcuni casi, aggiornare la configurazione di un cluster, incluso cambiare l'ambito. I pulsanti di opzione Condivisione consentono di selezionare Globale (condivisibile nella zona Kubernetes) o Progetto (accesso limitato a un singolo progetto). Se si seleziona Progetto, è inoltre necessario specificare il progetto applicabile nella selezione Progetto seguente.

Nota La modifica della configurazione della condivisione può influire sugli spazi dei nomi disponibili nel cluster.

Gli utenti possono fare clic sul collegamento Indirizzo nella scheda Riepilogo per aprire gli strumenti della CLI di Kubernetes di vSphere per gestire lo spazio dei nomi. Per accedere a un collegamento dei dettagli dello spazio dei nomi supervisore, gli utenti devono essere amministratori del cloud o membri dello spazio dei nomi per il progetto designato. Gli utenti possono inoltre scaricare un Kubectl personalizzato per utilizzare lo spazio dei nomi supervisore. Gli utenti possono accedere allo spazio dei nomi supervisore e utilizzarlo come qualsiasi altro spazio dei nomi, quindi creare modelli cloud distribuire applicazioni.

Aggiunta dei componenti Kubernetes ai modelli cloud in Cloud Assembly

Quando si aggiungono componenti Kubernetes a un modello cloud di Cloud Assembly, è possibile scegliere di aggiungere cluster o consentire agli utenti di creare spazi dei nomi in varie configurazioni. Questa scelta dipende in genere dalle esigenze di controllo degli accessi, da come sono stati configurati i componenti Kubernetes e dalle esigenze di distribuzione.

Per aggiungere un componente Kubernetes a un modello cloud in Cloud Assembly, selezionare **Progettazione > Modelli cloud**, fare clic su **Nuovo**, quindi individuare ed espandere l'opzione Kubernetes nel menu a sinistra. Selezionare quindi il valore desiderato, ovvero il cluster o lo spazio dei nomi KBS trascinandolo nella tela.

L'aggiunta a un modello cloud di un cluster Kubernetes associato a un progetto è il metodo più semplice per rendere le risorse Kubernetes disponibili per gli utenti validi. È possibile utilizzare i tag nei cluster per controllare dove sono distribuiti proprio come per le altre risorse di Cloud Assembly. È possibile utilizzare i tag per selezionare una zona e un piano VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) durante la fase di allocazione della distribuzione del cluster.

Dopo aver aggiunto un cluster tramite questa procedura, tale cluster è disponibile automaticamente per tutti gli utenti validi.

Esempi di modelli cloud

Il primo esempio di modello cloud mostra un modello per una distribuzione di Kubernetes semplice controllata da tag. Una zona Kubernetes è stata creata con due piani di distribuzione, configurati nella nuova pagina della zona Kubernetes. In questo caso, un tag denominato `placement:tag` è stato aggiunto come funzionalità nella zona ed è stato utilizzato in modo da corrispondere al vincolo analogo nel modello cloud. Se sono state configurate più zone con il tag, verrà selezionata quella con il numero di priorità più basso.

```
formatVersion: 1
inputs: {}
resources:
  Cluster_provisioned_from_tag:
    type: Cloud.K8S.Cluster
    properties:
      hostname: 109.129.209.125
      constraints:
        -tag: 'placement tag'
      port: 7003
      workers: 1
      connectBy: hostname
```

Il secondo esempio di modello cloud illustra come configurare un modello con una variabile denominata `$(input.hostname)` in modo che gli utenti possano immettere il nome host del cluster desiderato quando richiedono una distribuzione. I tag possono essere utilizzati anche per selezionare una zona e un piano TKGI durante la fase di allocazione delle risorse della distribuzione del cluster.

```
formatVersion: 1
inputs:
  hostname:
    type: string
    title: Cluster hostname
resources:
  Cloud_K8S_Cluster_1:
    type: Cloud.K8S.Cluster
```



```

properties:
  hostname: ${input.hostname}
  port: 8443
  connectBy: hostname
  workers: 1

```

Se si desidera utilizzare gli spazi dei nomi per gestire l'utilizzo del cluster, è possibile configurare una variabile nel modello cloud denominata *name: \${input.name}* per sostituire il nome dello spazio dei nomi che un utente immette quando richiede una distribuzione. Per questo tipo di distribuzione, è possibile creare un modello simile al seguente esempio:

```

1 formatVersion: 1
2 inputs:
3 name:
4   type: string
5   title: "Namespace name"
6 resources:
7   Cloud_KBS_Namespace_1:
8     type: Cloud.K8S.Namespace
9     properties:
10      name: ${input.name}

```

Gli utenti possono gestire i cluster distribuiti tramite i file kubeconfig accessibili dalla pagina **Infrastruttura > Risorse > Cluster Kubernetes**. Individuare la scheda nella pagina del cluster desiderato e fare clic su **Kubeconfig**.

Spazi dei nomi supervisore in VMware Cloud Templates

Di seguito è riportato lo schema relativo a uno spazio dei nomi supervisore di base in un modello cloud di Cloud Assembly.

```

{
  "title": "Supervisor namespace schema",
  "description": "Request schema for provisioning of Supervisor namespace resource",
  "type": "object",
  "properties": {
    "name": {
      "title": "Name",
      "description": "Alphabetic (a-z and 0-9) string with maximum length of 63 characters. The character '-' is allowed anywhere except the first or last position of the identifier.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9-]{1,63}$",
      "ignoreOnUpdate": true
    },
    "description": {
      "title": "Description",
      "description": "An optional description of this Supervisor namespace.",
      "type": "string",
      "ignoreOnUpdate": true
    },
    "content": {
      "title": "Content",
      "description": "Kubernetes Yaml Content",

```

```

    "type": "string",
    "maxLength": 65000
  },
  "constraints": {
    "title": "Constraints",
    "description": "To target the correct resources, blueprint constraints are matched
against infrastructure capability tags. Constraints must include the key name. Options
include value, negative [!], and hard or soft requirement.",
    "type": "array",
    "recreateOnUpdate": true,
    "items": {
      "type": "object",
      "properties": {
        "tag": {
          "title": "Tag",
          "description": "Constraint definition in syntax `[!]tag_key[:tag_value]
[:hard|soft]` \nExamples:\n```\n!location:eu:hard\n location:us:soft\n!pci\n```,
          "type": "string",
          "recreateOnUpdate": true
        }
      }
    }
  },
  "limits": {
    "title": "Limits",
    "description": "Defines namespace resource limits such as pods, services, etc.",
    "type": "object",
    "properties": {
      "stateful_set_count": {
        "title": "stateful_set_count",
        "description": "This represents the new value for 'statefulSetCount' option which
is the maximum number of StatefulSets in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
      },
      "deployment_count": {
        "title": "deployment_count",
        "description": "This represents the new value for 'deploymentCount' option which is
the maximum number of deployments in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
      },
      "cpu_limit_default": {
        "title": "cpu_limit_default",
        "description": "This represents the new value for the default CPU limit (in Mhz)
for containers in the pod. If specified, this limit should be at least 10 MHz.",
        "type": "integer",
        "recreateOnUpdate": false
      },
      "config_map_count": {
        "title": "config_map_count",
        "description": "This represents the new value for 'configMapCount' option which is
the maximum number of ConfigMaps in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
      }
    }
  }
}

```

```

    },
    "pod_count": {
      "title": "pod_count",
      "description": "This represents the new value for 'podCount' option which is the
maximum number of pods in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "job_count": {
      "title": "job_count",
      "description": "This represents the new value for 'jobCount' option which is the
maximum number of jobs in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "secret_count": {
      "title": "secret_count",
      "description": "This represents the new value for 'secretCount' option which is the
maximum number of secrets in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "cpu_limit": {
      "title": "cpu_limit",
      "description": "This represents the new value for 'limits.cpu' option which is
equivalent to the maximum CPU limit (in MHz) across all pods in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "cpu_request_default": {
      "title": "cpu_request_default",
      "description": "This represents the new value for the default CPU request (in Mhz)
for containers in the pod. If specified, this field should be at least 10 MHz.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_limit_default": {
      "title": "memory_limit_default",
      "description": "This represents the new value for the default memory limit (in
mebibytes) for containers in the pod.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_limit": {
      "title": "memory_limit",
      "description": "This represents the new value for 'limits.memory' option which is
equivalent to the maximum memory limit (in mebibytes) across all pods in the namespace.",
      "type": "integer",
      "recreateOnUpdate": false
    },
    "memory_request_default": {
      "title": "memory_request_default",
      "description": "This represents the new value for the default memory request (in
mebibytes) for containers in the pod.",
      "type": "integer",

```

```

        "recreateOnUpdate": false
    },
    "service_count": {
        "title": "service_count",
        "description": "This represents the new value for 'serviceCount' option which is
the maximum number of services in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "replica_set_count": {
        "title": "replica_set_count",
        "description": "This represents the new value for 'replicaSetCount' option which is
the maximum number of ReplicaSets in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "replication_controller_count": {
        "title": "replication_controller_count",
        "description": "This represents the new value for 'replicationControllerCount'
option which is the maximum number of ReplicationControllers in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "storage_request_limit": {
        "title": "storage_request_limit",
        "description": "This represents the new value for 'requests.storage' which is the
limit on storage requests (in mebibytes) across all persistent volume claims from pods in the
namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "persistent_volume_claim_count": {
        "title": "persistent_volume_claim_count",
        "description": "This represents the new value for 'persistentVolumeClaimCount'
option which is the maximum number of PersistentVolumeClaims in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    },
    "daemon_set_count": {
        "title": "daemon_set_count",
        "description": "This represents the new value for 'daemonSetCount' option which is
the maximum number of DaemonSets in the namespace.",
        "type": "integer",
        "recreateOnUpdate": false
    }
},
"additionalProperties": false
},
"vm_classes": {
    "title": "VM classes",
    "description": "Defines set of Virtual Machine classes to be assigned to the namespace",
    "type": "array",
    "recreateOnUpdate": false,
    "items": {
        "type": "object",

```

```

    "properties": {
      "name": {
        "title": "Name",
        "description": "Name of the Virtual Machine class.",
        "type": "string",
        "recreateOnUpdate": false
      }
    }
  },
  "storage": {
    "title": "Storage policies",
    "description": "Defines set of storage profiles to be used to assign storage policies
to the namespace.",
    "type": "array",
    "recreateOnUpdate": false,
    "items": {
      "type": "object",
      "properties": {
        "profile": {
          "type": "object",
          "title": "Storage profile",
          "description": "Defines storage policies to be assigned to the namespace",
          "recreateOnUpdate": false,
          "properties": {
            "constraints": {
              "title": "Constraints",
              "description": "To target the correct storage profiles, blueprint constraints
are matched against storage profile capability tags.",
              "type": "array",
              "recreateOnUpdate": false,
              "items": {
                "type": "object",
                "properties": {
                  "tag": {
                    "title": "Tag",
                    "description": "Constraint definition in syntax `[!]tag_key[:tag_value]
[:hard|:soft]` \nExamples:\n```\nlocation:eu:hard\n location:us:soft\n```,
                    "type": "string",
                    "recreateOnUpdate": false
                  }
                }
              }
            },
            "minItems": 1
          }
        },
        "limitMb": {
          "title": "Limit",
          "description": "The maximum amount of storage (in mebibytes) which can be
utilized by the namespace for this storage policy. Optional. If unset, no limits are placed.",
          "type": "integer"
        }
      }
    },
    "required": [
      "constraints"
    ]
  }
}

```

```

    }
  }
}
},
"required": [
  "name"
]
}

```

VMware Cloud Templates supporta l'utilizzo di limiti con gli spazi dei nomi supervisore. I limiti consentono di controllare l'utilizzo delle risorse per CPU e memoria, nonché il numero massimo di pod consentiti nello spazio dei nomi per le macchine distribuite.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: '${env.deploymentName}'
      limits:
        - cpu_limit: 1000
          cpu_request_default: 800
          memory_limit: 2000
          memory_limit_default: 1500
          pod_count: 200

```

L'esempio seguente illustra come specificare un criterio di storage utilizzando i tag.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: 'ns-with-storage-policy'
      description: 'sample'
      storage:
        - profile:
            limitMb: 1000
            constraints:
              - tag: 'storage:fast'
        - profile:
            constraints:
              - tag: 'storage:cheap'

```

Utilizzo di YAML arbitrari con uno spazio dei nomi self-service o VCT del cluster

Come parte della creazione di un cluster o di uno spazio dei nomi, spesso gli utenti desiderano eseguire personalizzazioni aggiuntive. Ad esempio, può essere necessario aggiungere utenti (ruolo/binding del ruolo) o creare un criterio di sicurezza pod o installare agenti. Utilizzando la proprietà `content` di YAML, gli utenti possono definire pacchetti personalizzati di cui desiderano eseguire il provisioning in tale cluster/spazio dei nomi/spazio dei nomi supervisore.

Ogni pacchetto di contenuti YAML associato alla proprietà `content` deve essere separato con tre trattini (---). Anche le informazioni dei contenuti devono essere una stringa a più righe. Fare riferimento al seguente esempio di YAML per capire come configurare i pacchetti di contenuti.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Tanzu_Cluster_1:
    type: Cloud.Tanzu.Cluster
    properties:
      name: ddonchev-tkc
      plan: small
      content: |-
        apiVersion: rbac.authorization.k8s.io/v1
        kind: ClusterRoleBinding
        metadata:
          name: psp:authenticated-from-yaml
        subjects:
        - apiGroup: rbac.authorization.k8s.io
          kind: Group
          name: system:authenticated
        roleRef:
          apiGroup: rbac.authorization.k8s.io
          kind: ClusterRole
          name: psp:vmware-system-privileged
        ---
        apiVersion: apiextensions.k8s.io/v1
        kind: CustomResourceDefinition
        metadata:
          # name must match the spec fields below, and be in the form: <plural>.<group>
          name: crontabs.stable.example.com
        spec:
          # group name to use for REST API: /apis/<group>/<version>
          group: stable.example.com
          # list of versions supported by this CustomResourceDefinition
          versions:
            - name: v1
              # Each version can be enabled/disabled by Served flag.
              served: true
              # One and only one version must be marked as the storage version.
              storage: true
              schema:
                openAPIV3Schema:
                  type: object
                  properties:
                    spec:
```

```

      type: object
    properties:
      cronSpec:
        type: string
      image:
        type: string
      replicas:
        type: integer
    # either Namespaced or Cluster
    scope: Namespaced
    names:
      # plural name to be used in the URL: /apis/<group>/<version>/<plural>
      plural: crontabs
      # singular name to be used as an alias on the CLI and for display
      singular: crontab
      # kind is normally the CamelCased singular type. Your resource manifests use this.
      kind: CronTab
      # shortNames allow shorter string to match your resource on the CLI
      shortNames:
        - ct

```

Il codice YAML definito nella proprietà del contenuto viene visualizzato anche nella scheda Proprietà per la distribuzione.

Cloud Assembly può creare risorse di contenuti solo nell'ambito della risorsa da distribuire. Ad esempio, se si esegue il provisioning di uno spazio dei nomi Kubernetes, Cloud Assembly non può creare una distribuzione all'interno di uno spazio dei nomi diverso. Gli utenti hanno gli stessi diritti che avrebbero se stessero usando kubeconfig con kubectl.

Dopo il provisioning della macchina virtuale, viene avviata l'installazione degli oggetti Kubernetes della proprietà `content`. Se per una delle risorse a cui si fa riferimento nella proprietà del contenuto YAML non è possibile eseguire il provisioning, Cloud Assembly eseguirà il rollback ed eliminerà tutti gli oggetti Kubernetes precedenti dalla risorsa e la distribuzione avrà lo stato Non riuscita. La risorsa verrà comunque sottoposta a provisioning e sarà visibile. Sarà inoltre possibile utilizzare le azioni giorno 2, incluso il tentativo di applicare nuovamente il contenuto.

È possibile migliorare la proprietà `content` con input del modello cloud come illustrato nell'esempio seguente.

```

formatVersion: 1
inputs: {}
resources:
  Cloud_SV_Namespace_1:
    type: Cloud.SV.Namespace
    properties:
      name: sv-namespace-with-vm-classes
      vm_classes:
        - name: best-effort-2xlarge
        - name: best-effort-4xlarge
        - name: best-effort-8xlarge

```


È inoltre possibile eseguire il provisioning di risorse personalizzate come `TanzuKubernetesCluster`. Questa operazione non riuscirà come operazione giorno 1 perché lo spazio dei nomi supervisore non conterrà le classi di storage e le classi di macchine virtuali necessarie. Quando le classi di macchine virtuali e le classi di storage sono associate allo spazio dei nomi supervisore, è possibile creare `TanzuKubernetesCluster` (o un'altra risorsa) utilizzando l'azione giorno 2.

Nota: è possibile eseguire il provisioning di una risorsa senza contenuto ed aggiungere comunque oggetti Kubernetes come YAML con l'azione giorno 2.

Il contenuto visualizzato nella proprietà YAML definisce il contenuto di cui viene eseguito il provisioning nella risorsa. Quando si modificano questi contenuti, la seguente tabella mostra i possibili risultati:

Azione	Risultato
Se si aggiunge un oggetto Kubernetes e si invia.	L'oggetto specificato viene creato nella risorsa.
Se si rimuove un oggetto Kubernetes e si invia.	L'oggetto specificato viene eliminato dalla risorsa.
Se si modifica un oggetto Kubernetes e si invia.	L'oggetto specificato è sottoposto a patch nella risorsa.

È importante chiarire quali azioni vengono considerate come modifiche dell'oggetto corrente. Ad esempio, se si modifica il campo dello spazio dei nomi di un oggetto, viene creato un nuovo oggetto anziché sottoporre a patch quello precedente.

L'univocità di una risorsa è definita dai seguenti campi: `apiVersion`, `kind`, `metadata.name`, `metadata.namespace`

Utilizzo dell'estendibilità di Cloud Assembly con Kubernetes

Cloud Assembly fornisce una serie di argomenti degli eventi che corrispondono alle azioni tipiche correlate alla distribuzione dello spazio dei nomi e del cluster Kubernetes. Gli utenti possono iscriversi a questi argomenti in base alle esigenze e questi verranno eseguiti nel momento appropriato. Gli utenti riceveranno la notifica al verificarsi dell'evento correlato all'argomento sottoscritto. È inoltre possibile configurare workflow vRO da eseguire in base alle notifiche degli eventi.

Gli argomenti seguenti sono disponibili per l'iscrizione nella pagina **Estendibilità > Libreria > Argomenti dell'evento** in Cloud Assembly. Per visualizzare questi argomenti, cercare Kubernetes nella casella di testo di ricerca degli argomenti dell'evento.

- Allocations di cluster Kubernetes
- Post-provisioning di cluster Kubernetes
- Post-rimozione di cluster Kubernetes
- Provisioning di cluster Kubernetes
- Rimozione di cluster Kubernetes
- Allocations di spazio dei nomi Kubernetes
- Post-provisioning di spazio dei nomi Kubernetes

- Post-rimozione di spazio dei nomi Kubernetes
- Rimozione di spazio dei nomi Kubernetes
- Allocazione di spazio dei nomi Kubernetes
- Allocazione di spazio dei nomi supervisore Kubernetes
- Post-provisioning di spazio dei nomi supervisore Kubernetes
- Post-rimozione di spazio dei nomi supervisore Kubernetes
- Rimozione di spazio dei nomi supervisore Kubernetes
- Allocazione di spazio dei nomi supervisore Kubernetes

Fare clic su uno degli argomenti per visualizzare lo schema di tale argomento che mostra tutte le informazioni raccolte e trasmesse. Sono disponibili argomenti relativi agli spazi dei nomi sia per gli spazi dei nomi Kubernetes che per gli spazi dei nomi supervisore. È possibile utilizzare una di queste informazioni sullo schema per configurare varie notifiche e attività di gestione e di creazione di report.

È possibile configurare gli script di azione per le azioni correlate a CMX nella pagina **Estendibilità > Libreria > Azioni**. Gli script di azione possono essere utilizzati per vari scopi: ad esempio, per creare un record DNS del provisioning del cluster Kubernetes. Se si sta creando un record DNS, è possibile utilizzare il campo `masternodeips` nell'argomento del post-provisioning di cluster Kubernetes con un comando REST in uno script di azione per creare un record DNS.

La pagina Sottoscrizioni definisce la relazione tra gli argomenti degli eventi e gli script di azione. È possibile visualizzare e gestire tali componenti nella pagina Sottoscrizioni in Cloud Assembly.

Per ulteriori informazioni, vedere la documentazione sull'estendibilità di Cloud Assembly qui: [Estensione e automazione dei cicli di vita delle applicazioni con l'estendibilità](#).

Che cos'è la gestione della configurazione in Cloud Assembly

Cloud Assembly supporta l'integrazione con Puppet Enterprise, Ansible Open Source e Ansible Tower in modo da poter gestire le distribuzioni per la configurazione e la deviazione.

Integrazione di Puppet

Per integrare la gestione della configurazione basata su Puppet, è necessario disporre di un'istanza valida di Puppet Enterprise installata su un cloud pubblico o privato con un carico di lavoro di vSphere. È necessario stabilire una connessione tra questo sistema esterno e l'istanza di Cloud Assembly. È quindi possibile rendere disponibile la gestione della configurazione di Puppet a Cloud Assembly aggiungendola ai blueprint appropriati.

Il fornitore di Puppet del servizio di blueprint di Cloud Assembly installa, configura ed esegue l'agente Puppet su una risorsa di elaborazione distribuita. Il fornitore di Puppet supporta le connessioni SSH e WinRM con i seguenti prerequisiti:

- Connessioni SSH:
 - Il nome utente deve essere un super utente o un utente con autorizzazioni sudo per eseguire comandi con NOPASSWD.
 - Disattivare `requiretty` per l'utente specificato.
 - cURL deve essere disponibile nella risorsa di elaborazione della distribuzione.
- Connessioni WinRM:
 - PowerShell 2.0 deve essere disponibile nella risorsa di elaborazione della distribuzione.
 - Configurare il modello di Windows come descritto nella documentazione di vRealize Orchestrator.

L'amministratore di DevOps è responsabile della gestione delle connessioni a un Puppet Master e dell'applicazione di ruoli di Puppet o delle regole di configurazione a distribuzioni specifiche. Dopo la distribuzione, le macchine virtuali configurate per supportare la gestione della configurazione vengono registrate con il Puppet Master designato.

Quando le macchine virtuali vengono distribuite, gli utenti possono aggiungere o eliminare un Puppet Master come sistema esterno o aggiornare i progetti assegnati al Puppet Master. Infine, gli utenti appropriati possono annullare la registrazione delle macchine virtuali distribuite dal Puppet Master quando le macchine vengono disattivate.

Integrazione di Ansible Open Source

Quando si configura un'integrazione di Ansible, installare Ansible Open Source in conformità alle istruzioni di installazione di Ansible. Per ulteriori informazioni sull'installazione, vedere la documentazione di Ansible.

Ansible attiva per impostazione predefinita il controllo della chiave host. Se un host viene reinstallato con una chiave diversa nel file `known_hosts`, verrà visualizzato un messaggio di errore. Se un host non è elencato nel file `known_hosts`, è necessario fornire la chiave all'avvio. È possibile disattivare il controllo della chiave host con le seguenti impostazioni nel file `/etc/ansible/ansible.cfg` o `~/.ansible.cfg`:

```
[defaults]
host_key_checking = False
localhost_warning = False

[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null
```

Per evitare errori di controllo della chiave host, impostare `host_key_checking` e `record_host_keys` su `False`, inclusa l'aggiunta di un'opzione `UserKnownHostsFile=/dev/null` aggiuntiva impostata in `ssh_args`. Inoltre, se l'inventario è vuoto inizialmente, Ansible segnala che l'elenco degli host è vuoto. In questo modo, il controllo della sintassi del playbook non riesce.

Ansible Vault consente di archiviare informazioni riservate, ad esempio password o chiavi, in file crittografati anziché come testo normale. Vault è crittografato con una password. In Cloud Assembly, Ansible utilizza Vault per crittografare dati quali le password ssh per le macchine host. Si presuppone che il percorso della password di Vault sia stato impostato.

È possibile modificare il file `ansible.cfg` per specificare la posizione del file della password utilizzando il formato seguente.

```
vault_password_file = /path to/file.txt
```

È inoltre possibile impostare la variabile di ambiente `ANSIBLE_VAULT_PASSWORD_FILE` in modo che Ansible cerchi automaticamente la password. Ad esempio, `ANSIBLE_VAULT_PASSWORD_FILE=~/.vault_pass.txt`.

Cloud Assembly gestisce il file di inventario Ansible, pertanto è necessario assicurarsi che l'utente di Cloud Assembly disponga dell'accesso `rwX` nel file di inventario.

```
cat ~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/
user_defined_script/ | head -1)/log.txt
```

Se si desidera utilizzare un utente non root con l'integrazione open source di Cloud Assembly, gli utenti richiedono una serie di autorizzazioni per eseguire i comandi utilizzati dal provider open source di Cloud Assembly. I seguenti comandi devono essere impostati nel file `sudoers` dell'utente.

```
Defaults:myuser !requiretty
```

Se l'utente non fa parte di un gruppo di amministratori che non dispone di alcuna applicazione `askpass` specificata, impostare il comando seguente nel file `sudoers` dell'utente.

```
myuser ALL=(ALL) NOPASSWD: ALL
```

Se si verificano errori o altri problemi durante la configurazione dell'integrazione di Ansible, fare riferimento al file `log.txt` nel percorso `'cat~/var/tmp/vmware/provider/user_defined_script/$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ | head -1)'` in Ansible Control Machine.

Integrazione di Ansible Tower

Tipi di sistemi operativi supportati

- Red Hat Enterprise Linux 8.0 o versione successiva a 64 bit (x86) supporta solo Ansible Tower 3.5 e versione successiva.
- Red Hat Enterprise Linux 7.4 o versione successiva a 64 bit (x86).

- CentOS 7.4 o versione successiva a 64 bit (x86).

Di seguito è riportato un file di inventario di esempio, generato durante un'installazione di Ansible Tower. Potrebbe essere necessario modificarlo per gli utilizzi di integrazione di Cloud Assembly.

```
[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# pwd

/root/ansible-tower-install/ansible-tower-setup-bundle-3.5.2-1.el8

[root@cava-env8-dev-001359 ansible-tower-setup-bundle-3.5.2-1.el8]# cat inventory

[tower]

localhost ansible_connection=local


[database]


[all:vars]

admin_password='VMware1!'


pg_host=''

pg_port=''


pg_database='awx'

pg_username='awx'

pg_password='VMware1!'


rabbitmq_port=5672

rabbitmq_vhost=tower

rabbitmq_username=tower

rabbitmq_password='VMware1!'

rabbitmq_cookie=cookiemonster
```

```
# Needs to be true for fqdns and ip addresses

rabbitmq_use_long_name=false


# Isolated Tower nodes automatically generate an RSA key for authentication;

# To deactivate this behavior, set this value to false

# isolated_key_generation=true
```

Configurazione dell'integrazione di Puppet Enterprise in Cloud Assembly

Cloud Assembly supporta l'integrazione con la gestione della configurazione di Puppet Enterprise.

Quando si aggiunge Puppet Enterprise a Cloud Assembly come sistema esterno, per impostazione predefinita è disponibile in tutti i progetti. È possibile limitarlo a progetti specifici.

Per aggiungere un'integrazione di Puppet Enterprise, è necessario disporre del nome master di Puppet e del nome host o indirizzo IP del master.

I registri di Puppet sono disponibili nella seguente posizione nel caso in cui sia necessario controllarli per errori o a scopo informativo.

Descrizione	Posizione registro
Registro per gli eventi correlati alla creazione e all'installazione	I registri si trovano nella macchina distribuita in <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/`.</code> Per i registri completi, fare riferimento al file log.txt . Per i registri dettagliati dell'agente di Puppet, fare riferimento a https://puppet.com/docs/puppet/4.8/services_agent_unix.html#logging
Registro per le attività correlate all'esecuzione e all'eliminazione di Puppet	I registri si trovano in PE all'indirizzo <code>~/var/tmp/vmware/provider/user_defined_script/\$(ls -t ~/var/tmp/vmware/provider/user_defined_script/ head -1)/`.</code> Per i registri completi, fare riferimento al file log.txt .

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare Puppet.

3 Immettere le informazioni richieste nella pagina di configurazione di Puppet.

Per il corretto funzionamento dell'integrazione di Puppet, le credenziali fornite devono essere valide sia per l'account SSH sia per l'account API. Inoltre, gli account utente del sistema operativo e dell'applicazione specificati devono avere lo stesso nome utente e la stessa password.

4 Fare clic su **Convalida** per verificare l'integrazione.

5 Fare clic su **Aggiungi**.

Risultati

Puppet è disponibile per l'uso con i modelli cloud.

Operazioni successive

Aggiungere i componenti di Puppet ai modelli cloud desiderati.

- 1 In Modelli di cloud in Cloud Assembly, selezionare Puppet sotto l'intestazione Gestione contenuti nel menu Modello cloud e trascinare il componente Puppet nella tela.
- 2 Immettere le proprietà di Puppet nel riquadro a destra.

Proprietà	Descrizione
Master	Immettere il nome della macchina primaria di Puppet utilizzata con questo modello cloud.
Ambiente	Selezionare l'ambiente per la macchina principale di Puppet.
Ruolo	Selezionare il ruolo di Puppet da utilizzare con questo modello cloud.
Intervallo di esecuzione dell'agente	La frequenza con cui si desidera che l'agente Puppet esegua il polling della macchina principale di Puppet affinché i dettagli della configurazione vengano applicati alle macchine virtuali distribuite correlate a questo modello cloud.

- 3 Fare clic sulla scheda Codice nel riquadro a destra per visualizzare il codice YAML per le proprietà di configurazione di Puppet.

Quando si aggiunge un componente Puppet a un modello cloud, è possibile aggiungere la proprietà `installMaster` al file YAML in modo che punti a un master di installazione Puppet, definito anche come master di compilazione. Il valore di questa proprietà può essere l'indirizzo IP o il nome host del master di compilazione Puppet. L'utilizzo di questa proprietà consente di accedere a funzionalità avanzate per le macchine virtuali Puppet distribuite e inoltre supporta azioni del giorno 2 aggiuntive.

```
Puppet_Agent:
  type: Cloud.Puppet
  properties:
    account: PEIntegrationAccount
```

```

environment: production
role: 'role::linux_webserver'
host: '${CentOS-Puppet.*}'
username: root
password: password123!
installMaster: my-pe-compile-master.example.com
agentConfiguration:
  certName: '${CentOS-Puppet.address}'
osType: linux
count: 1

```

Nota Sebbene l'utente definito qui sia root, il modello cloud può essere configurato con qualsiasi utente incluso nell'elenco sudoers.

In alcuni casi, per impostazione predefinita, vRealize Automation passa alcune informazioni relative alla macchina alle macchine virtuali Puppet come dati. I dati personalizzati non sono supportati per le macchine Windows. Nelle macchine Linux vengono trasmesse alcune informazioni per impostazione predefinita e gli utenti possono passare informazioni aggiuntive utilizzando le proprietà personalizzate.

Esistono alcune limitazioni di ciò che viene passato alle macchine Puppet in Linux. Le proprietà personalizzate nelle risorse host e nell'agente Puppet vengono passate alle macchine virtuali Puppet. Le proprietà personalizzate nelle risorse di rete non vengono passate alla macchina virtuale. Gli elementi passati includono proprietà semplici, proprietà booleane, nonché tipi personalizzati denominati e complessi come le mappe nidificate con array.

L'esempio seguente mostra come è possibile richiamare varie risorse personalizzate su risorse host:

```

resources:
  Puppet-Host:
    type: Cloud.AWS.EC2.Instance
    properties:
      customer_specified_property_on_ec2_resource: "property"

customer_specified_property_on_network_resource_that_should_also_be_a_fact_and_is_boolean:
true
  CustomerNameStuff: "zone A"
  try_map:
    key: value
    keytwo: value
  nested_array:
    - one
    - two
    - true
  try_array:
    - one
    - two
    -three:
      inner_key: value

```


Se un comando di rimozione di Puppet causa errori, nella maggior parte dei casi vRealize Automation ignorerà gli errori di rimozione dei nodi e procederà con l'eliminazione del nodo. Anche se non viene trovato un certificato per un nodo specifico, vRealize Automation procederà con l'eliminazione. Se vRealize Automation non è in grado di procedere con l'eliminazione del nodo per un motivo qualsiasi, è possibile fare clic su Elimina nel menu Azioni della pagina Distribuzioni per aprire una finestra di dialogo che consentirà di procedere con l'eliminazione del nodo. Viene eseguito un workflow simile quando si rimuove un'integrazione di Puppet da un modello cloud e quindi si applica il modello alla distribuzione. Questo workflow attiva un'operazione di rimozione del nodo gestita come descritto in precedenza.

L'integrazione con Puppet Enterprise richiede un indirizzo IP pubblico. Se per la macchina Puppet Enterprise non è configurato alcun indirizzo IP pubblico, viene utilizzato l'indirizzo IP della prima scheda NIC.

Se la scheda NIC di una macchina sottoposta a provisioning Puppet eseguita su una macchina vSphere dispone di più indirizzi IP, è possibile utilizzare la proprietà YAML `primaryAddress` nei modelli cloud per specificare l'indirizzo IP da utilizzare per le connessioni. Quando la proprietà `primaryAddress` è assegnata a una scheda NIC, l'indirizzo IP di tale scheda NIC viene utilizzato da Puppet. È possibile designare una sola scheda NIC come primaria. Vedere il seguente frammento di codice YAML per un esempio di come viene utilizzata la proprietà `primaryAddress`.

```
BaseVM:
  type: Cloud.vSphere.Machine
  properties:
    image: photon
    count: 2
    customizationSpec: Linux
    cpuCount: 1
    totalMemoryMB: 1024
    networks:
      - network: '${resource.dev.id}'
        deviceIndex: 0
        primaryAddress: true
        assignment: static
      - network: '${resource.prod.id}'
        deviceIndex: 1
        assignment: static
```

Se la proprietà `primaryAddress` non è impostata per alcuna scheda NIC di una macchina virtuale, la logica dei modelli cloud utilizzerà per impostazione predefinita il comportamento corrente per la selezione dell'indirizzo IP.

Configurazione dell'integrazione di Ansible Open Source in Cloud Assembly

Cloud Assembly supporta l'integrazione con la gestione della configurazione di Ansible Open Source. Dopo aver configurato l'integrazione, è possibile aggiungere i componenti di Ansible a distribuzioni nuove o esistenti.

Quando si integra Ansible Open Source con Cloud Assembly, è possibile configurarlo in modo che esegua uno o più playbook di Ansible in un determinato ordine quando viene eseguito il provisioning di una nuova macchina, per automatizzare la gestione della configurazione. È possibile specificare i playbook desiderati nel modello cloud di una distribuzione.

Quando si configura un'integrazione di Ansible, è necessario specificare la macchina host di Ansible Open Source, nonché il percorso del file di inventario che definisce le informazioni per la gestione delle risorse. È inoltre necessario specificare un nome e una password per accedere all'istanza di Ansible Open Source. In un secondo momento, quando si aggiunge un componente di Ansible a una distribuzione, è possibile aggiornare la connessione in modo che utilizzi l'autenticazione basata su chiave.

Per impostazione predefinita, Ansible utilizza SSH per connettersi alle macchine fisiche. Se si utilizzano macchine Windows come specificato nel modello cloud con la proprietà `osType` di Windows, la variabile `connection_type` viene impostata automaticamente su `winrm`.

Inizialmente, l'integrazione di Ansible utilizza le credenziali utente/password o utente/chiave fornite nell'integrazione per connettersi alla macchina di controllo Ansible. Una volta completata la connessione, viene convalidata la sintassi dei playbook forniti nel modello cloud.

Se la convalida viene completata correttamente, viene creata una cartella di esecuzione sulla macchina di controllo Ansible in `~/var/tmp/vmware/provider/user_defined_script/`. Questa è la posizione da cui gli script vengono eseguiti per aggiungere l'host all'inventario, creare file `host_vars`, tra cui la configurazione della modalità di autenticazione per la connessione all'host e infine eseguire i playbook. A questo punto vengono utilizzate le credenziali fornite nel modello cloud per connettersi all'host dalla macchina di controllo Ansible.

L'integrazione di Ansible supporta le macchine fisiche che non utilizzano un indirizzo IP. Per le macchine con provisioning su cloud pubblici come AWS, Azure e GCP, la proprietà `address` nella risorsa creata viene compilata con l'indirizzo IP pubblico della macchina solo quando la macchina è connessa a una rete pubblica. Per le macchine non connesse a una rete pubblica, l'integrazione di Ansible cerca l'indirizzo IP dalla rete collegata alla macchina. Se sono presenti più reti collegate, l'integrazione di Ansible cerca la rete con il valore minimo di `deviceIndex`, ovvero l'indice della scheda NIC (Network Interface Card) collegata alla macchina. Se la proprietà `deviceIndex` non è specificata nel blueprint, l'integrazione utilizza la prima rete collegata.

Vedere [Che cos'è la gestione della configurazione in Cloud Assembly](#) per ulteriori informazioni sulla configurazione di Ansible Open Source per l'integrazione in Cloud Assembly.

Prerequisiti

- La macchina di controllo Ansible deve utilizzare una versione di Ansible. Fare riferimento alla [Matrice di supporto di vRealize Automation](#) per informazioni sulle versioni supportate.
- Il livello di dettaglio del registro Ansible deve essere impostato sul valore predefinito pari a zero.

- L'utente deve disporre dell'accesso in lettura/scrittura alla directory in cui si trova il file di inventario di Ansible. L'utente deve inoltre disporre dell'accesso in lettura/scrittura al file di inventario, se esiste già.

- Se si utilizza un utente non root con l'opzione sudo, assicurarsi che nel file sudoers sia impostato quanto segue:

```
Defaults:user_name !requiretty
```

e

```
username ALL=(ALL) NOPASSWD: ALL
```

- Verificare che il controllo della chiave host sia disattivato impostando `host_key_checking = False` in `/etc/ansible/ansible.cfg` o `~/.ansible.cfg`.
- Assicurarsi che la password del vault sia impostata aggiungendo la seguente riga al file `/etc/ansible/ansible.cfg` o `~/.ansible.cfg`:

```
vault_password_file = /path/to/password_file
```

Il file della password di Vault contiene la password in testo normale e viene utilizzato solo quando i modelli cloud o le distribuzioni forniscono la combinazione di nome utente e password da utilizzare tra ACM e il nodo come mostrato nell'esempio seguente.

```
echo 'myStr0ng9@88w0rd' > ~/.ansible_vault_password.txt
echo 'ANSIBLE_VAULT_PASSWORD_FILE=~/.ansible_vault_password.txt' > ~/.profile
# Instead of this way, you can also set it setting
'vault_password_file=~/.ansible_vault_password.txt' in either /etc/ansible/ansible.cfg or
~/.ansible.cfg
```

- Per evitare errori della chiave host durante il tentativo di esecuzione dei playbook, è consigliabile includere le seguenti impostazioni in `/etc/ansible/ansible config`.

```
[paramiko_connection]
record_host_keys = False

[ssh_connection]
#ssh_args = -C -o ControlMaster=auto -o ControlPersist=60s
ssh_args = -o UserKnownHostsFile=/dev/null # If you already have any
options set for ssh_args, just add the additional option shown here at the end.
```

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Fare clic su **Ansible**.
Viene visualizzata la pagina di configurazione di Ansible.
- 3 Immettere il nome host, il percorso del file di inventario e le altre informazioni necessarie per l'istanza di Ansible Open Source.
- 4 Fare clic su **Convalida** per verificare l'integrazione.

5 Fare clic su **Aggiungi**.

Risultati

Ansible è disponibile per l'uso con i modelli cloud.

Operazioni successive

Aggiungere i componenti di Ansible ai modelli cloud desiderati.

- 1 Nella pagina della tela del modello cloud, selezionare Ansible sotto l'intestazione Gestione configurazione nel menu delle opzioni del modello cloud e trascinare il componente di Ansible nella tela.
- 2 Utilizzare il pannello a destra per configurare le proprietà di Ansible appropriate, ad esempio specificando i playbook da eseguire.

In Ansible, gli utenti possono assegnare una variabile a un singolo host, quindi utilizzarla in un secondo momento nei playbook. L'integrazione di Ansible Open Source consente di specificare queste variabili host nei modelli cloud. La proprietà `hostVariables` deve essere in formato YAML corretto, come previsto dalla macchina di controllo Ansible, e questo contenuto verrà collocato nella seguente posizione:

```
parent_directory_of_inventory_file/host_vars/host_ip_address/vra_user_host_vars.yml
```

La posizione predefinita del file di inventario di Ansible è definita nell'account Ansible aggiunto nella pagina Integrazioni in Cloud Assembly. L'integrazione di Ansible non convaliderà la sintassi YAML `hostVariable` nel modello cloud, ma la macchina di controllo Ansible genererà un errore quando si esegue un playbook in caso di formattazione o sintassi non corretta.

Il seguente frammento di codice YAML del modello cloud mostra un esempio di utilizzo della proprietà `hostVariables`.

```
Cloud_Ansible_1:
  type: Cloud.Ansible
  properties:
    host: '${resource.AnsibleLinuxVM.*}'
    osType: linux
    account: ansible-CAVA
    username: ${input.username}
    password: ${input.password}
    maxConnectionRetries: 20
    groups:
      - linux_vms
    playbooks:
      provision:
        - /root/ansible-playbooks/install_web_server.yml
    hostVariables: |
      message: Hello ${env.requestedBy}
      project: ${env.projectName}
```

Le integrazioni di Ansible prevedono che le credenziali di autenticazione siano presenti in un modello cloud in uno dei modi seguenti:

- Nome utente e password nella risorsa Ansible.
- Nome utente e file di chiave privata nella risorsa Ansible.
- Nome utente nella risorsa Ansible e chiave privata nella risorsa di elaborazione specificando `remoteAccess` in `generatedPublicPrivateKey`.

Quando si crea un'integrazione di Ansible Open Source, è necessario fornire le informazioni di accesso per consentire all'utente dell'integrazione di connettersi alla macchina di controllo Ansible utilizzando SSH. Per eseguire i playbook con un'integrazione, è possibile specificare un altro utente nel codice YAML di integrazione. La proprietà `username` è obbligatoria e necessaria per connettersi alla macchina virtuale in cui Ansible apporta modifiche. La proprietà `playbookRunUsername` è facoltativa e può essere fornita per eseguire il playbook nel nodo Ansible. Il valore predefinito di `playbookRunUsername` è il nome utente di integrazione dell'endpoint Ansible.

Se si specifica un altro utente, tale utente deve disporre dell'accesso in scrittura al file `host` di Ansible e deve disporre dell'autorizzazione per la creazione di file di chiavi private.

Quando si aggiunge un riquadro Ansible Open Source a un modello cloud, vRealize Automation crea la voce dell'host per la macchina virtuale collegata. Per impostazione predefinita, vRealize Automation utilizza il nome della risorsa della macchina virtuale per creare la voce dell'host, ma è possibile specificare qualsiasi nome utilizzando la proprietà `hostName` nel codice YAML del blueprint. Per comunicare con la macchina, vRealize Automation creerà la variabile `host ansible_host: IP Address` per la voce dell'host. È possibile ignorare il comportamento predefinito per configurare la comunicazione utilizzando il nome di dominio completo, specificando la parola chiave `ansible_host` in `hostVariables` e fornendo il nome di dominio completo come valore. Il seguente frammento di codice YAML mostra un esempio di come è possibile configurare la comunicazione del nome host e del nome di dominio completo:

```
Cloud_Ansible:
  type: Cloud Ansible
  properties:
    osType: linux
    username: ubuntu
  groups:
    - sample
  hostName: resource name
  host: name of host
  account: name of account
  hostVariables:
    ansible_host: Host FQDN
```

In questo esempio si sovrascrive il valore `ansible_host` predefinito fornendo il nome di dominio completo. Questo può essere utile per gli utenti che desiderano che Ansible Open Source si connetta alla macchina host utilizzando il nome di dominio completo.

Il valore predefinito di `hostVariables` nel codice YAML sarà `ansible_host:IP_address` e l'indirizzo IP viene utilizzato per comunicare con il server.

Se la proprietà `count` del codice YAML è maggiore di 1 per Ansible Open Source, il nome `host` può essere mappato a qualsiasi proprietà della rispettiva macchina virtuale. L'esempio seguente mostra la mappatura per una risorsa di una macchina virtuale denominata `Ubuntu-VM` se si desidera che la relativa proprietà `address` sia mappata al nome `host`.

```
hostname: '${resource.Ubuntu-VM.address[count.index]}'
```

Nei modelli cloud, assicurarsi che il percorso del playbook Ansible sia accessibile all'utente specificato nell'account di integrazione. È possibile utilizzare un percorso assoluto per specificare la posizione del playbook, ma non è necessario. È consigliabile un percorso assoluto per la cartella principale dell'utente in modo che il percorso rimanga valido anche se le credenziali di integrazione di Ansible cambiano nel tempo.

Configurazione dell'integrazione di Ansible Tower in Cloud Assembly

È possibile integrare Ansible Tower con Cloud Assembly per supportare la gestione della configurazione delle risorse distribuite. Dopo aver configurato l'integrazione, è possibile aggiungere i componenti virtuali di Ansible Tower a distribuzioni nuove o esistenti dall'editor di modelli cloud.

Prerequisiti

- Concedere agli utenti non amministratori le autorizzazioni appropriate per accedere ad Ansible Tower. Sono disponibili due opzioni che sono compatibili con la maggior parte delle configurazioni. Scegliere quella più appropriata per la propria configurazione.
 - Concedere all'amministratore dell'inventario e all'amministratore dei modelli di processo ruoli a livello di organizzazione.
 - Concedere agli utenti l'autorizzazione di amministratore per un particolare inventario e il ruolo Esegui per tutti i modelli di processo utilizzati per il provisioning.
- È necessario configurare le credenziali e i modelli appropriati in Ansible Tower per l'utilizzo con le distribuzioni. I modelli possono essere modelli di processo o modelli di workflow. I modelli di processo definiscono l'inventario e il playbook da utilizzare con una distribuzione. Esiste una mappatura 1:1 tra un modello di processo e un playbook. I playbook utilizzano una sintassi simile a YAML per definire le attività associate al modello. Per la maggior parte delle distribuzioni tipiche, utilizzare le credenziali della macchina per l'autenticazione.

I modelli di workflow consentono agli utenti di creare sequenze composte da una combinazione qualsiasi di modelli di processo, sincronizzazioni di progetti e sincronizzazioni di inventario collegate tra loro in modo che sia possibile eseguirle come singola unità. Il visualizzatore di workflow di Ansible Tower consente agli utenti di progettare modelli di workflow. Per la maggior parte delle distribuzioni tipiche, è possibile utilizzare le credenziali della macchina per l'autenticazione.

- a Accedere ad Ansible Tower e passare alla sezione Modelli.
- b Selezionare Aggiunta di un nuovo modello di processo.
 - Selezionare le credenziali già create. Queste sono le credenziali della macchina che deve essere gestita da Ansible Tower. Per ogni modello di processo, può essere presente un solo oggetto credenziali.
 - Per la selezione del limite, selezionare Richiedi all'avvio. In questo modo, il modello di processo viene eseguito in base al nodo sottoposto a provisioning o a deprovisioning da Cloud Assembly. Se questa opzione non è selezionata, viene visualizzato un errore di limite non impostato quando viene distribuito il blueprint che contiene il modello di processo.
- c Selezionare Aggiunta di un nuovo modello di workflow.
 - Selezionare le credenziali già create e quindi definire l'inventario. Utilizzando il visualizzatore di workflow, progettare il modello di workflow.

Nella casella Limite dei modelli di processo o workflow è in genere possibile selezionare Richiedi all'avvio. In questo modo, il modello di processo o workflow viene eseguito in base al nodo sottoposto a provisioning o a deprovisioning da Cloud Assembly.

- È possibile visualizzare l'esecuzione dei modelli di processo o dei modelli di workflow richiamati da Cloud Assembly nella scheda Processi di Ansible Tower.

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Fare clic su Ansible Tower.
Viene visualizzata la pagina di configurazione di Ansible.
- 3 Immettere il **nome host**, che può essere un indirizzo IP e le altre informazioni necessarie per l'istanza di Ansible Tower.
- 4 Immettere il **nome utente** e la **password** dell'autenticazione basata sull'interfaccia utente per l'istanza di Ansible Tower applicabile.
- 5 Fare clic su **Convalida** per verificare l'integrazione.
- 6 Digitare un **nome** e una **descrizione** appropriati per l'integrazione.
- 7 Fare clic su **Aggiungi**.

Risultati

Ansible Tower è disponibile per l'uso nei modelli cloud.

Operazioni successive

Aggiungere i componenti di Ansible Tower ai modelli cloud desiderati. È necessario specificare il modello di processo applicabile con l'autorizzazione di esecuzione per l'utente specificato nell'account di integrazione.

- 1 Nella pagina della tela del modello cloud, selezionare Ansible sotto l'intestazione Gestione configurazione nel menu delle opzioni del blueprint e trascinare il componente di Ansible Tower nella tela.
- 2 Utilizzare il pannello a destra per configurare le proprietà di Ansible Tower appropriate, ad esempio i modelli di processo.

Quando si aggiunge un riquadro Ansible Tower a un modello cloud, vRealize Automation crea la voce dell'host per la macchina virtuale collegata in Ansible Tower. Per impostazione predefinita, vRealize Automation utilizza il nome della risorsa della macchina virtuale per creare la voce dell'host, ma è possibile specificare qualsiasi nome utilizzando la proprietà `hostName` nel codice YAML del blueprint. Per comunicare con la macchina, vRealize Automation creerà la variabile host `ansible_host: IP Address` per la voce dell'host. È possibile ignorare il comportamento predefinito per configurare la comunicazione utilizzando il nome di dominio completo, specificando la parola chiave `ansible_host` in `hostVariables` e fornendo il nome di dominio completo come valore. Il seguente frammento di codice YAML mostra un esempio di come è possibile configurare la comunicazione del nome host e del nome di dominio completo:

```
Cloud_Ansible_Tower_1:
  type: Cloud Ansible Tower
  properties:
    host: name of host
    account: name of account
    hostName: resource name
    hostVariables:
      ansible_host:Host FQDN
```

In questo esempio si sovrascrive il valore `ansible_host` predefinito fornendo il nome di dominio completo. Questo può essere utile per gli utenti che desiderano che Ansible Tower si connetta alla macchina host utilizzando il nome di dominio completo.

Il valore predefinito di `hostVariables` nel codice YAML sarà `ansible_host:IP_address` e l'indirizzo IP viene utilizzato per comunicare con il server.

Se la proprietà `count` del codice YAML è maggiore di 1 per Ansible Tower, il nome `host` può essere mappato a qualsiasi proprietà della rispettiva macchina virtuale. L'esempio seguente mostra la mappatura per una risorsa di una macchina virtuale denominata `Ubuntu-VM` se si desidera che la relativa proprietà `address` sia mappata al nome `host`.

```
hostname: '${resource.Ubuntu-VM.address[count.index]}'
```

Quando si aggiunge un componente Ansible Tower a un modello cloud, è possibile il modello di processo da richiamare nel codice YAML del modello cloud. È inoltre possibile specificare i modelli di workflow o una combinazione di modelli di processo e modelli di workflow. Se non si specifica il tipo di modello, per impostazione predefinita vRealize Automation presuppone che venga richiamato un modello di processo.

Il seguente frammento di codice YAML illustra un esempio di come è possibile richiamare una combinazione di modelli di processo e workflow in un modello cloud di Ansible Tower.

```
Cloud_Ansible_1:
  type: Cloud.Ansible.Tower
  properties:
    host: '${resource.CentOS_Machine.*}'
    account:
    maxConnectionRetries: 2
    maxJobRetries: 2
  templates:
    provision:
      - name: My workflow
        type: workflow
      - name: My job template
```

Sono stati aggiunti `maxConnectionsRetries` e `maxJobRetries` per gestire gli errori relativi ad Ansible. I modelli cloud accettano il valore personalizzato e, nel caso non venga specificato alcun valore, utilizzano il valore predefinito. Per `maxConnectionRetries`, il valore predefinito è 10, mentre per `maxJobRetries` è 3.

Nota Le versioni precedenti di vRealize Automation supportavano l'esecuzione dei modelli di processo utilizzando solo lo schema `jobTemplate` nel modello cloud. `jobTemplate` è ora obsoleto e potrebbe essere rimosso nelle versioni future. Per il momento, l'utilizzo della proprietà `jobTemplate` continuerà a funzionare come previsto. Per eseguire modelli di workflow e utilizzare le funzionalità aggiuntive, è consigliabile utilizzare lo schema dei modelli.

I modelli cloud di Cloud Assembly per le integrazioni di Ansible Tower includono la proprietà `useDefaultLimit` con un valore `true` o `false` per definire la posizione di esecuzione dei modelli di Ansible. I modelli di Ansible possono essere modelli di processo o modelli di workflow. Se questo valore è impostato su `true`, i modelli specificati vengono eseguiti per la macchina specificata nella casella Limite della pagina dei modelli di Ansible. Se il valore è impostato su `false`, i modelli

vengono eseguiti per la macchina sottoposta a provisioning, ma gli utenti devono selezionare la casella di controllo Richiedi all'avvio nella pagina dei modelli di Ansible Tower. Per impostazione predefinita, il valore di questa proprietà è `false`. Il seguente esempio di codice YAML illustra come viene visualizzata la proprietà `useDefaultLimit` nei modelli cloud.

```
templates:
  provision:
    - name: ping aws_credentials
      type: job
      useDefaultLimit: false
      extraVars: '{"rubiconSurveyJob" : "checkSurvey"}'
```

Inoltre, come illustrato nell'esempio precedente, è possibile utilizzare la proprietà `extraVars` per specificare variabili aggiuntive o variabili di sondaggio. Questa funzionalità può essere utile per l'esecuzione di modelli che richiedono input. Se un utente mantiene la variabile di sondaggio, è necessario passare la variabile nella sezione `extraVars` del modello cloud per evitare errori.

Creazione di un'integrazione di SaltStack Config in vRealize Automation

È possibile creare un'integrazione di SaltStack Config per accedere al servizio SaltStack Config e utilizzare gli oggetti e le azioni di SaltStack Config in vRealize Automation.

Con vRealize Automation SaltStack Config, è possibile eseguire il provisioning, configurare e distribuire software alle macchine virtuali su qualsiasi scala, utilizzando l'automazione basata su eventi. È inoltre possibile utilizzare SaltStack Config per definire e applicare gli stati del software ottimali e conformi nell'intero ambiente.

Installazione

Prima di integrare SaltStack Config con vRealize Automation, è necessario installarlo nel proprio ambiente. Per ulteriori informazioni, vedere [Installazione e configurazione di SaltStack Config](#).

Considerazioni

vRealize Automation SaltStack Config integrato è disponibile per vRealize Automation con le seguenti condizioni:

- L'integrazione di SaltStack Config viene associata a un host specifico durante l'installazione.
- vRealize Automation al momento non supporta la multi-tenancy per SaltStack Config.
- Il tenant di vRealize Automation può supportare un'integrazione di SaltStack Config e un Salt Master. Salt Master può supportare più minion.
- Prima di poter eliminare un'integrazione di SaltStack Config in vRealize Automation, è necessario eliminare tutte le distribuzioni esistenti che utilizzano l'integrazione di SaltStack Config.

Prerequisiti

- Verificare di disporre delle credenziali di amministratore di vRealize Automation e delle credenziali di amministratore di SaltStack Config (accesso a livello root).

Sono necessarie le credenziali di amministratore di vRealize Automation e le credenziali di amministratore di SaltStack Config (accesso a livello root) per creare un'integrazione di SaltStack Config.

Sono inoltre necessarie le credenziali di amministratore di SaltStack Config per aprire e utilizzare il servizio SaltStack Config stesso.

È necessario utilizzare le credenziali di vRealize Automation per accedere a vRealize Automation e le credenziali di SaltStack Config per accedere a SaltStack Config.

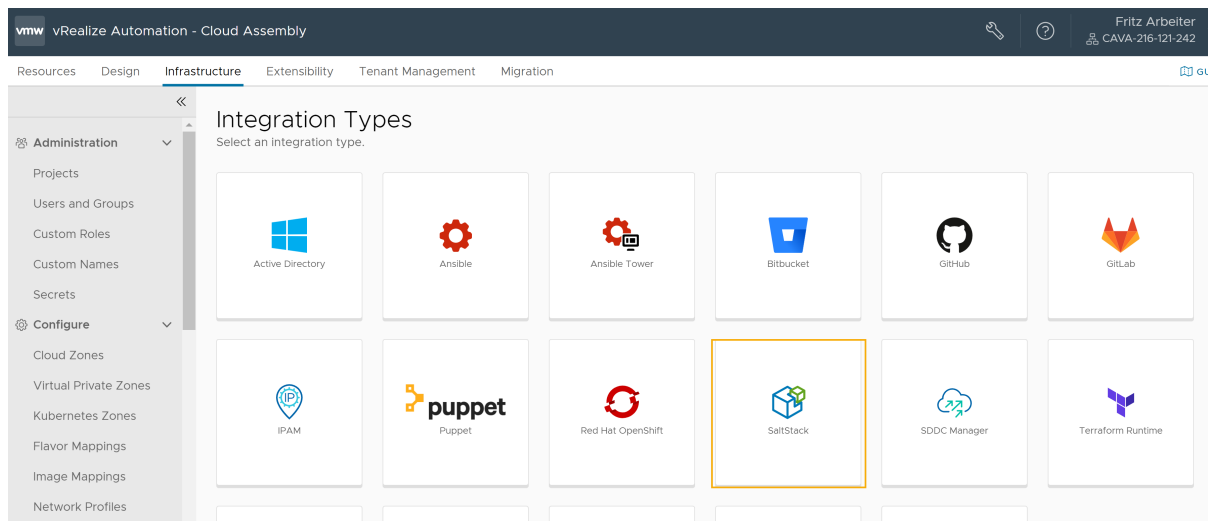
Per informazioni sulle credenziali di amministratore di SaltStack Config, vedere la guida [Installazione e configurazione di SaltStack Config](#).

- Verificare che il servizio SaltStack Config sia installato.
- Verificare che l'istanza di Salt Master da utilizzare nell'integrazione di SaltStack Config contenga il plug-in Master.
- Verificare di disporre del ruolo di amministratore del servizio SaltStack Config in vRealize Automation. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre del ruolo di amministratore del servizio Cloud Assembly in vRealize Automation. Vedere [Ruoli utente di organizzazione e servizio in vRealize Automation](#).

Configurazione di un'integrazione di SaltStack Config in vRealize Automation

Dopo aver installato SaltStack Config per vRealize Automation, è possibile configurare l'integrazione in Cloud Assembly.

- 1 In Cloud Assembly, selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare il tipo di integrazione SaltStack Config.



3 Compilare il modulo.

The screenshot shows the 'New Integration' form in the vRealize Automation - Cloud Assembly interface. The form is titled 'New Integration' and includes the following fields:

- Name ***: A text input field.
- Description**: A text input field.
- SaltStack Integration**: A section header.
- Hostname ***: A text input field with an information icon.
- Running environment**: A text input field with a search icon and the text 'Search for running environment'.
- Username ***: A text input field.
- Password ***: A text input field.

Below the Password field is a **VALIDATE** button. At the bottom of the form are **ADD** and **CANCEL** buttons. The left sidebar shows a navigation menu with categories like Terraform Versions, Tags, Onboarding, Resources, Compute, Networks, Security, Storage, Kubernetes, Activity, Requests, Events Log, Connections, Cloud Accounts, and Integrations.

- Immettere un nome per l'integrazione.
- Facoltativamente, specificare una descrizione per l'integrazione.
- Immettere il nome host per il server SaltStack Config.
- Specificare l'ambiente in esecuzione per l'integrazione di SaltStack Config.

Se si utilizza la proprietà `saltConfiguration` per distribuire i minion e applicare file di stato nelle macchine virtuali, non è necessario configurare un ambiente in esecuzione. Tuttavia, è consigliabile aggiornare i modelli cloud in modo che utilizzino la risorsa SaltStack Config. La proprietà `saltConfiguration` verrà tuttavia deprecata in una versione futura.

Se si utilizza la risorsa SaltStack Config per distribuire i minion e applicare file di stato nelle macchine virtuali, selezionare l'ambiente in esecuzione **embedded-ABX-onprem**.

- Immettere il nome utente e la password dell'amministratore di SaltStack Config utilizzati per accedere all'host specificato.
- Fare clic su **Convalida** per verificare l'accesso dell'amministratore all'host dell'integrazione di SaltStack Config.

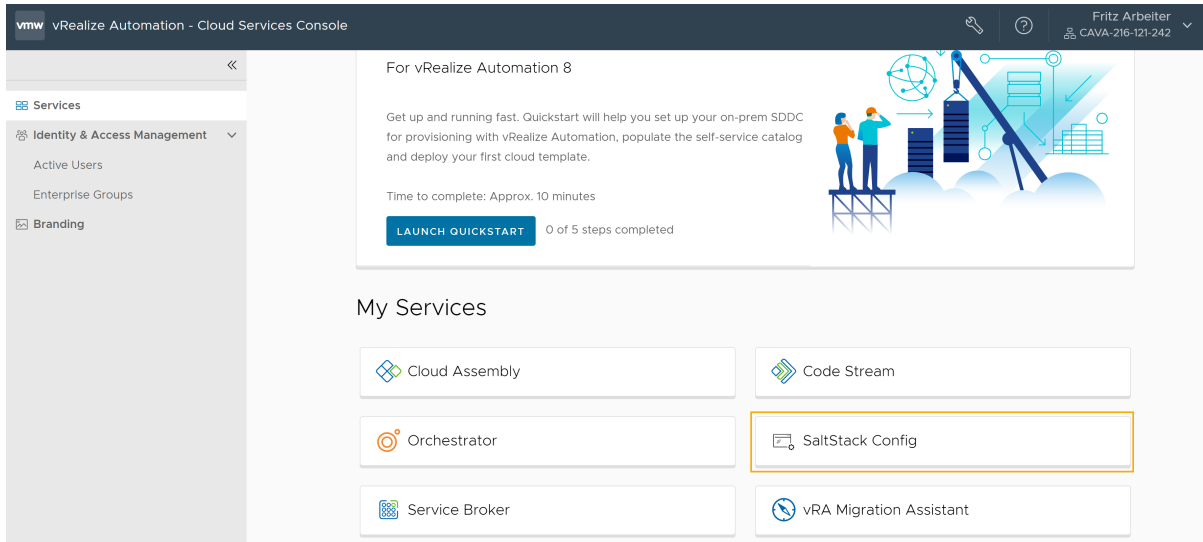
Se la convalida non riesce, assicurarsi di aver immesso il nome host, il nome utente e la password corretti.

- Fare clic su **Salva**.

Accesso all'integrazione di SaltStack Config

Dopo aver salvato il punto di integrazione di SaltStack Config, è possibile aprire il servizio di integrazione di SaltStack Config.

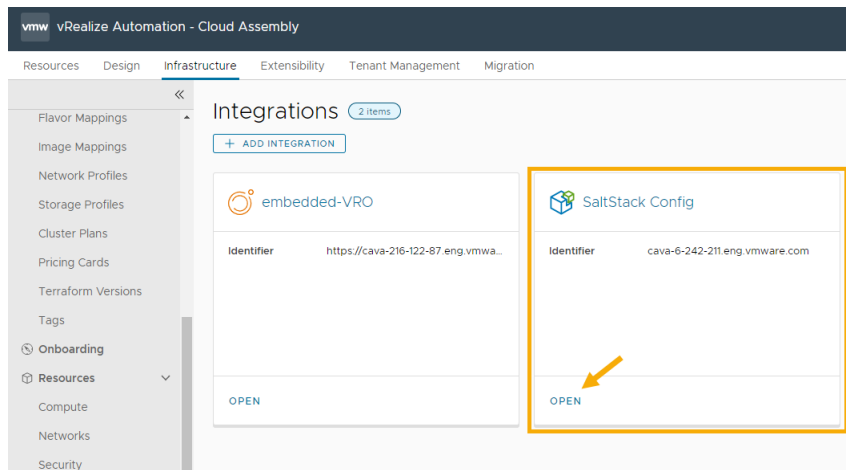
- 1 Se SaltStack Config è distribuito tramite vRealize Suite Lifecycle Manager, è possibile fare clic sul riquadro del servizio dalla console del servizio vRealize Automation per aprire l'integrazione e accedere all'host.



Se si esegue un'installazione autonoma di SaltStack Config, è possibile accedere al servizio utilizzando il nome host di SaltStack Config.

- 2 Quando viene richiesto di accedere a SaltStack Config, immettere il nome utente e la password dell'amministratore di SaltStack Config.

Se è necessario apportare modifiche all'integrazione, selezionare **Infrastruttura > Connessioni > Integrazioni**, selezionare il riquadro dell'integrazione di SaltStack Config disponibile e fare clic su **Apri**.



Il nome host non può essere modificato dopo aver configurato l'integrazione. È possibile modificare solo il nome, la descrizione, l'ambiente in esecuzione e le credenziali per l'integrazione.

The screenshot shows the vRealize Automation - Cloud Assembly interface. The top navigation bar includes tabs for Resources, Design, Infrastructure (selected), Extensibility, Tenant Management, and Migration. A left sidebar contains a tree view with categories like Terraform Versions, Tags, Onboarding, Resources, Compute, Networks, Security, Storage, Kubernetes, Activity, Requests, Events Log, Connections, Cloud Accounts, and Integrations. The main content area displays the 'SaltStack Config' configuration page. It includes a 'Name' field with the value 'SaltStack Config', a 'Description' field, and a 'SaltStack Integration' section with fields for 'Hostname' (cava-6-242-211.eng.vmware.com), 'Running environment' (Q embedded-ABX-onprem), 'Username' (root), and 'Password'. There is a 'VALIDATE' button and a warning message: 'Validate credentials before making changes.' At the bottom are 'SAVE' and 'CANCEL' buttons.

Informazioni sull'utilizzo di SaltStack Config

SaltStack Config è un prodotto autonomo che è possibile integrare con e utilizzare in vRealize Automation.

- Informazioni su come aggiungere [la risorsa SaltStack Config](#) per installare minion nelle macchine virtuali nelle distribuzioni di Cloud Assembly.
- Informazioni su come [distribuire i minion utilizzando l'API \(RaaS\)](#) in un ambiente Linux o Windows.

Come creare un'integrazione di Active Directory in Cloud Assembly

Cloud Assembly supporta l'integrazione con i server di Active Directory per fornire la possibilità di creare account di computer in un'unità organizzativa specifica all'interno di un server di Active Directory prima di eseguire il provisioning di una macchina virtuale. Active Directory supporta una connessione LDAP al server di Active Directory.

Un criterio di Active Directory associato a un progetto viene applicato a tutte le macchine virtuali sottoposte a provisioning nell'ambito di tale progetto. Gli utenti possono specificare uno o più tag per applicare selettivamente il criterio alle macchine virtuali di cui viene eseguito il provisioning nelle zone cloud con tag di funzionalità corrispondenti.

Per le distribuzioni in locale, l'integrazione di Active Directory consente di configurare una funzionalità di controllo dello stato che mostra lo stato dell'integrazione e l'integrazione di ABX sottostante su cui si basa, incluso il proxy di estendibilità del cloud necessario. Prima di applicare un criterio di Active Directory, Cloud Assembly controlla lo stato delle integrazioni sottostanti. Se l'integrazione è integra, Cloud Assembly crea gli oggetti computer distribuiti nell'istanza di Active Directory specificata. Se l'integrazione non è integra, l'operazione di distribuzione ignora la fase di Active Directory durante il provisioning.

Prerequisiti

- L'integrazione di Active Directory richiede una connessione LDAP al server di Active Directory.
- Se si sta configurando l'integrazione di Active Directory con vCenter in locale, è necessario configurare un'integrazione di ABX con un proxy di estendibilità del cloud. Selezionare **Estendibilità > Attività > Integrazioni** e scegliere **Azioni di estendibilità locali**.
- Se si sta configurando un'integrazione con Active Directory nel cloud, è necessario disporre di un account Microsoft Azure o Amazon Web Services.
- È necessario disporre di un progetto configurato con zone cloud appropriate e mappature di immagini e caratteristiche da utilizzare con l'integrazione di Active Directory.
- L'unità organizzativa desiderata nell'istanza di Active Directory deve essere già stata creata prima di associare l'integrazione di Active Directory a un progetto.

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Nuova integrazione**.
- 2 Fare clic su **Active Directory**.
- 3 Nella scheda **Riepilogo**, immettere i nomi dell'host e dell'ambiente LDAP appropriati.
L'host LDAP specificato viene utilizzato per convalidare l'integrazione di Active Directory e viene utilizzato anche per le distribuzioni successive se non vengono specificati e richiamati host alternativi a causa di errori o indisponibilità.
- 4 Immettere il nome e la password del server LDAP.
- 5 Immettere il DN di base appropriato che specifica la radice per le risorse di Active Directory desiderate.

Nota È possibile specificare un solo DN per ogni integrazione di Active Directory.

- 6 Fare clic su **Convalida** per verificare che l'integrazione funzioni.
- 7 Immettere un nome e una descrizione per questa integrazione.
- 8 Fare clic su **Salva**.

- 9 Fare clic sulla scheda **Progetto** per aggiungere un progetto all'integrazione di Active Directory.

Nella finestra di dialogo **Aggiungi progetti**, è necessario selezionare un nome di progetto e un DN relativo, ovvero un DN esistente all'interno del DN di base specificato nella scheda Riepilogo.

- 10 Sotto la selezione Opzioni estese, fornire un elenco separato da virgole di **Host alternativi** che verranno utilizzati se il server selezionato inizialmente non è disponibile durante la distribuzione. Il server primario viene sempre utilizzato per la convalida iniziale dell'integrazione.

Nota Se il formato dell'host primario è LDAP, LDAPS non è supportato per gli host alternativi.

- 11 Immettere il tempo di attesa in secondi per la risposta del server iniziale prima di provare un server alternativo nella casella **Timeout connessione**.

- 12 Fare clic su **Salva**.

Risultati

È ora possibile associare il progetto con l'integrazione di Active Directory a un modello cloud. Quando viene eseguito il provisioning di una macchina utilizzando questo modello cloud, ne viene eseguito lo staging preventivo nell'istanza di Active Directory e nell'unità organizzativa specificate.

Inizialmente, le integrazioni di Active Directory vengono distribuite in un'unità organizzativa predefinita con limitazioni minime per l'utente. L'unità organizzativa viene configurata per impostazione predefinita quando si mappa un'integrazione di Active Directory a un progetto. È possibile aggiungere una proprietà denominata `FinalRelativeDN` ai blueprint per modificare l'unità organizzativa per le distribuzioni di Active Directory. Questa proprietà consente di specificare l'unità organizzativa da utilizzare con una distribuzione di Active Directory.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: CenOS8
      flavor: tiny
      activeDirectory:
        finalRelativeDN: ou=test
        securityGroup: TestSecurityGroup
```

Come illustrato nell'esempio YAML precedente, gli utenti possono aggiungere una proprietà a una distribuzione dell'integrazione di Active Directory che aggiunge un account computer al gruppo di sicurezza in modo che vengano assegnate le autorizzazioni appropriate per accedere alla risorsa condivisa in una rete. La macchina virtuale Active Directory viene inizialmente distribuita in un'unità organizzativa fissa, ma quando la macchina è pronta per il rilascio, viene spostata in un'altra unità organizzativa con il criterio appropriato applicabile per gli utenti.

Se un account computer viene spostato in un'unità organizzativa diversa dopo la distribuzione, Cloud Assembly tenta di eliminare gli account nell'unità organizzativa iniziale. L'eliminazione degli account computer viene eseguita solo nel caso di macchine virtuali spostate in un'altra unità organizzativa all'interno dello stesso dominio.

È inoltre possibile implementare un controllo dello stato basato su tag per le integrazioni di Active Directory in locale come indicato di seguito.

- 1 Creare un'integrazione di Active Directory come descritto nei passaggi precedenti.
- 2 Fare clic sulla scheda **Progetto** per aggiungere un progetto all'integrazione di Active Directory.
- 3 Selezionare un nome di progetto e un DN relativo nella finestra di dialogo Aggiungi progetti. Il DN relativo deve esistere all'interno del DN di base specificato.

In questa finestra di dialogo sono presenti due commutatori che consentono di controllare la configurazione di Active Directory dai modelli cloud. Entrambi i commutatori sono disattivati per impostazione predefinita.

- **Sostituisci:** questo commutatore consente di sostituire le proprietà di Active Directory, in modo specifico il DN relativo nei modelli cloud. Quando attivato, è possibile modificare l'unità organizzativa specificata nella proprietà `relativeDN` nel modello cloud. Una volta sottoposta a provisioning, la macchina verrà aggiunta all'unità organizzativa specificata nella proprietà `relativeDN` nel modello cloud. L'esempio seguente mostra la gerarchia di modelli cloud in cui viene visualizzata questa proprietà.

```
activeDirectory:
  relativeDN: OU=ad_integration_machine_override
```

- **Ignora:** questa opzione consente di ignorare la configurazione di Active Directory per il progetto. Quando attivata, aggiunge una proprietà al modello cloud denominato `ignoreActiveDirectory` per la macchina virtuale associata. Quando questa proprietà è impostata su `true` significa che la macchina non viene aggiunta ad Active Directory durante la distribuzione.
- 4 Aggiungere i tag appropriati. Questi tag sono applicabili alla zona cloud in cui può essere applicato il criterio di Active Directory.
 - 5 Fare clic su Salva.

Lo stato dell'integrazione di Active Directory viene visualizzato per ogni integrazione nella pagina **Infrastruttura > Connessioni > Integrazioni** in Cloud Assembly.

È possibile associare il progetto con l'integrazione di Active Directory a un modello cloud. Quando viene eseguito il provisioning di una macchina utilizzando questo modello, tale macchina viene preinstallata nell'unità organizzativa e nell'istanza di Active Directory specificate.

Configurazione di un'integrazione di VMware SDDC Manager

È possibile aggiungere un'integrazione di VMware SDDC Manager in vRealize Automation per semplificare l'utilizzo dei domini del carico di lavoro come parte degli account cloud di VMware Cloud Foundation (VCF) in vRealize Automation.

Prerequisiti

- vRealize Automation supporta l'integrazione solo con VMware SDDC Manager 4.1 e versioni successive.

Procedura

- 1 Selezionare **Infrastruttura > Connessioni > Integrazioni** e fare clic su **Aggiungi integrazione**.
- 2 Selezionare SDDC Manager.

Viene visualizzata la pagina di configurazione dell'integrazione di SDDC Manager.

- 3 Nella sezione Riepilogo, immettere un **Nome** e una **Descrizione** per l'integrazione.
- 4 Nella sezione Credenziali SDDC Manager, immettere l'**Indirizzo IP/FQDN di SDDC Manager** per la macchina del server SDDC Manager.
- 5 Immettere il nome utente e la password per l'account amministratore da utilizzare per connettersi inizialmente a SDDC Manager. È consigliabile evitare di utilizzare l'account amministratore per la connessione. Utilizzare un account diverso che disponga di privilegi di amministratore in SDDC Manager per creare ruoli di servizio.

Queste credenziali vengono utilizzate per impostare inizialmente la connessione a SDDC Manager, quindi vengono create le credenziali del servizio da utilizzare durante la connessione da un account cloud di VCF.

- 6 Fare clic su **Convalida** per verificare la connessione a SDDC Manager.
- 7 Fare clic su **Aggiungi**.

Risultati

Dopo aver creato l'integrazione, è possibile visualizzare i carichi di lavoro associati a SDDC nella scheda Dominio carico di lavoro visualizzata nella pagina dell'integrazione completata. Inoltre, è possibile visualizzare e selezionare i carichi di lavoro associati all'integrazione e quindi fare clic sul pulsante **Aggiungi account cloud** per aprire una pagina per la creazione di un account cloud di VCF che utilizzerà il carico di lavoro selezionato.

Operazioni successive

Dopo aver configurato l'account cloud di VCF, nella parte superiore della pagina viene visualizzato un pulsante **Configura cloud**. Fare clic su questo pulsante per avviare la configurazione guidata del cloud di VCF.

Integrazione con vRealize Operations Manager

vRealize Automation può utilizzare vRealize Operations Manager per eseguire il posizionamento avanzato dei carichi di lavoro, fornire metriche relative all'integrità della distribuzione e macchine virtuali e visualizzare i prezzi.

Numero e tipo di integrazioni

L'integrazione tra i due prodotti dev'essere da locale a locale, non una combinazione di locale e cloud.

È possibile integrare un'istanza di vRealize Automation con più istanze di vRealize Operations Manager, ma un'istanza di vRealize Operations Manager può essere connessa solo a un'istanza di vRealize Automation.

Non è possibile connettere un cluster di vRealize Operations Manager aggregato a vRealize Automation.

Requisiti di base per l'integrazione

Per eseguire l'integrazione con vRealize Operations Manager, passare a **Infrastruttura > Connessioni > Integrazioni**. Per aggiungere l'integrazione, sono necessari l'URL di vRealize Operations Manager e le credenziali dell'account di accesso descritti nella sezione successiva. Inoltre, vRealize Automation e vRealize Operations Manager devono gestire lo stesso endpoint vSphere.

Account di accesso per l'integrazione

In vRealize Operations Manager, è necessario un account di accesso vRealize Operations Manager locale o non locale per l'integrazione da utilizzare. L'account richiede privilegi di sola lettura per l'istanza dell'adattatore di vCenter per l'endpoint vSphere. Si noti che potrebbe essere necessario importare un account non locale in vRealize Operations Manager, con il relativo ruolo di sola lettura assegnato. Per l'integrazione, il formato del nome utente per l'accesso di un account non locale è *username@domain@authenticated-source*, ad esempio *jdoe@company.com@workspaceone*. Le origini autenticate vengono definite durante la configurazione iniziale del server di vRealize Operations Manager.

Per dettagli, vedere le seguenti sezioni. Per informazioni sui prezzi, vedere [Come utilizzare le schede dei prezzi in vRealize Automation](#).

Posizionamento avanzato dei carichi di lavoro tramite vRealize Operations Manager

vRealize Automation e vRealize Operations Manager possono collaborare per posizionare i carichi di lavoro della distribuzione in modo ottimale.

È possibile selezionare il posizionamento dei carichi di lavoro al livello di zona cloud basata su vSphere. Solo i cluster abilitati per Distributed Resource Scheduler (DRS) di una zona cloud sono idonei per il posizionamento avanzato con vRealize Operations Manager.

- **Posizionamento di vRealize Automation:** il motore di posizionamento di vRealize Automation è basato sullo scopo dell'applicazione. Considera i vincoli basati su tag, l'appartenenza al progetto e le zone cloud associate, oltre ai filtri di affinità correlati alla rete, allo storage e all'elaborazione. Il posizionamento delle risorse dipende da tutti questi fattori, oltre alla presenza di altre risorse di destinazione correlate nella stessa distribuzione.
- **Posizionamento di vRealize Operations Manager:** vRealize Operations Manager considera lo scopo operativo per un posizionamento ottimale. Lo scopo operativo può tenere conto dei carichi di lavoro passati e delle previsioni what-if future.

Quando si utilizza il posizionamento avanzato dei carichi di lavoro, è necessario applicare l'assegnazione dei tag di vRealize Automation per implementare le decisioni correlate allo scopo di business, anziché utilizzare le opzioni dello scopo di business di vRealize Operations Manager.

Quando si esegue l'integrazione con vRealize Operations Manager, vRealize Automation continua a seguire il modello di scopo dell'applicazione e i relativi vincoli da filtrare per il posizionamento di destinazione. Quindi, dall'interno di tali risultati, utilizza il consiglio di vRealize Operations Manager per ottimizzare ulteriormente il posizionamento.

In assenza di un suggerimento

Se si abilita il posizionamento avanzato dei carichi di lavoro e l'analisi di vRealize Operations Manager non restituisce suggerimenti, è possibile configurare vRealize Automation affinché venga riportato all'impostazione predefinita, ovvero il posizionamento dello scopo dell'applicazione.

Limitazioni relative al posizionamento dei carichi di lavoro

Quando si utilizza vRealize Operations Manager per posizionare i carichi di lavoro, si applicano alcune limitazioni.

- vRealize Operations Manager non supporta il posizionamento di carichi di lavoro su pool di risorse in vCenter Server.
- Se vRealize Operations Manager è inattivo, il timeout utilizzato per il posizionamento dei carichi di lavoro per la chiamata a vRealize Operations Manager scade.
- Il posizionamento non attraversa più zone cloud. vRealize Automation invia una zona cloud a vRealize Operations Manager per i consigli sul posizionamento all'interno di tale zona cloud singola.

Come abilitare il posizionamento dei carichi di lavoro

Per abilitare il posizionamento dei carichi di lavoro, è necessario eseguire i passaggi necessari per vSphere, vRealize Operations Manager e vRealize Automation.

- 1 In Cloud Assembly, connettersi all'account cloud di vCenter Server.

Le opzioni si trovano in **Infrastruttura > Connessioni > Account cloud**.

- 2 In vCenter Server, verificare che i cluster con abilitazione DRS esistano e siano impostati come completamente automatizzati.

- 3 In vRealize Operations Manager, verificare che sia gestito lo stesso vCenter Server.

È necessario vRealize Operations Manager 8 o versione successiva.

- 4 In Cloud Assembly, aggiungere l'integrazione di vRealize Operations Manager.

Le opzioni si trovano in **Infrastruttura > Connessioni > Integrazioni**.

Per aggiungere l'integrazione, è necessario l'URL del nodo primario di vRealize Operations Manager indicato di seguito, oltre al nome utente e alla password di accesso.

<https://operations-manager-IP-address-or-FQDN/suite-api>

Dopo aver immesso i valori, fare clic su **Convalida**.

- 5 Sincronizzare l'integrazione con vCenter Server facendo clic su **Sincronizza**.

Eseguire inoltre la sincronizzazione ogni volta che Cloud Assembly e vRealize Operations Manager avviano la gestione di un nuovo vCenter Server.

- 6 In Cloud Assembly, creare una zona cloud per l'account vCenter Server.

Le opzioni si trovano in **Infrastruttura > Configura > Zone cloud**.

- 7 Nella scheda Riepilogo della zona cloud, impostare il criterio di posizionamento su **Avanzato**.

- 8 In Criterio di posizionamento, selezionare se deve essere ripristinato il posizionamento predefinito di vRealize Automation nel caso in cui vRealize Operations Manager non restituisca suggerimenti.

Risoluzione dei problemi relativi al posizionamento dei carichi di lavoro

Se vRealize Operations Manager non consiglia il posizionamento dei carichi di lavoro nel modo previsto, rivedere i dettagli della richiesta di distribuzione in Cloud Assembly o vRealize Automation Service Broker.

- 1 Passare a **Infrastruttura > Attività > Richieste** e fare clic sulla richiesta.

- 2 In Dettagli richiesta, esaminare le fasi di allocazione.

Cercare le destinazioni che sono state identificate correttamente o meno.

- 3 In Dettagli richiesta, in alto a destra, abilitare **Modalità sviluppo**.

- 4 Seguire il percorso della richiesta per individuare i blocchi di filtro.

5 Fare clic su un blocco di filtro ed esaminare la sezione seguente.

```
filterName: ComputePlacementPolicyAffinityHostFilter
  v computeLinksBefore
  v computeLinksAfter
  v filteredOutHostsReasons
```

Voce	Descrizione
computeLinksBefore	Elenco dei potenziali host di posizionamento in base agli algoritmi di vRealize Automation.
computeLinksAfter	Host di posizionamento selezionato.
filteredOutHostsReasons	Messaggi che descrivono il motivo per cui un host è stato selezionato o rifiutato. Quando vRealize Operations Manager seleziona l'host, viene visualizzato il seguente messaggio. advance policy filter: Filtered hosts based on recommendation from vROPS.

Ulteriori informazioni sul posizionamento dei carichi di lavoro

Per individuare l'infrastruttura migliore in cui posizionare una distribuzione, vRealize Automation prende diverse decisioni di filtraggio. L'integrazione di vRealize Automation con vRealize Operations Manager può perfezionare ulteriormente la decisione di posizionamento.

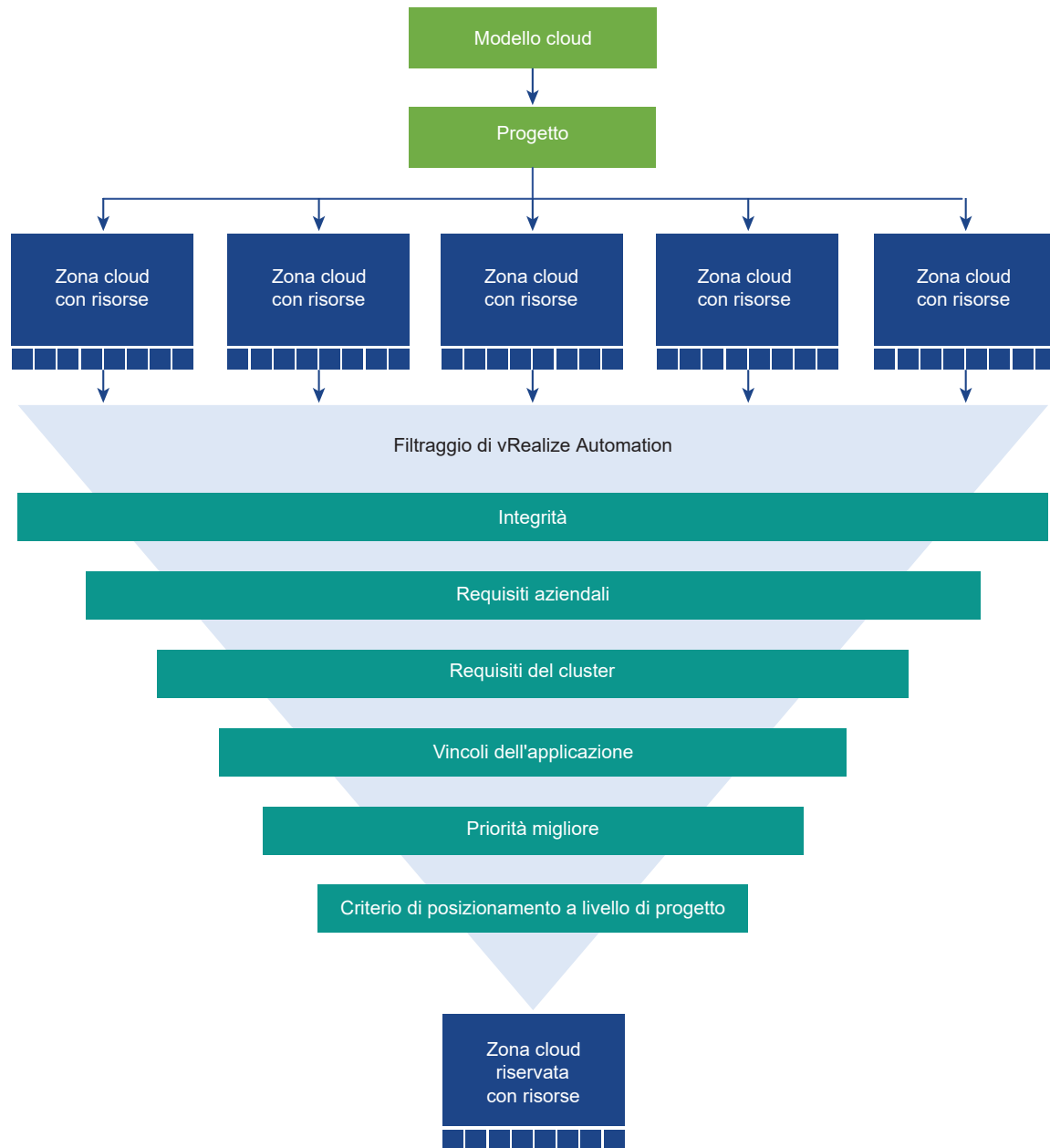
vRealize Operations Manager può contribuire a posizionare i carichi di lavoro in modo ottimale, a condizione che sia stata abilitata l'opzione Criterio di posizionamento avanzato nelle zone cloud basate su vSphere.

Inoltre, gli account cloud di vSphere per le zone cloud devono essere monitorati da vRealize Operations Manager.

Fase 1: prenotazione

Nota Anche se il nome è lo stesso, la prenotazione non è correlata alla funzionalità di prenotazione di vRealize Automation 7.

La fase di prenotazione di vRealize Automation è identica indipendentemente dal fatto che si abiliti il posizionamento avanzato con vRealize Operations Manager.



- 1 La prenotazione inizia con un modello cloud collegato a un progetto. Tale progetto è a sua volta collegato alle zone cloud.
- 2 Le zone cloud sono composte da host, pool e cluster di risorse di elaborazione e da storage collegato.
Inizialmente, qualsiasi zona cloud nel progetto potrebbe essere una potenziale destinazione di posizionamento.
- 3 vRealize Automation filtra le zone cloud che non dispongono di risorse sufficientemente integre per la distribuzione.
Ad esempio, se troppe risorse sono spente o in manutenzione, tale zona cloud viene filtrata.

- 4 vRealize Automation filtra le zone cloud che non sono in grado di soddisfare i requisiti aziendali.

Ad esempio, la distribuzione potrebbe superare un limite di prezzi o budget per la zona.

- 5 vRealize Automation filtra le zone cloud che non sono in grado di soddisfare i requisiti del cluster.

Ad esempio, le risorse della zona cloud potrebbero avere limiti di utilizzo della CPU o della memoria troppo bassi per la distribuzione.

- 6 vRealize Automation filtra le zone cloud che non hanno affinità con i vincoli dell'applicazione.

L'affinità richiede che i tag di vincolo a livello di progetto o del modello cloud corrispondano ai tag di funzionalità presenti in qualche punto delle risorse della zona cloud.

Ad esempio, se il modello cloud o il progetto include un vincolo di storage per utilizzare `pci` con tag di storage, una zona cloud in cui nessuna delle risorse di storage dispone di tale tag di funzionalità verrà filtrata.

- 7 vRealize Automation seleziona le zone cloud con la priorità di provisioning migliore.

- 8 Se il criterio di posizionamento a livello di progetto è diverso da Predefinito, vRealize Automation seleziona una zona cloud che supporta il criterio di posizionamento non predefinito.

In questa versione, Spread è l'unico criterio non predefinito. Spread distribuisce il carico selezionando la zona cloud con il rapporto più basso tra macchine virtuali e host.

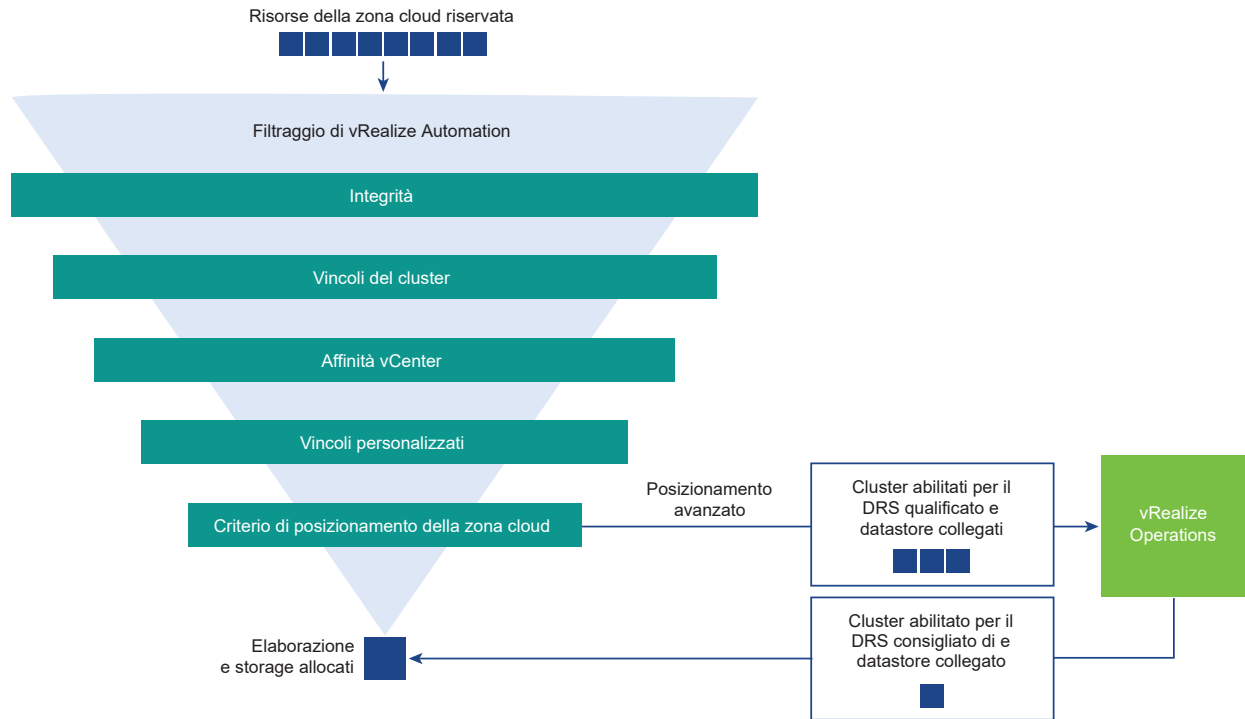
L'impostazione predefinita viene distribuita semplicemente nella prima zona disponibile.

Il criterio di posizionamento del progetto è solo un fattore durante la fase di prenotazione della zona cloud. Non ha alcun effetto né relazione con il criterio di posizionamento della zona cloud nella fase di allocazione.

Al termine, la fase di prenotazione seleziona una zona cloud e le relative risorse. vRealize Automation riserva la prima zona disponibile che resta qualificata dopo aver passato i filtri precedenti.

Fase 2: allocazione

vRealize Automation ispeziona le risorse di elaborazione della zona cloud riservata e lo storage collegato.



- 1 All'interno della zona cloud, vRealize Automation filtra le risorse che si trovano nello stato di manutenzione o spegnimento.

Si noti che vi è comunque un numero sufficiente di risorse integre per la distribuzione. In caso contrario, l'intera zona cloud sarebbe stata filtrata durante la fase di prenotazione.

- 2 vRealize Automation filtra le risorse che non corrispondono ai vincoli a livello di cluster presenti nel modello cloud o nel progetto.

Ad esempio, una risorsa nella zona cloud potrebbe essere contrassegnata con il tag `test` in **Infrastruttura > Risorse > Elaborazione**.

Se il modello cloud o il progetto include un tag di vincolo per utilizzare una risorsa `dev`, la risorsa `test` viene filtrata.

Inoltre, i profili di storage o di rete nella zona cloud potrebbero essere contrassegnati in modo da non corrispondere ai vincoli di storage o di rete a livello di cluster nel modello cloud o nel progetto.

- 3 vRealize Automation filtra le risorse in base alle impostazioni di affinità definite in vCenter.

Ad esempio, potrebbe essere presente una regola in vCenter in cui la presenza di una macchina virtuale in un cluster potrebbe impedire l'uso di un altro cluster.

- 4 vRealize Automation filtra le risorse che non corrispondono ad alcun vincolo personalizzato rimanente trovato nel modello cloud o nel progetto.

Ad esempio, se il modello cloud include un vincolo per l'utilizzo di un'immagine con tag `ubuntu`, una zona cloud in cui nessuna delle mappature dell'immagine è contrassegnata con tag `ubuntu` verrà filtrata.

- 5 vRealize Automation cerca la migliore risorsa di elaborazione e storage possibile in base al criterio di posizionamento della zona cloud.

vRealize Automation utilizza vRealize Operations Manager solo quando sono vere le due condizioni seguenti:

- Il criterio di posizionamento della zona cloud è impostato su Avanzato.
- Dopo aver applicato il filtro al passaggio 4, almeno un cluster abilitato per DRS e lo storage a cui è collegato restano qualificati.

In caso contrario, vRealize Automation procede con il proprio algoritmo di posizionamento senza input da vRealize Operations Manager.

Consiglio sul posizionamento di vRealize Operations Manager

Se qualificato per l'input da vRealize Operations Manager, vRealize Automation contatta vRealize Operations Manager per ricevere un consiglio sulla migliore risorsa di elaborazione e storage possibile per la distribuzione. vRealize Automation invia i seguenti dati a vRealize Operations Manager:

- Cluster abilitati per DRS di destinazione qualificati e relativi datastore o cluster di datastore collegati
- Il numero di risorse o le dimensioni del cluster della distribuzione
- Requisiti di CPU e memoria per le macchine virtuali nella distribuzione
- Requisiti del disco per le macchine virtuali nella distribuzione

Dalle destinazioni qualificate, se vRealize Operations Manager può restituire un posizionamento ottimale per ciascuna macchina virtuale, vRealize Automation alloca le risorse di elaborazione e storage in base al consiglio di vRealize Operations Manager.

Per ulteriori informazioni sulle modalità con cui vRealize Operations Manager gestisce i carichi di lavoro, vedere la [documentazione di vRealize Operations](#).

Se vRealize Operations Manager non è in grado di trovare un consiglio o vRealize Automation non è in grado di trovare cluster e storage abilitati per DRS, vRealize Automation controlla l'impostazione di fallback della zona cloud:

- Con fallback
vRealize Automation alloca risorse di elaborazione e storage che restano qualificate anche senza un consiglio di vRealize Operations Manager.
- Senza fallback
vRealize Automation annulla la richiesta e non procede con il provisioning.

Fase 3: provisioning

vRealize Automation distribuisce le macchine virtuali, lo storage e la rete richiesti tramite l'adattatore per la destinazione di posizionamento selezionata alla fine della fase di allocazione.

La destinazione di posizionamento è costituita da host di elaborazione, cluster o pool di risorse e da un datastore o un cluster di datastore collegato.

Ottimizzazione continua con vRealize Operations Manager

Quando si aggiunge l'adattatore di vRealize Automation in vRealize Operations Manager, vRealize Operations Manager crea automaticamente un nuovo data center personalizzato (CDC, Custom Data Center) per i carichi di lavoro basati su vRealize Automation.

L'ottimizzazione continua consente di sfruttare i vantaggi del ribilanciamento e del riposizionamento del carico di lavoro e di utilizzare vRealize Automation con vRealize Operations Manager oltre il posizionamento del carico di lavoro iniziale. Quando le risorse di virtualizzazione vengono spostate o ricevono carichi più pesanti o più leggeri, è possibile spostare i carichi di lavoro di vRealize Automation forniti in provisioning secondo necessità.

- L'ottimizzazione continua crea automaticamente un nuovo CDC in vRealize Operations Manager.

È disponibile un nuovo CDC per ogni zona cloud vSphere di vRealize Automation.

- Il CDC appena creato contiene ogni cluster gestito di vRealize Automation associato alla zona cloud.

Nota Non creare manualmente un CDC misto di cluster di vRealize Automation e non di vRealize Automation.

- È possibile utilizzare vRealize Operations Manager per eseguire l'ottimizzazione continua per il CDC basato su vRealize Automation appena creato.
- I carichi di lavoro possono essere ribilanciati o riposizionati solo all'interno della stessa zona cloud o CDC.
- L'ottimizzazione non crea mai una nuova violazione del posizionamento di vRealize Automation o vRealize Operations Manager.
 - Se sono già presenti violazioni del posizionamento, l'ottimizzazione può risolvere i problemi dello scopo operativo di vRealize Operations Manager.
 - Se sono già presenti violazioni del posizionamento, l'ottimizzazione non può risolvere i problemi dello scopo di business di vRealize Operations Manager.

Ad esempio, se si utilizza vRealize Operations Manager per spostare manualmente una macchina virtuale in un cluster che non supporta i vincoli, vRealize Operations Manager non rileva una violazione né tenta di risolverla.

- Questo rilascio rispetta lo scopo operativo a livello di CDC. Tutti i cluster di vRealize Automation membro sono ottimizzati con le stesse impostazioni.

Per impostare uno scopo operativo diverso per i cluster, è necessario configurarli in CDC di vRealize Automation separati, associati a zone cloud di vSphere distinte. Una situazione di esempio può essere costituita da cluster di verifica e di produzione diversi.

- Lo scopo dell'applicazione vRealize Automation e i vincoli definiti in vRealize Automation vengono rispettati durante le operazioni di ribilanciamento o riposizionamento dell'ottimizzazione.
- I tag di posizionamento di vRealize Operations Manager non possono essere applicati ai carichi di lavoro di vRealize Automation sottoposti a provisioning.

Inoltre, è supportata l'ottimizzazione pianificata con più macchine. Le ottimizzazioni regolarmente pianificate non sono processi radicali. Se le condizioni interrompono il movimento della macchina, le macchine correttamente trasferite rimangono trasferite e il ciclo di vRealize Operations Manager successivo tenta di trasferire il resto come di consueto per vRealize Operations Manager. Tale ottimizzazione parzialmente completata non causa alcun impatto negativo in vRealize Automation.

Come abilitare l'ottimizzazione continua

Quando si aggiunge l'adattatore vRealize Automation in vRealize Operations Manager, vRealize Operations Manager crea automaticamente un nuovo data center dedicato per i carichi di lavoro basati su vRealize Automation.

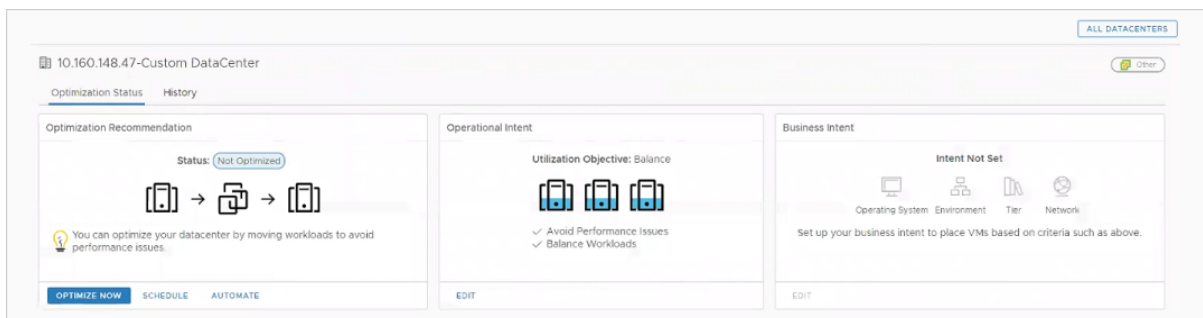
Oltre ad aggiungere l'integrazione in Cloud Assembly, non esistono passaggi di installazione separati per l'ottimizzazione continua. È possibile iniziare a configurare e utilizzare vRealize Operations Manager per il trasferimento dei carichi di lavoro nel nuovo data center. Vedere [Esempio di ottimizzazione continua](#).

Esempio di ottimizzazione continua

L'esempio seguente illustra un workflow di ribilanciamento per l'ottimizzazione continua di vRealize Automation con vRealize Operations Manager.

- 1 Nella pagina iniziale di vRealize Operations Manager, fare clic su **Ottimizzazione carico di lavoro**.
- 2 Selezionare il data center di vRealize Automation creato automaticamente.
- 3 In **Scopo operativo**, fare clic su **Modifica** e selezionare **Bilancia**.

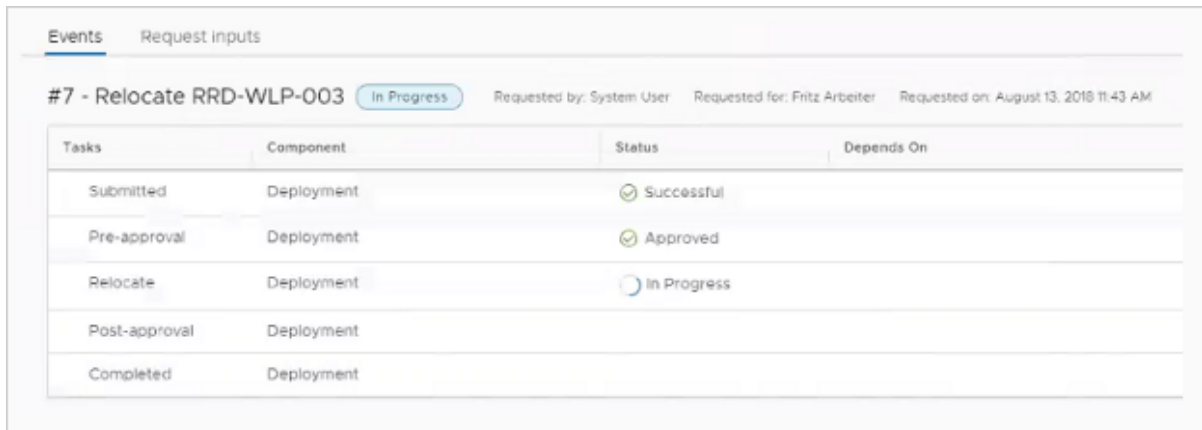
Non è possibile selezionare o modificare lo scopo di business, che è disabilitato quando il data center è dedicato all'ottimizzazione di vRealize Automation.



- 4 In **Raccomandazione ottimizzazione**, fare clic su **Ottimizza ora**.

vRealize Operations Manager mostra un diagramma sulla situazione precedente e successiva all'operazione proposta.

- 5 Fare clic su **Avanti**.
- 6 Fare clic su **Inizia azione**.
- 7 In vRealize Automation, monitorare l'operazione in corso facendo clic su **Risorse** > **Distribuzioni** e controllando lo stato dell'evento.

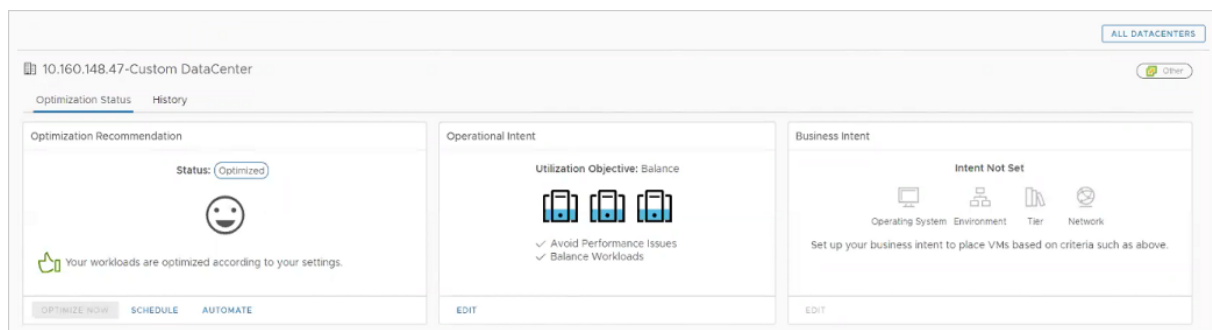


The screenshot shows the 'Events' tab in vRealize Automation. It displays a task titled '#7 - Relocate RRD-WLP-003' with a status of 'In Progress'. The task was requested by 'System User' for 'Fritz Arbeiter' on 'August 13, 2018 11:43 AM'. Below the task header is a table with the following data:

Tasks	Component	Status	Depends On
Submitted	Deployment	Successful	
Pre-approval	Deployment	Approved	
Relocate	Deployment	In Progress	
Post-approval	Deployment		
Completed	Deployment		

Quando il ribilanciamento termina, vRealize Automation viene aggiornato. La pagina Risorse di elaborazione indica che le macchine sono state spostate.

In vRealize Operations Manager, la raccolta dati successiva aggiorna la visualizzazione per indicare che l'ottimizzazione è completa.



The screenshot shows the 'Optimization Status' page in vRealize Operations Manager for a custom data center. The page is divided into three main sections:

- Optimization Recommendation:** Shows a status of 'Optimized' with a smiley face icon. A message states: 'Your workloads are optimized according to your settings.' Below this are buttons for 'OPTIMIZE NOW', 'SCHEDULE', and 'AUTOMATE'.
- Operational Intent:** Shows a 'Utilization Objective: Balance' with three server icons. It lists two goals: 'Avoid Performance Issues' and 'Balance Workloads'. There is an 'EDIT' button.
- Business Intent:** Shows 'Intent Not Set' with icons for Operating System, Environment, Tier, and Network. A message says: 'Set up your business intent to place VMs based on criteria such as above.' There is an 'EDIT' button.

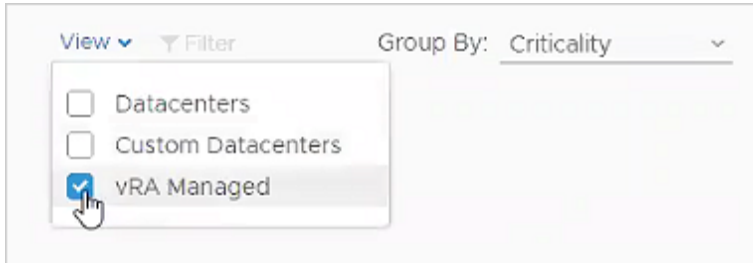
In vRealize Operations Manager, è possibile rivedere l'operazione facendo clic su **Amministrazione** > **Cronologia** > **Attività recenti**.

Come individuare i data center gestiti da vRealize Automation

È possibile utilizzare vRealize Operations Manager per visualizzare solo i data center gestiti da vRealize Automation.

Procedura

- 1 Nella pagina iniziale di vRealize Operations Manager, fare clic su **Ottimizzazione carico di lavoro**.
- 2 In alto a destra, fare clic sul menu a discesa **Visualizza**.
- 3 Selezionare solo i data center gestiti da vRealize Automation.

**Monitoraggio della distribuzione basato su vRealize Operations Manager**

vRealize Automation può mostrare i dati di vRealize Operations Manager sulle distribuzioni.

Esaminare il set filtrato delle metriche direttamente in vRealize Automation consente di evitare le attività di accesso o ricerca in vRealize Operations Manager. Sebbene non sia possibile avviare il contesto in vRealize Operations Manager, è ovviamente possibile accedere e utilizzare vRealize Operations Manager per gli eventuali dati aggiuntivi.

Abilitazione dei dati di vRealize Operations Manager

Affinché vRealize Automation visualizzi i dati di vRealize Operations Manager, devono essere presenti integrazioni specifiche. Le integrazioni richiedono l'indirizzo e le credenziali di accesso per vRealize Automation, vRealize Operations Manager e vCenter.

Procedura

- 1 In vRealize Operations Manager, andare in **Origini dati > Integrazioni** e verificare o aggiungere l'integrazione dell'account di vCenter.
- 2 In Cloud Assembly, andare in **Infrastruttura > Connessioni > Account cloud** e verificare o aggiungere l'account vCenter.

vRealize Operations Manager e vRealize Automation devono essere connessi allo stesso vCenter.

- 3 In vRealize Operations Manager, andare in **Origini dati > Integrazioni** e aggiungere l'integrazione dell'account della scheda di vRealize Automation 8.x.
- 4 In Cloud Assembly, andare in **Infrastruttura > Connessioni > Integrazioni** e aggiungere l'integrazione di vRealize Operations Manager.

Immettere l'indirizzo vRealize Operations Manager nel formato seguente:

`https://operations-manager-IP-address-or-FQDN/suite-api`

Per ulteriore background, vedere [Integrazione con vRealize Operations Manager](#).

Operazioni successive

In Cloud Assembly fare clic su **Risorse > Distribuzioni**, selezionare una distribuzione in vCenter e verificare che venga visualizzata la scheda **Monitora**.

Integrità e avvisi forniti da vRealize Operations Manager

Quando è abilitato il monitoraggio, vRealize Automation recupera lo stato di integrità di vRealize Operations Manager e gli avvisi associati relativi alle distribuzioni.

Per accedere al monitoraggio, fare clic su una distribuzione e selezionare la scheda **Monitora**. Se la scheda non è presente, vedere [Abilitazione dei dati di vRealize Operations Manager](#).

Per visualizzare gli avvisi, selezionare il nome della distribuzione nella parte superiore della struttura del componente nel pannello a sinistra.

- È possibile rivedere il livello di gravità e il testo degli avvisi.
- Per concentrarsi sulle aree di interesse, filtrare e ordinare i dati nelle colonne.
- Vengono visualizzati solo i badge di integrità e gli avvisi di integrità. Altri tipi di avviso come quelli relativi all'efficienza o al rischio non sono supportati.

Metriche fornite da vRealize Operations Manager

Quando è abilitato il monitoraggio, vRealize Automation recupera le metriche di vRealize Operations Manager relative alle distribuzioni.

Per accedere al monitoraggio, fare clic su una distribuzione e selezionare la scheda **Monitora**. Se la scheda non è presente, vedere [Abilitazione dei dati di vRealize Operations Manager](#).

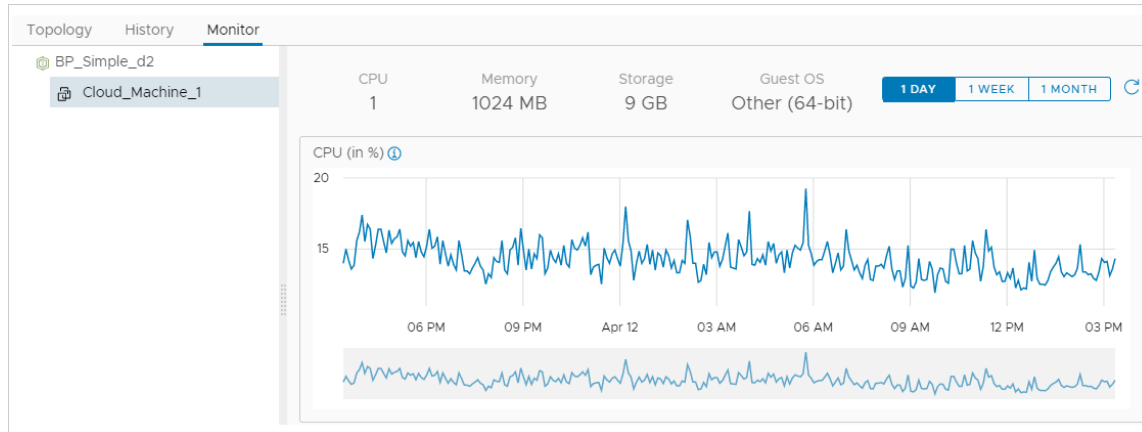
Per visualizzare le metriche, espandere la struttura del componente a sinistra ed evidenziare una macchina virtuale.

- Le metriche non vengono memorizzate nella cache. Provenengono direttamente da vRealize Operations Manager e possono richiedere del tempo per caricarsi.
- Vengono visualizzate solo le metriche della macchina virtuale. Le metriche di altri componenti, come vCloud Director, Software o XaaS, non sono supportate.
- Vengono visualizzate solo le metriche della macchina virtuale di vSphere. Altri fornitori cloud, come AWS o Azure, non sono supportati.

Le metriche vengono visualizzate come grafici temporali che mostrano valori massimi e minimi per le seguenti misure.

- CPU
- Memoria
- IOPS storage
- MBPS rete

Per visualizzare il nome della metrica specifica, fare clic sull'icona blu delle informazioni in alto a sinistra nella linea temporale.

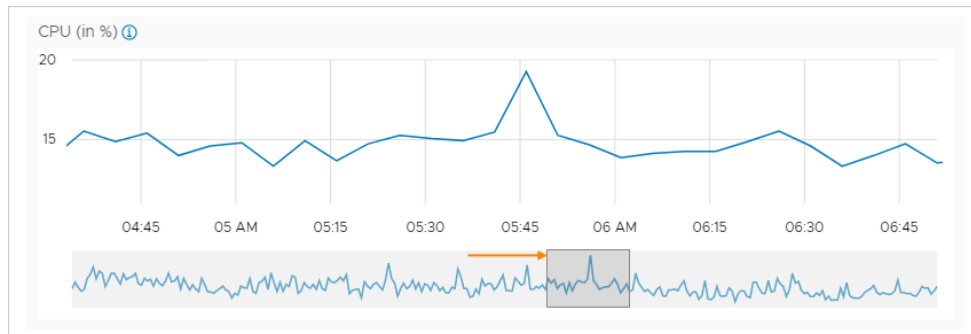


Azioni sui dati forniti da vRealize Operations Manager

Quando le metriche fornite da vRealize Operations Manager espongono un problema, è possibile identificare le aree dei problemi direttamente in vRealize Automation.

Per visualizzare le metriche fornite da vRealize Operations Manager, fare clic su una distribuzione e selezionare la scheda **Monitoraggio**. Se la scheda non è presente, vedere [Abilitazione dei dati di vRealize Operations Manager](#).

Sono disponibili le metriche per l'ultimo giorno, l'ultima settimana o l'ultimo mese. Per ingrandire un'area di interesse, selezionare un'area di piccole dimensioni nella parte ombreggiata inferiore sotto la sequenza temporale di una metrica qualsiasi:



Ottimizzazione di distribuzione e gestione delle risorse utilizzando metriche di vRealize Operations Manager in vRealize Automation

In un ambiente vRealize Automation e vRealize Operations Manager integrato, è possibile accedere a informazioni dettagliate e avvisi per gli oggetti di vRealize Automation monitorati da vRealize Operations Manager.

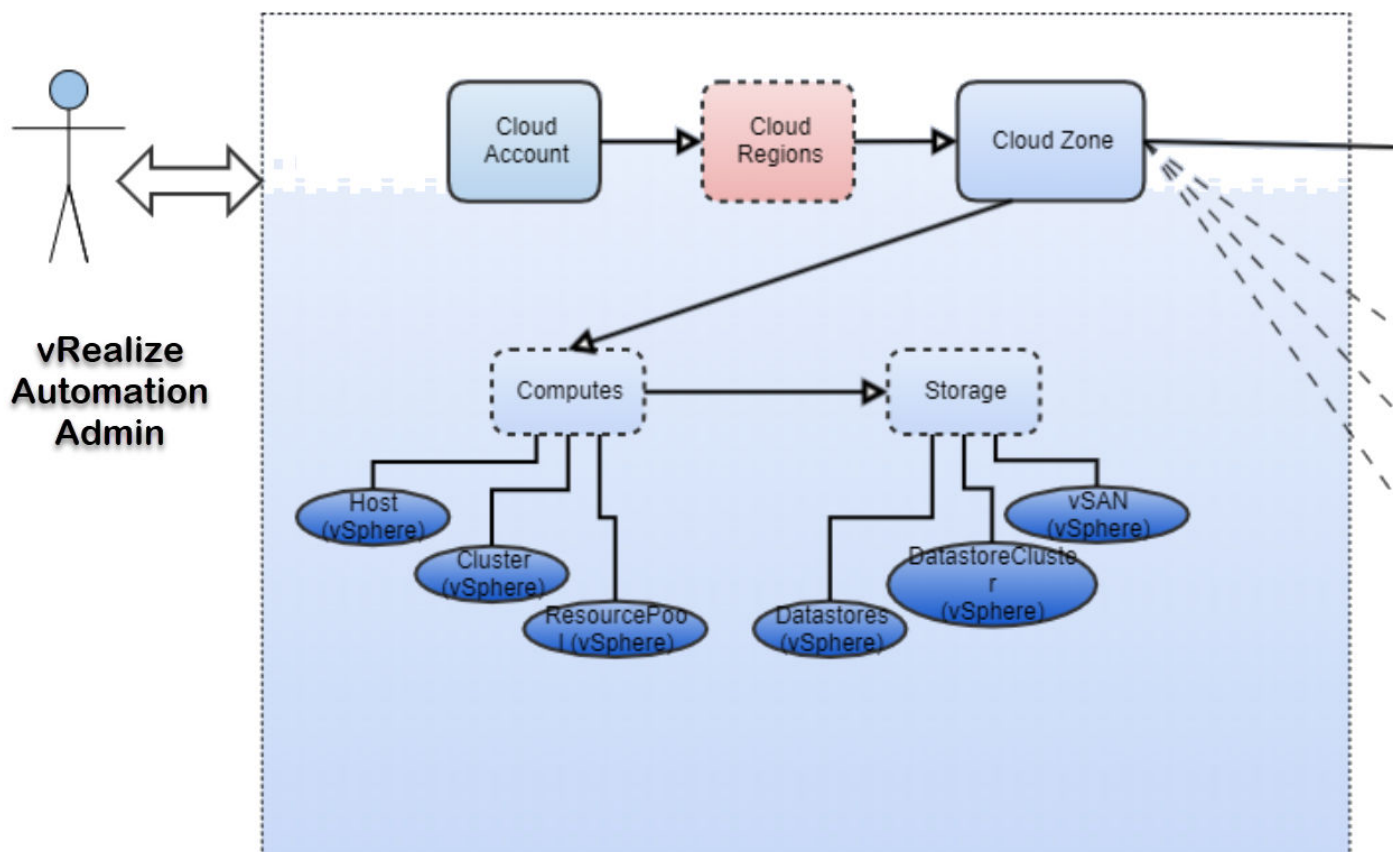
Il dashboard **Dettagli** e le pagine della scheda **Avvisi** forniscono la capacità in tempo reale e le informazioni dettagliate correlate necessarie per prendere decisioni di gestione in vRealize Automation senza dover aprire vRealize Operations Manager. Le informazioni sono fornite dall'applicazione vRealize Operations Manager associata.

Utilizzo del dashboard Dettagli e degli avvisi delle risorse

Il dashboard **Dettagli** fornisce informazioni sul consumo della capacità relative a tutte le elaborazioni all'interno della zona cloud e raggruppate per progetti. Può inoltre visualizzare le distribuzioni di progetti che necessitano di ottimizzazione.

Le pagine **Avvisi** mostrano potenziali problemi di capacità e prestazioni per oggetti quali zone cloud, progetti, distribuzioni e macchine virtuali. Contengono inoltre informazioni per i proprietari dei progetti in cui sono individuate quali delle loro distribuzioni possono essere ottimizzate. Ogni collegamento alla distribuzione apre la scheda **Ottimizza** nella distribuzione, dove vengono fornite istruzioni specifiche.

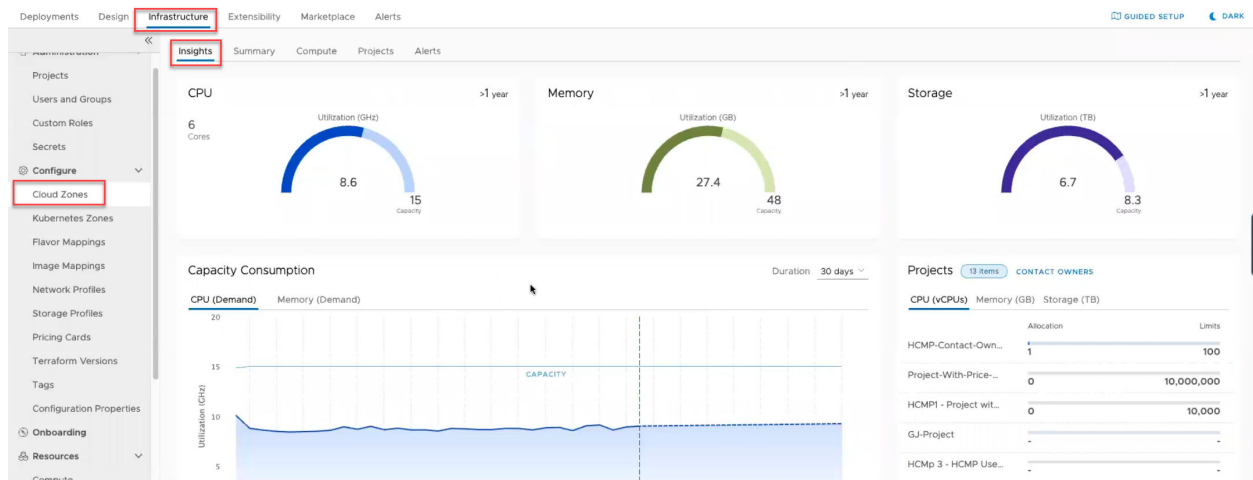
Il diagramma seguente illustra la relazione tra le risorse e le distribuzioni di vRealize Automation e i dati forniti dall'applicazione vRealize Operations Manager associata in vRealize Automation.



Utilizzo del dashboard Dettagli

Il dashboard **Dettagli**, disponibile nella pagina di tutte le zone cloud, fornisce le metriche vRealize Operations Manager seguenti:

- Utilizzo di CPU, memoria e storage come percentuale di capacità
- Riepilogo del consumo di funzionalità
- Richiesta di CPU e memoria e cronologia di utilizzo
- Consumo tra i progetti
- Capacità di risorse recuperabile, con risparmi sui costi, per distribuzioni e progetti in una zona cloud



Offre inoltre un'opzione per informare i proprietari dei progetti di eventuali distribuzioni che possono essere ottimizzate.

Il dashboard **Dettagli** è disponibile per le zone cloud di vSphere e VMware Cloud on AWS, a condizione che gli account cloud siano configurati in vRealize Automation e in vRealize Operations Manager e che siano monitorati in vRealize Operations Manager.

Per i dettagli, vedere [Come utilizzare il dashboard Dettagli per monitorare la capacità delle risorse e informare i proprietari dei progetti in vRealize Automation](#).

Utilizzo degli avvisi

Le pagine **Avvisi** offrono le seguenti categorie di filtro. Le categorie di filtro sono fornite dall'applicazione vRealize Operations Manager associata.

- Gravità
- Stato
- Impatto
- Tipo
- Sottotipo

■ Risorsa

Ogni filtro può essere ulteriormente affinato utilizzando filtri rapidi. Ad esempio, il filtro delle risorse può essere ulteriormente affinato mediante i tipi di filtro rapidi zona cloud, macchina virtuale, distribuzione e risorsa di progetto.

È possibile utilizzare combinazioni di filtri e filtri rapidi per controllare quali avvisi sono disponibili per la visualizzazione.

The screenshot displays the vRealize Automation Alerts interface. At the top, there are tabs for Deployments, Design, Infrastructure, Extensibility, Marketplace, and Alerts. Below the tabs, there is a filter section with a 'Resource Type' dropdown and a 'Quick filters' search bar. A dropdown menu is open under 'Resource Type', showing options: Cloud Zone (checked), Virtual Machine (checked), Deployment (unchecked), and Project (checked). To the right of the filter section, there are three filter buttons: 'Status: Active', 'Resource Type: Virtual Machine, Project, Cloud Zone', and 'Impact: Health'. The main content area shows a list of alerts. The first alert is 'Virtual machine is powered off for more than 5 days' with a warning icon and a timestamp of 4:40 PM. Below it are three alerts with error icons and timestamps of 1:26 PM. On the right side, there is a detailed view of the first alert, showing its severity (Warning), status (Active), impact (Health), and type (Infrastructure). It also includes a 'Suggestions' section with two items: 'Delete powered off machines' and 'Manually power on the virtual machine.' Below the suggestions is a 'Notes' section with a text input field and an 'ADD NOTE' button.

Alcuni **Avvisi** forniscono informazioni e collegamenti alle distribuzioni che possono essere ottimizzate. Un avviso singolo può fornire l'opzione per contattare il proprietario del progetto, esaminare un dashboard Dettagli o eseguire possibili azioni.

The screenshot displays the vRealize Automation Alerts interface. At the top, navigation tabs include Deployments, Design, Infrastructure, Extensibility, Marketplace, and Alerts (highlighted). Below the tabs, there's a filter bar with 'Severity' dropdown, 'Quick filters', and buttons for 'Status: Active' and 'Severity: Critical'. The main content area is divided into 'Today' and 'Yesterday' sections. A red box highlights an alert in the 'Today' section: 'The project has some deployments that contain optimizable resources.' This alert is linked to 'Project » vc65 project'. A red arrow points from this alert to a detailed view on the right. The detailed view shows the alert title, creation and update timestamps, project name, and a 'Suggestions' section with a 'REVIEW PROJECT' link. Below this, a 'Deployments to review' table lists deployment names and owners. A red arrow points to the deployment 'contact-owner-test-dep-2'. At the bottom, there's a 'Notes' section with a text area containing 'Investigating' and an 'ADD NOTE' button.

Gli avvisi sono disponibili per gli oggetti risorsa di vSphere e VMware Cloud on AWS.

Per informazioni dettagliate su come configurare e utilizzare gli avvisi integrati, vedere [Come utilizzare Avvisi per gestire capacità, prestazioni e disponibilità delle risorse in vRealize Automation](#) e [Come utilizzare gli avvisi per ottimizzare le distribuzioni in vRealize Automation](#).

Che cosa sono i piani di onboarding in Cloud Assembly

Il piano di onboarding del carico di lavoro serve per identificare le macchine di cui sono stati raccolti i dati da un tipo di account cloud in una regione o in un data center di destinazione, ma che non sono ancora gestite da un progetto Cloud Assembly.

Quando si aggiunge un account cloud che contiene macchine distribuite al di fuori di Cloud Assembly, le macchine non sono gestite da Cloud Assembly fino a quando non ne viene eseguito l'onboarding. Utilizzare un piano di onboarding per portare le macchine non gestite nella gestione di Cloud Assembly. Si crea un piano, si popola con le macchine, quindi si esegue per importare le macchine. Utilizzando il piano di onboarding, è possibile creare un modello cloud e anche una o più distribuzioni.

È possibile eseguire l'onboarding di una o più macchine non gestite in un unico piano selezionando le macchine manualmente.

- È possibile eseguire l'onboarding di un massimo di 3.500 macchine non gestite all'ora all'interno di un singolo piano di onboarding.
- È possibile eseguire l'onboarding di un massimo di 17.000 macchine non gestite simultaneamente all'ora all'interno di piani di onboarding multipli.

Le macchine disponibili per l'onboarding del carico di lavoro sono elencate in **Risorse > Risorse > Macchine virtuali** etichettate come *Discovered* nella Colonna origine. Sono elencate solo le macchine di cui sono stati raccolti i dati. Dopo aver eseguito l'onboarding delle macchine, queste vengono visualizzate nella colonna Origine come *Deployed*. È possibile applicare un filtro in base

alle macchine rilevate o distribuite facendo clic sull'icona del filtro



The screenshot shows the VMware Cloud Assembly interface. The top navigation bar includes 'Resources', 'Design', 'Infrastructure', and 'Extensibility'. The left sidebar shows 'Resources' selected, with a dropdown menu showing 'All Resources', 'Virtual Machines', 'Volumes', and 'Networking & Security'. The main area displays a list of virtual machines under the 'Discovered' filter. The table has columns for Name and Depl. The first row shows 'popove-vSphere Server...'. The second row shows 'aws-vm-mcm602-1866...'. The third row shows 'dboikliev-vRealizeOrch...'.

La persona che esegue il piano di onboarding del carico di lavoro viene indicata automaticamente come proprietario della macchina.

L'onboarding supporta inoltre le proprietà personalizzate dell'onboarding, i dischi collegati, la modifica dei proprietari delle distribuzioni e le reti di vSphere.

- Proprietà personalizzate: è possibile impostare proprietà personalizzate a livello del piano e delle singole macchine. Un set di proprietà personalizzate a livello di macchina sovrascrive la stessa proprietà a livello del piano.
- Dischi collegati: se una macchina dispone di dischi non avviabili, viene automaticamente eseguito l'onboarding dei dischi nella macchina principale. Per visualizzare i dischi non avviabili, fare clic sul nome della macchina nel piano e passare alla scheda **Storage**.

- Proprietà della distribuzione: l'onboarding consente di cambiare il proprietario della distribuzione predefinito. Per modificare il proprietario, selezionare una distribuzione nella scheda **Distribuzione**, fare clic su **Azioni > Modifica proprietario** e selezionare l'utente desiderato associato al progetto.

Esempi di onboarding

Per esempi di tecniche di onboarding, vedere [Esempio: onboarding delle macchine selezionate come singola distribuzione in Cloud Assembly](#).

Sottoscrizioni agli eventi di onboarding

Quando si esegue il piano, viene creato un evento `Deployment Onboarded`. Utilizzando le opzioni della scheda Estendibilità, è possibile eseguire la sottoscrizione a questi eventi di distribuzione ed eseguire azioni su di essi.

Dopo l'onboarding, è possibile aggiornare un progetto come azione giorno 2 per le distribuzioni di cui è stato eseguito l'onboarding. Per utilizzare l'azione di modifica del progetto, il progetto di destinazione deve utilizzare le stesse risorse della zona cloud della distribuzione. Non è possibile eseguire l'azione di modifica del progetto in alcuna distribuzione di onboarding in cui sono state apportate modifiche dopo l'onboarding.

Esempio: onboarding delle macchine selezionate come singola distribuzione in Cloud Assembly

In questo esempio si esegue l'onboarding di due macchine non gestite come singola distribuzione di Cloud Assembly e si crea un singolo modello cloud per tutte le macchine nel piano.

Quando si crea un account cloud, vengono raccolti i dati di tutte le macchine associate a tale account e le macchine vengono visualizzate nella pagina **Risorse > Risorse > Macchine virtuali**. Se l'account cloud include macchine distribuite all'esterno di Cloud Assembly, è possibile utilizzare un piano di onboarding per consentire a Cloud Assembly di gestire le distribuzioni delle macchine.

Nota È possibile rinominare le distribuzioni solo prima che vengano sottoposte a onboarding. Dopo l'onboarding, l'opzione **Rinomina** viene disabilitata.

Prerequisiti

- Verificare di disporre del ruolo utente necessario. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Rivedere [Che cosa sono i piani di onboarding in Cloud Assembly](#).
- Creare e preparare un progetto Cloud Assembly.

Questa procedura comporta alcuni passaggi dal caso d'uso di base di Wordpress. Vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).

- Creare un progetto, aggiungere utenti e assegnare ruoli utente nel progetto. Vedere [Parte 2: creazione del progetto Cloud Assembly di esempio](#).

- Creare un account cloud di Amazon Web Services per il progetto. Vedere la sezione relativa all'account cloud dell'[Parte 1: configurazione dell'infrastruttura Cloud Assembly di esempio](#).

L'account cloud di Amazon Web Services in questa procedura contiene le macchine che sono state distribuite prima che l'account cloud fosse aggiunto a Cloud Assembly e da un'applicazione diversa da Cloud Assembly.

- Verificare che la pagina **Risorse > Risorse > Macchine virtuali** contenga le macchine di cui eseguire l'onboarding. Per ulteriori informazioni, vedere [Gestione delle risorse in Cloud Assembly](#).

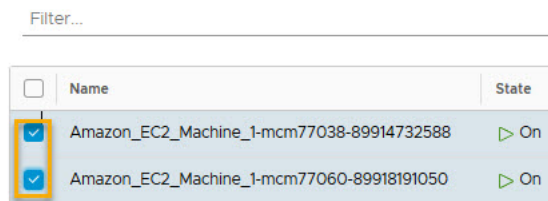
Procedura

- 1 Passare a **Infrastruttura > Onboarding**.
- 2 Fare clic su **Nuovo piano di onboarding** e immettere i valori di esempio.

Impostazione	Valore di esempio
Nome del piano	VC-sqa-deployments
Descrizione	Esempio di piano di onboarding per la macchina AWS per l'account cloud OurCo-AWS
Account cloud	OurCo-AWS
Progetto predefinito	WordPress

- 3 Fare clic su **Crea**.
- 4 Nella scheda **Distribuzioni** del piano, fare clic su **Seleziona macchine**, scegliere una o più macchine e fare clic su **OK**.

Select Machines



- 5 Selezionare **Crea una distribuzione che contenga tutte le macchine** e fare clic su **Crea**.
- 6 Fare clic sulla casella di controllo accanto al nome della nuova distribuzione e fare clic su **Modello cloud....**

- 7 Fare clic su **Crea modello cloud in formato Cloud Assembly** e immettere un nome per il modello cloud oppure fare clic su **Assegna un modello cloud esistente** e selezionare il modello cloud desiderato da assegnare.

Nota La mappatura dei modelli cloud nelle distribuzioni di cui è stato eseguito l'onboarding è solo per la parità visiva per i consumatori finali. Le distribuzioni di cui è stato eseguito l'onboarding non sono compatibili con i modelli cloud.

8 Fare clic su **Salva**.

Cloud Template Configuration

Mapping of Cloud Templates to onboarding deployments is only for visual parity for end consumers. Onboarded deployments are not compatible with Cloud Templates.

Deployment: Demo

☐ None (use runtime snapshot)
☐ Create Cloud Template in Cloud Assembly format
☒ Assign an existing Cloud Template

	Name	Project	Last Updated
<input checked="" type="radio"/>	Demo	onboarding	Oct 21, 2021, 1:36:15 PM
<input type="radio"/>	171	onboarding	Jun 10, 2021, 8:21:55 AM
<input type="radio"/>	asdf	onboarding	May 25, 2021, 9:24:07 AM
<input type="radio"/>	asdf	onboarding	Dec 7, 2020, 3:03:53 PM

CANCEL SAVE

Nota Quando il piano di onboarding utilizza una macchina vSphere, è necessario modificare il modello cloud dopo aver completato il processo di integrazione. Il processo di onboarding non può collegare la macchina vSphere di origine e il relativo modello di macchina e il modello cloud risultante conterrà la voce `imageRef: "no image available"` nel codice del modello cloud. Il modello cloud non può essere distribuito finché non si specifica il nome del modello corretto nel campo `imageRef:`. Per semplificare l'individuazione e l'aggiornamento del modello cloud dopo il completamento del processo di integrazione, utilizzare l'opzione **Nome modello cloud** nella pagina **Configurazione modello cloud** della distribuzione. Registrare il nome del modello cloud generato automaticamente o immettere e registrare il nome di un modello cloud secondo preferenza. Al termine dell'onboarding, individuare e aprire il modello cloud e sostituire la voce `"no image available"` nel campo `imageRef:` con il nome del modello corretto.

9 Fare clic sulla casella di controllo Nome distribuzione, fare clic su **Esegui**, quindi fare di nuovo clic su **Esegui** nella pagina **Esegui piano**.

L'onboarding delle macchine selezionate viene eseguito come distribuzione singola insieme a un modello cloud.

- 10 Aprire ed esaminare il modello cloud facendo clic sulla pagina **Progettazione > Modelli cloud**, quindi fare clic sul nome del modello cloud.
- 11 Aprire ed esaminare la distribuzione facendo clic sulla pagina **Risorse > Distribuzioni**, quindi sul nome della distribuzione.

Configurazione avanzata per l'ambiente Cloud Assembly

È possibile configurare l'ambiente Cloud Assembly in modo che supporti ulteriormente la configurazione, l'integrazione e la distribuzione del progetto.

Per informazioni correlate e aggiuntive sui metodi di amministrazione, ad esempio l'utilizzo di utenti e registri e la partecipazione o l'uscita dal programma Analisi utilizzo software, vedere la guida [Amministrazione di vRealize Automation](#).

Come configurare un server proxy Internet per vRealize Automation

Per le installazioni di vRealize Automation in reti isolate senza accesso diretto a Internet, è possibile utilizzare un server proxy Internet per consentire la funzionalità Internet tramite proxy. Il server proxy Internet supporta HTTP e HTTPS.

Per configurare e utilizzare provider di cloud pubblici come Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP), nonché punti di integrazione esterni come IPAM, Ansible e Puppet, con vRealize Automation, è necessario configurare un server proxy Internet per accedere al server proxy Internet interno di vRealize Automation.

vRealize Automation contiene un server proxy interno che comunica con il server proxy Internet. Questo server comunica con il server proxy se è stato configurato con il comando `vracli proxy set . . .`. Se non è stato configurato un server proxy Internet per l'organizzazione, il server proxy interno di vRealize Automation tenta di connettersi direttamente a Internet.

È possibile configurare vRealize Automation affinché utilizzi un server proxy Internet tramite l'utilità della riga di comando `vracli` specificata. Le informazioni su come utilizzare l'API `vracli` possono essere visualizzate utilizzando l'argomento `--help` nella riga di comando `vracli`, ad esempio `vracli proxy --help`.

L'accesso al server proxy Internet richiede l'utilizzo dei controlli incorporati locali di estendibilità basata su azioni (ABX) integrati in vRealize Automation.

Nota L'accesso a Workspace ONE Access (denominato in precedenza VMware Identity Manager) non è supportato tramite il proxy Internet. Non è possibile utilizzare il comando `vracli set vidm` per accedere a Workspace ONE Access tramite il server proxy Internet.

Il server proxy interno richiede IPv4 come formato IP predefinito. Non richiede autenticazione, azioni man-in-the-middle o limitazioni del protocollo Internet nel traffico di certificati TLS (HTTPS).

Prerequisiti

- Verificare di disporre di un server HTTP o HTTPS esistente, che possa essere utilizzato come server proxy Internet, nella rete di vRealize Automation in grado di passare il traffico in uscita ai siti esterni. La connessione deve essere configurata per IPv4.
- Verificare che il server proxy Internet di destinazione sia configurato per supportare IPv4 come formato IP predefinito e non per IPv6.
- Se il server proxy Internet utilizza TLS e richiede una connessione HTTPS con i propri client, è necessario importare il certificato del server utilizzando uno dei comandi seguenti, prima di impostare la configurazione del proxy.

- `vracli certificate proxy --set path_to_proxy_certificate.pem`
- `vracli certificate proxy --set stdin`

Utilizzare il parametro `stdin` per l'input interattivo.

Procedura

- 1 Creare una configurazione proxy per i pod o i contenitori utilizzati da Kubernetes. In questo esempio, si accede al server proxy utilizzando lo schema HTTP.

```
vracli proxy set --host http://proxy.vmware.com:3128
```

- 2 Visualizzare la configurazione del proxy.

```
vracli proxy show
```

Il risultato sarà simile a:

```
{
  "enabled": true,
  "host": "10.244.4.51",
  "java-proxy-exclude": "*.local|*.localdomain|localhost|10.244.*|
192.168.*|172.16.*|kubernetes|sc2-rdops-vm06-dhcp-198-120.eng.vmware.com|10.192.204.9|
*.eng.vmware.com|sc2-rdops-vm06-dhcp-204-9.eng.vmware.com|10.192.213.146|sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com|10.192.213.151|sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "java-user": null,
  "password": null,
  "port": 3128,
  "proxy-
exclude": ".local,.localdomain,localhost,10.244.,192.168.,172.16.,kubernetes,sc2-
rdops-vm06-dhcp-198-120.eng.vmware.com,10.192.204.9,.eng.vmware.com,sc2-
rdops-vm06-dhcp-204-9.eng.vmware.com,10.192.213.146,sc2-rdops-vm06-
dhcp-213-146.eng.vmware.com,10.192.213.151,sc2-rdops-vm06-dhcp-213-151.eng.vmware.com",
  "scheme": "http",
  "upstream_proxy_host": null,
  "upstream_proxy_password_encoded": "",
  "upstream_proxy_port": null,
  "upstream_proxy_user_encoded": "",
  "user": null,
  "internal.proxy.config": "dns_v4_first on \nhttp_port
0.0.0.0:3128\nlogformat squid %ts.%03tu %6tr %>a %Ss/%03>Hs
%<st %rm %ru %<un %Sh/%<a %mt\naccess_log stdio:/tmp/logger squid\ncoredump_dir /\ncache
```

```
deny all \nappend_domain .prelude.svc.cluster.local\nacl mylan src 10.0.0.0/8\nacl mylan
src 127.0.0.0/8\nacl mylan src 192.168.3.0/24\nacl proxy-exclude dstdomain .local\nacl
proxy-exclude dstdomain .localdomain\nacl proxy-exclude dstdomain localhost\nacl
proxy-exclude dstdomain 10.244.\n acl proxy-exclude dstdomain 192.168.\n acl proxy-exclude
dstdomain 172.16.\n acl proxy-exclude dstdomain kubernetes\nacl proxy-exclude dstdomain
10.192.204.9\nacl proxy-exclude dstdomain .eng.vmware.com\nacl proxy-exclude dstdomain
10.192.213.146\nacl proxy-exclude dstdomain 10.192.213.151\nalways_direct allow proxy-
exclude\nhttp_access allow mylan\nhttp_access deny all\n# End autogen configuration\n",
    "internal.proxy.config.type": "default"
}
```

Nota Se è stato configurato un server proxy Internet per l'organizzazione, nell'esempio precedente viene visualizzato "internal.proxy.config.type": "non-default" anziché 'default'. Per motivi di sicurezza, la password non viene visualizzata.

Nota Se si utilizza il parametro `-proxy-exclude`, è necessario modificare i valori predefiniti. Ad esempio, se si desidera aggiungere `acme.com` come dominio a cui non è possibile accedere utilizzando il server proxy Internet, eseguire i passaggi seguenti:

- a Immettere `vracli proxy default-no-proxy` per ottenere le impostazioni proxy-exclude predefinite. Si tratta di un elenco di domini e reti generati automaticamente.
- b Modificare il valore per aggiungere `.acme.com`.
- c Immettere `vracli proxy set --proxy-exclude ...` per aggiornare le impostazioni di configurazione.
- d Eseguire il comando `/opt/scripts/deploy.sh` per ridistribuire l'ambiente.

- 3 (Facoltativo) Escludere i domini DNS, i nomi di dominio completi e gli indirizzi IP a cui il server proxy Internet non deve accedere.

Modificare i valori predefiniti della variabile `proxy-exclude` sempre utilizzando `parameter --proxy-exclude`. Per aggiungere il dominio `exclude.vmware.com`, utilizzare innanzitutto il comando `vracli proxy show`, quindi copiare la variabile `proxy-exclude` e aggiungere il valore del dominio utilizzando il comando `vracli proxy set ...` come indicato di seguito:

```
vracli proxy set --host http://
proxy.vmware.com:3128 --proxy-exclude "exclude.vmware.com,docker-
registry.prelude.svc.cluster.local,localhost,.local,.cluster.local,10.244.,192.,172.16.,sc-
rdops-vm11-dhcp-75-38.eng.vmware.com,10.161.75.38,.eng.vmware.com"
```

Nota Aggiungere elementi a `proxy-exclude` anziché sostituire i valori. Se si eliminano i valori predefiniti di `proxy-exclude`, vRealize Automation non funzionerà correttamente. Se succede, eliminare la configurazione del proxy e ricominciare.

- 4 Dopo aver impostato il server proxy Internet con il comando `vracli proxy set ...`, è possibile utilizzare il comando `vracli proxy apply` per aggiornare la configurazione del server proxy Internet e rendere attive le impostazioni del proxy più recenti.

- 5 Se non è già stato fatto, attivare le modifiche dello script eseguendo il comando seguente:

```
/opt/scripts/deploy.sh
```

- 6 (Facoltativo) Se necessario, configurare il server proxy per supportare l'accesso esterno sulla porta 22.

Per supportare integrazioni come Puppet e Ansible, il server proxy deve consentire alla porta 22 di accedere agli host pertinenti.

Esempio: Esempio di configurazione di Squid

Rispetto al passaggio 1, se si sta configurando un proxy Squid, è possibile modificare la configurazione in `/etc/squid/squid.conf` adattandola all'esempio seguente:

```
acl localnet src 192.168.11.0/24

acl SSL_ports port 443

acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

http_access allow !Safe_ports
http_access allow CONNECT !SSL_ports
http_access allow localnet

http_port 0.0.0.0:3128

maximum_object_size 5 GB
cache_dir ufs /var/spool/squid 20000 16 256
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320

client_persistent_connections on
server_persistent_connections on
```

Quali operazioni è possibile eseguire con la mappatura di NSX-T a più vCenter in vRealize Automation

È possibile associare un account cloud di NSX-T a uno o più account cloud di vCenter per supportare vari obiettivi di distribuzione.

È possibile associare la stessa rete esistente di NSX-T a profili di rete per diversi vCenter ed eseguire il provisioning di una distribuzione in uno dei vCenter in base a vincoli. Di seguito sono riportati alcuni esempi:

- Modelli cloud che contengono una sola macchina con più NIC che utilizzano lo stesso profilo di rete, dove tale profilo di rete contiene una rete NSX-T che si estende su più vCenter.
- Modelli cloud che contengono una macchina in una rete *privata* che utilizza un profilo di rete con isolamento basato su subnet e che utilizza una rete NSX-T *esistente* che si estende su più vCenter.
- Modelli cloud che contengono una sola macchina in una rete *privata* che utilizza un profilo di rete con isolamento basato su gruppi di sicurezza e che utilizza una rete di NSX-T che si estende su più vCenter.
- Modelli cloud che contengono una sola macchina in una rete *instradata* che utilizza un profilo di rete contenente una rete di NSX-T che si estende su più vCenter.
- Modelli cloud contengono un bilanciamento del carico su richiesta definito in un profilo di rete in cui il bilanciamento del carico viene applicato a tutte le macchine vCenter della rete.
- Modelli cloud contengono una rete su richiesta definita in un profilo di rete in cui la rete su richiesta viene utilizzata da tutti i vCenter che utilizzano il profilo di rete.
- Modelli cloud che contengono un gruppo di sicurezza su richiesta che contiene facoltativamente le regole del firewall e dove il gruppo di sicurezza è associato a tutti i vCenter presenti nella rete.

È possibile configurare IPAM interno o esterno di vRealize Automation nella rete NSX-T e condividere lo stesso indirizzo IP per le macchine di cui viene eseguito il provisioning in diversi vCenter.

Se nel sistema non è stato definito alcun profilo di rete, è possibile eseguire il provisioning di un Modello cloud che contenga più macchine su diversi vCenter che condividono una singola rete NSX-T *esistente*.

Che cosa accade se si rimuove un'associazione di account cloud di NSX in vRealize Automation

Se si rimuove un'associazione tra un account cloud di NSX e un account cloud di vCenter, è necessario aggiornare anche i profili di rete correlati per rimuovere gli oggetti di NSX associati.

Se si rimuove un'associazione tra un account cloud di NSX e un account cloud di vCenter, gli elementi dell'infrastruttura non vengono aggiornati automaticamente da vRealize Automation. È necessario aggiornare i profili di rete esistenti per rimuovere gli oggetti di NSX associati.

L'interfaccia utente fornisce informazioni che consentono di evidenziare gli elementi del profilo di rete interessati nel modo seguente:

- Se nel profilo di rete è selezionata una rete di NSX esistente:
 - L'oggetto è contrassegnato come *non valido* e viene visualizzato il messaggio *Alcuni oggetti di rete sono mancanti o non validi*.
 - Gli oggetti vengono rimossi quando si salva il profilo di rete.
- Se nel profilo di rete è configurato l'isolamento app, è necessario aggiornare le impostazioni del Criterio di isolamento prima di poter salvare il profilo di rete.
- Se nel profilo di rete sono selezionati gruppi di sicurezza o bilanciamenti del carico, al salvataggio del profilo di rete gli oggetti vengono rimossi.

Le distribuzioni esistenti continuano a funzionare come progettate per i componenti esistenti, ma avranno esito negativo durante la creazione di nuovi componenti, ad esempio in un'operazione di scalabilità orizzontale.

Se si ristabilisce l'associazione, il profilo di rete viene ripopolato e le distribuzioni esistenti funzionano secondo la progettazione.

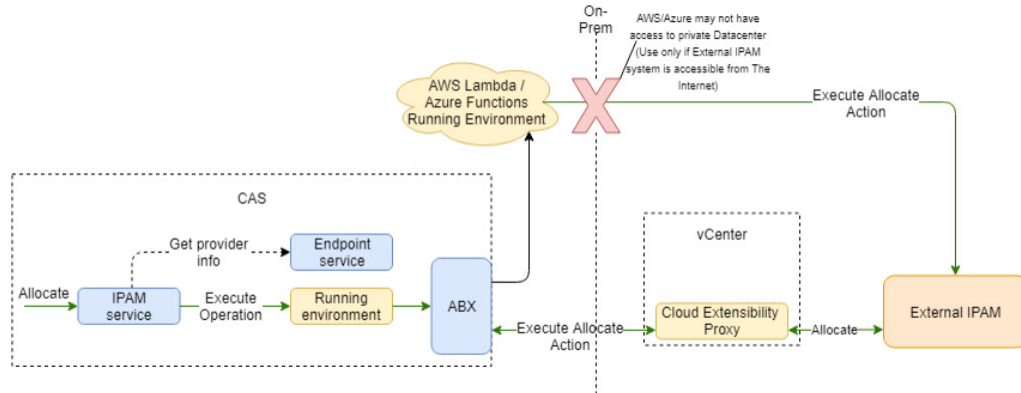
Se si rimuove l'account cloud di NSX, il comportamento precedente è lo stesso, ma gli oggetti di rete sono contrassegnati come *mancanti* anziché come *non validi*.

Come utilizzare l'SDK IPAM per creare un pacchetto di integrazione IPAM esterno specifico del provider per vRealize Automation

I fornitori e i partner IPAM esterni possono scaricare e utilizzare l'SDK IPAM per creare un pacchetto di integrazione IPAM che consenta a vRealize Automation di supportare la propria soluzione IPAM specifica del provider.

Il processo per la creazione e la distribuzione di un pacchetto di integrazione IPAM personalizzato per vRealize Automation utilizzando l'SDK IPAM fornito è descritto nel documento [Creazione e distribuzione di un pacchetto di integrazione IPAM specifico del provider per VMware Cloud Assembly](#). Come descritto nel documento, è possibile scaricare la versione più recente di *VMware vRealize Automation Third-Party IPAM SDK* dal sito [VMware Code](#). Sono disponibili i seguenti pacchetti IPAM SDK:

- [VMware vRealize Automation Third-Party IPAM SDK 1.1.0](#)
- [VMware vRealize Automation Third-Party IPAM SDK 1.0.0](#)



Prima di creare un pacchetto di integrazione IPAM specifico del fornitore utilizzando l'SDK IPAM, verificare se ne esiste già uno per vRealize Automation. È possibile controllare un pacchetto di integrazione IPAM specifico del provider sul sito Web del provider IPAM o da [VMware Marketplace](#).

Sebbene l'esempio [Tutorial: configurazione dell'integrazione di un provider IPAM esterno specifico del provider per vRealize Automation](#) sia specifico del fornitore, contiene anche informazioni di riferimento utili.

Utilizzo di vRealize Automation con Azure VMware Solution

Questa procedura descrive come configurare vRealize Automation affinché funzioni con un ambiente di cloud ibrido self-service Microsoft Azure VMware Solution, in modo che sia possibile utilizzare i carichi di lavoro di vRealize Automation all'interno di questo ambiente.

vRealize Automation supporta le connessioni con Azure VMware Solution (AVS) per spostare ed eseguire carichi di lavoro VMware virtuali in un ambiente cloud Azure. AVS è stato creato da Microsoft per supportare un'interfaccia con gli ambienti VMware.

L'uso di AVS è documentato in maniera completa da Microsoft. La documentazione è disponibile alla pagina seguente:

- Azure VMware Solution - <https://docs.microsoft.com/en-us/azure/azure-vmware/>

Per utilizzare AVS in vRealize Automation, è necessario configurare account cloud sia vCenter che NSX-T. Per la configurazione di questi account cloud, consultare la documentazione seguente:

- Configurazione di account cloud vCenter: [Creazione di un account cloud di vCenter in vRealize Automation](#)
- Creazione di un account cloud NSX-T: [Creazione di un account cloud di NSX-T in vRealize Automation](#)

La procedura seguente descrive i principali passaggi per configurare l'ambiente in modo da poter distribuire carichi di lavoro di vRealize Automation su AVS.

- 1 Installare e configurare Azure VMware Solution in base alle istruzioni del fornitore appropriate per il proprio ambiente.

- 2 Creare account cloud di vCenter e NSX-T all'interno della distribuzione di vRealize Automation.

Uso di vRealize Automation con Google Cloud VMware Engine

Questa procedura descrive come configurare vRealize Automation affinché funzioni con un ambiente di cloud ibrido self-service Google Cloud ibrido VMware Solution, in modo che sia possibile utilizzare i carichi di lavoro di vRealize Automation all'interno di questo ambiente.

vRealize Automation supporta le connessioni con Google Cloud VMware Engine (GCVE) per spostare ed eseguire carichi di lavoro VMware su Google Cloud. GCVE è stato creato da Google per supportare un'interfaccia con gli ambienti VMware.

L'uso di GCVE è documentato in maniera completa da Google. La documentazione è disponibile alla pagina seguente:

- Google Cloud VMware Engine - <https://cloud.google.com/vmware-engine/docs>

Per utilizzare GCVE con vRealize Automation, è necessario configurare account cloud sia vCenter che NSX-T in vRealize Automation. Per la configurazione di questi account cloud, consultare la documentazione seguente:

- Configurazione di account cloud vCenter: [Creazione di un account cloud di vCenter in vRealize Automation](#)
- Creazione di un account cloud NSX-T: [Creazione di un account cloud di NSX-T in vRealize Automation](#)

La procedura seguente descrive i principali passaggi per configurare l'ambiente in modo da poter distribuire carichi di lavoro di vRealize Automation su GCVE.

- 1 Installare e configurare Google Cloud VMware Engine in base alle istruzioni del fornitore appropriate per il proprio ambiente.
- 2 Creare account cloud di vCenter e NSX-T all'interno della distribuzione di vRealize Automation.

Utilizzo di vRealize Automation con Oracle Cloud VMware Solution

Questa procedura descrive come configurare vRealize Automation affinché funzioni con un ambiente di cloud ibrido self-service Oracle Cloud ibrido VMware Solution, in modo che sia possibile utilizzare i carichi di lavoro di vRealize Automation all'interno di questo ambiente.

vRealize Automation supporta le connessioni con Oracle Cloud VMware Solution (OCVS) per spostare ed eseguire carichi di lavoro VMware su Oracle Cloud. OCVS è stato creato da Oracle per supportare un'interfaccia con gli ambienti VMware.

L'uso di OCVS è documentato in maniera completa da Oracle. La documentazione è disponibile alla pagina seguente:

- Oracle Cloud VMware Solution - <https://docs.oracle.com/en-us/iaas/Content/VMware/Concepts/ocvsoverview.htm>

Per utilizzare OCVS, è necessario configurare account cloud sia vCenter che NSX-T. Per la configurazione di questi account cloud, consultare la documentazione seguente:

- Configurazione di account cloud vCenter: [Creazione di un account cloud di vCenter in vRealize Automation](#)
- Creazione di un account cloud NSX-T: [Creazione di un account cloud di NSX-T in vRealize Automation](#)

La procedura seguente descrive i principali passaggi per configurare l'ambiente in modo da poter distribuire carichi di lavoro di vRealize Automation su OCVS.

- 1 Installare e configurare Oracle Cloud VMware Solution in base alle istruzioni del fornitore appropriate per il proprio ambiente.
- 2 Creare account cloud di vCenter e NSX-T all'interno della distribuzione di vRealize Automation.

Utilizzo di vRealize Automation con VMware Cloud on Dell EMC

Questa procedura descrive come configurare vRealize Automation affinché funzioni con un ambiente di cloud ibrido self-service VMware Cloud on Dell EMC, in modo che sia possibile utilizzare i carichi di lavoro di vRealize Automation all'interno di questo ambiente.

vRealize Automation supporta la connessione con VMware Cloud on Dell EMC per spostare ed eseguire carichi di lavoro VMware.

Per ulteriori informazioni, vedere la documentazione di VMware Cloud on Dell EMC all'indirizzo <https://docs.vmware.com/it/VMware-Cloud-on-Dell-EMC/index.html>.

Per utilizzare vRealize Automation con VMware Cloud on Dell EMC, è necessario configurare un account cloud di vCenter. Per la configurazione di questo account cloud, consultare la documentazione seguente:

- Configurazione di account cloud vCenter: [Creazione di un account cloud di vCenter in vRealize Automation](#)

La procedura seguente descrive i principali passaggi per configurare l'ambiente in modo da poter distribuire carichi di lavoro di vRealize Automation su VMware Cloud on Dell EMC.

- 1 Installare e configurare VMware Cloud on Dell EMC in base alle istruzioni del fornitore appropriate per il proprio ambiente.
- 2 Creare un account cloud di vCenter all'interno della distribuzione di vRealize Automation.

Creazione dell'infrastruttura delle risorse di Cloud Assembly

4

Nell'infrastruttura delle risorse di Cloud Assembly si definiscono le regioni dell'account cloud come zone in cui è possibile distribuire i modelli cloud e i relativi carichi di lavoro.

L'infrastruttura delle risorse implica inoltre la creazione di mappature comuni di immagini e dimensioni delle macchine, nonché profili che definiscono le funzionalità di rete e storage nelle regioni dell'account cloud o nei data center.

Questo capitolo include i seguenti argomenti:

- Come aggiungere zone cloud che definiscano data center o regioni di posizionamento di destinazione di Cloud Assembly
- Come aggiungere le mappature delle caratteristiche in vRealize Automation per specificare le dimensioni delle macchine comuni
- Come aggiungere la mappatura delle immagini in vRealize Automation per accedere a sistemi operativi comuni
- Come aggiungere profili di rete in vRealize Automation
- Come aggiungere i profili di storage di Cloud Assembly che rappresentano requisiti diversi
- Come utilizzare le schede dei prezzi in vRealize Automation
- Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly
- Come utilizzare le risorse in vRealize Automation
- Configurazione delle risorse tenant multi-provider con vRealize Automation

Come aggiungere zone cloud che definiscano data center o regioni di posizionamento di destinazione di Cloud Assembly

Una zona cloud di Cloud Assembly è un insieme di risorse all'interno di un tipo di account cloud come AWS o vSphere.

Le zone cloud nella regione di un account specifico sono quelle in cui i modelli cloud distribuiscono i carichi di lavoro. Ogni zona cloud è associata a un progetto di Cloud Assembly.

Selezionare **Infrastruttura > Configura > Zone cloud** e fare clic su **Aggiungi nuova zona**.

Ulteriori informazioni sulle zone cloud di Cloud Assembly

Le zone cloud di Cloud Assembly sono sezioni di risorse di elaborazione specifiche per il tipo di account cloud, ad esempio AWS o vSphere.

Le zone cloud sono specifiche di una regione ed è necessario assegnarle a un progetto. Esiste una relazione molti-a-molti tra i progetti e le zone cloud. Cloud Assembly supporta la distribuzione nei cloud pubblici più diffusi, tra cui Azure, AWS e GCP, oltre che a vSphere. Vedere [Aggiunta di account cloud a Cloud Assembly](#).

I controlli di posizionamento aggiuntivi includono le opzioni dei criteri di posizionamento, i tag di funzionalità e i tag di elaborazione.

■ Criterio di posizionamento

Il criterio di posizionamento determina la selezione dell'host per le distribuzioni all'interno della zona cloud specificata.

- **predefinito:** distribuisce le risorse di elaborazione tra i cluster e le macchine host in base alla disponibilità. Ad esempio, il provisioning di tutte le macchine in una determinata distribuzione viene eseguito sul primo host applicabile.
- **binpack:** inserisce le risorse di elaborazione nell'host più carico che dispone di risorse sufficienti per eseguire la risorsa di elaborazione specificata.
- **spread:** esegue il provisioning delle risorse di elaborazione, a livello di distribuzione, nel cluster o nell'host con il minor numero di macchine virtuali. Per vSphere, Distributed Resource Scheduler (DRS) distribuisce le macchine virtuali tra gli host. Ad esempio, tutte le macchine necessarie in una distribuzione vengono posizionate nello stesso cluster, ma la distribuzione successiva può scegliere un altro cluster vSphere in base al carico corrente.

Ad esempio, si supponga di avere la seguente configurazione:

- Cluster di DRS 1 con 5 macchine virtuali
- Cluster di DRS 2 con 9 macchine virtuali
- Cluster di DRS 3 con 6 macchine virtuali

Se si richiede un cluster di 3 macchine virtuali e si seleziona un criterio spread, tutte devono essere posizionate nel cluster 1. I carichi aggiornati diventano 8 macchine virtuali per il cluster 1, mentre i carichi per i cluster 2 e 3 restano invariati a 9 e 6.

Quindi, se si richiedono altre 2 macchine virtuali, vengono posizionate nel cluster di DRS 3, che ora avrà 8 macchine virtuali. Il carico per i cluster 1 e 3 rimane invariato a 8 e 9.

Se due zone cloud corrispondono a tutti i criteri necessari per il provisioning, la logica di posizionamento seleziona quella con priorità più alta.

■ Tag di funzionalità

I blueprint contengono tag di vincoli che consentono di determinare il posizionamento della distribuzione. Durante la distribuzione, i tag di vincoli dei blueprint vengono mappati ai tag delle funzionalità corrispondenti in zone cloud e risorse di elaborazione per determinare quali zone cloud sono disponibili per il posizionamento delle risorse delle macchine virtuali.

- **Risorse di elaborazione**

È possibile visualizzare e gestire le risorse di elaborazione disponibili per eseguire il provisioning dei carichi di lavoro, ad esempio zone di disponibilità AWS e cluster di vCenter, in questa zona cloud.

Nota A partire dalla versione vRealize Automation 8.3, le zone cloud non possono più condividere risorse di elaborazione. Le zone cloud legacy che utilizzano risorse di elaborazione condivise sono comunque supportate, ma agli utenti viene richiesto di aggiornarle in modo che siano conformi agli standard correnti.

Le zone cloud generate automaticamente durante la creazione dell'account cloud sono associate alle risorse di elaborazione sottostanti dopo la raccolta dei dati.

Se un cluster di elaborazione di vCenter è abilitato per DRS, la zona cloud mostra solo il cluster nell'elenco delle elaborazioni e non mostra gli host secondari. Se un cluster di elaborazione di vCenter non è abilitato per DRS, nella zona cloud vengono visualizzati solo gli host ESXi standalone, se presenti.

Aggiungere risorse di elaborazione appropriate per la zona cloud. La scheda Risorsa di elaborazione contiene un meccanismo di filtro che consente di controllare il modo in cui le risorse di elaborazione vengono incluse nelle zone cloud. Inizialmente la selezione del filtro è Includi elaborazione completa. L'elenco seguente include le risorse di elaborazione che sono tutte disponibili per l'utilizzo nelle distribuzioni. Sono disponibili altre due opzioni per aggiungere risorse di elaborazione a una zona cloud.

- **Seleziona manualmente elaborazione:** selezionare questa opzione per scegliere manualmente le risorse di elaborazione nell'elenco seguente. Dopo averle selezionate, fare clic su **Aggiungi elaborazione** per aggiungere le risorse alla zona. Le risorse selezionate sono disponibili per l'utilizzo nelle distribuzioni.
- **Includi dinamicamente elaborazione in base ai tag:** selezionare questa opzione per includere o escludere le risorse di elaborazione per la zona in base ai tag. Vengono visualizzate tutte le risorse di elaborazione finché non vengono aggiunti tag appropriati che corrispondono a tag esistenti nelle risorse di elaborazione. Dopo aver aggiunto uno o più tag, le risorse di elaborazione con tag che corrispondono al filtro vengono incluse nella zona e sono disponibili per l'utilizzo nelle distribuzioni, mentre quelle che non corrispondono vengono escluse.

Per entrambe le opzioni di elaborazione, è possibile rimuovere una o più risorse di elaborazione visualizzate nella pagina selezionando la casella di controllo alla loro destra e facendo clic su **Rimuovi**.

I tag di elaborazione consentono di controllare ulteriormente il posizionamento. È possibile utilizzare i tag per filtrare le risorse di elaborazione disponibili per visualizzare solo quelle che corrispondono a uno o più tag, come illustrato negli esempi seguenti.

- Le risorse di elaborazione non contengono tag e non viene utilizzato alcun filtro.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

Filter tags ⓘ

⌵ TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1b	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1c	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1e	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1f	Amazon / us-east-1	Availability Zone	

6 computes

- Due risorse di elaborazione contengono lo stesso tag, ma non viene utilizzato alcun filtro.

New Cloud Zone

Summary **Compute** Projects

All compute resources listed apply to this cloud zone. Use the filter to add or remove resources from the list.

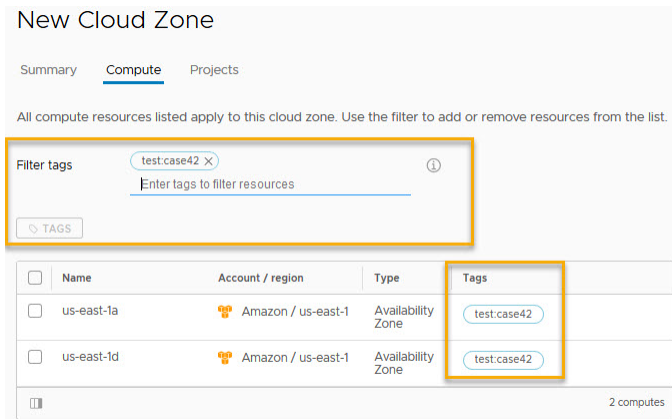
Filter tags ⓘ

⌵ TAGS

<input type="checkbox"/>	Name	Account / region	Type	Tags
<input type="checkbox"/>	us-east-1a	Amazon / us-east-1	Availability Zone	test.case42
<input type="checkbox"/>	us-east-1b	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1c	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1d	Amazon / us-east-1	Availability Zone	test.case42
<input type="checkbox"/>	us-east-1e	Amazon / us-east-1	Availability Zone	
<input type="checkbox"/>	us-east-1f	Amazon / us-east-1	Availability Zone	

6 computes

- Due risorse di elaborazione contengono lo stesso tag e il filtro dei tag corrisponde al tag utilizzato nelle due risorse.



■ Progetti

È possibile visualizzare i progetti configurati per supportare il provisioning del carico di lavoro in questa zona cloud.

Dopo aver creato una zona cloud, è possibile convalidarne la configurazione.

Dashboard Dettagli

Se si dispone di un'applicazione vRealize Operations Manager associata configurata per funzionare con vRealize Automation, è possibile accedere a un dashboard **Dettagli** nella zona cloud.

Nel dashboard vengono visualizzate le informazioni relative alla capacità delle risorse e delle distribuzioni per la zona cloud vSphere o VMware Cloud on AWS, purché gli account cloud siano configurati in vRealize Automation e vRealize Operations Manager e monitorati in vRealize Operations Manager. Per ulteriori informazioni sul dashboard **Dettagli**, vedere [Ottimizzazione di distribuzione e gestione delle risorse utilizzando metriche di vRealize Operations Manager in vRealize Automation](#).

Come aggiungere le mappature delle caratteristiche in vRealize Automation per specificare le dimensioni delle macchine comuni

Nella mappa delle caratteristiche di vRealize Automation viene utilizzato il linguaggio naturale per definire le dimensioni della distribuzione di destinazione per una regione o un account cloud specifici.

Le mappe delle caratteristiche esprimono le dimensioni della distribuzione adatte all'ambiente. Un esempio potrebbe essere *piccolo* per 1 CPU e 2 GB di memoria e *grande* per 2 CPU e 8 GB di memoria per un account di vCenter in un data center denominato e t2.nano per un account di Amazon Web Services in una regione denominata.

Selezionare **Gestione tenant > Mappature caratteristiche o Infrastruttura > Mappature caratteristiche** e fare clic su **Nuova mappatura caratteristica**.

Ulteriori informazioni sulle mappature delle caratteristiche in vRealize Automation

Una mappatura delle caratteristiche raggruppa un set di dimensioni della distribuzione di destinazione per una regione o un account cloud specifici in vRealize Automation utilizzando la denominazione del linguaggio naturale.

La mappatura delle caratteristiche consente di creare una mappatura denominata che contiene caratteristiche di dimensioni simili nelle regioni dell'account. Ad esempio, una mappa delle caratteristiche denominata `standard_small` potrebbe contenere cratteristiche di dimensioni simili (come 1 CPU, 2 GB di RAM) per alcuni o tutti gli account o le regioni disponibili nel progetto. Quando si crea un modello cloud, è possibile scegliere una caratteristica disponibile in base alle proprie esigenze.

Organizzare le mappature delle caratteristiche per il progetto in base alla finalità di distribuzione.

Per semplificare la creazione del modello cloud, è possibile selezionare un'opzione di pre-configurazione quando si aggiunge un nuovo account cloud. Quando si seleziona l'opzione di pre-configurazione, vengono selezionate la mappatura delle caratteristiche e la mappatura dell'immagine più comuni dell'organizzazione per la regione specificata.

Per quanto riguarda la mappatura delle immagini nei modelli di cloud che contengono risorse di vSphere, se non sono presenti mappature delle caratteristiche definite per una zona cloud di vSphere, è possibile configurare CPU e memoria illimitata utilizzando le impostazioni specifiche di vSphere nel modello cloud. Se sono presenti mappature delle caratteristiche definite per una zona cloud di vSphere, la mappatura delle caratteristiche funge da limite per le configurazioni specifiche di vSphere nel modello cloud.

Come aggiungere la mappatura delle immagini in vRealize Automation per accedere a sistemi operativi comuni

In una mappa dell'immagine di vRealize Automation viene utilizzato il linguaggio naturale per definire i sistemi operativi della distribuzione di destinazione per una regione o un account cloud specifici.

Selezionare **Gestione tenant > Mappature immagine** e fare clic su **Nuova mappatura immagine**.

Create Image Mapping

Account / region *

Image name *

Image *

Constraints

Tenant *

Cloud configuration

1	
---	--

Ulteriori informazioni sulle mappature dell'immagine in vRealize Automation

Una mappatura dell'immagine raggruppa un set di specifiche predefinite del sistema operativo di destinazione per una regione o un account cloud specifici in vRealize Automation utilizzando le denominazioni del linguaggio naturale.

Gli account dei fornitori di soluzioni cloud come Microsoft Azure e Amazon Web Services utilizzano le immagini per raggruppare una serie di condizioni di distribuzione di destinazione, incluso il sistema operativo e le impostazioni di configurazione correlate. Gli ambienti basati su vCenter e NSX, incluso VMware Cloud on AWS, utilizzano un meccanismo di raggruppamento simile per definire un set di condizioni di distribuzione del sistema operativo. Quando si crea, quindi si distribuisce e si itera un modello cloud, si sceglie l'immagine disponibile più adatta alle proprie esigenze.

Organizzare le mappature delle immagini per un progetto in base a impostazioni del sistema operativo, strategia di tag e scopo della distribuzione funzionale simili.

Per semplificare la creazione del modello cloud, è possibile selezionare un'opzione di pre-configurazione quando si aggiunge un nuovo account cloud. Quando si seleziona l'opzione di pre-configurazione, vengono selezionate la mappatura delle caratteristiche e la mappatura dell'immagine più comuni dell'organizzazione per la regione specificata.

Quando si aggiungono informazioni sull'immagine a un modello cloud, si utilizza la voce `image` o `imageRef` nella sezione `properties` di un componente macchina. Ad esempio, se si desidera eseguire la clonazione da uno snapshot, utilizzare la proprietà `imageRef`.

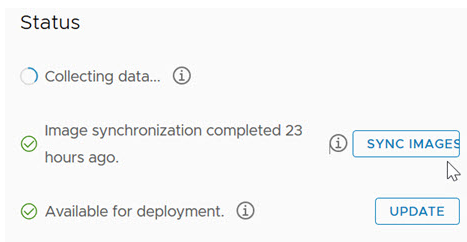
Per esempi di voci `image` e `imageRef` nel codice del modello cloud, vedere [Capitolo 6 Progettazione delle distribuzioni di Cloud Assembly](#).

Per assegnare un'autorizzazione per una libreria di contenuti, un amministratore deve concedere l'autorizzazione all'utente come autorizzazione globale. Per informazioni correlate, vedere [Ereditarietà gerarchica delle autorizzazioni per le librerie di contenuti](#) in *Amministrazione delle macchine virtuali di vSphere* nella [documentazione di VMware vSphere](#).

Sincronizzazione delle immagini per la regione o l'account cloud

È possibile eseguire la sincronizzazione delle immagini per assicurarsi che le immagini che si stanno aggiungendo o rimuovendo per una determinata regione o account cloud nella pagina **Infrastruttura > Configura > Mappatura immagine** siano aggiornate.

- 1 Aprire **la regione o l'account cloud** associati selezionando **Infrastruttura > Connessioni > Account cloud**. Selezionare una regione o un account cloud esistente.
- 2 Fare clic sul pulsante **Sincronizza immagini** e attendere il completamento dell'azione.



- 3 Al termine dell'azione, fare clic su **Infrastruttura > Configura > Mappatura immagine**. Definire una nuova mappatura immagine o modificarne una esistente, quindi selezionare la regione o l'account cloud dal passaggio 1.
- 4 Fare clic sull'icona Sincronizzazione immagine nella pagina **Mappatura immagine**.



- 5 Configurare le impostazioni delle mappature delle immagini per la regione o l'account cloud specificati nella pagina **Mappatura immagine**.

Visualizzazione dei dettagli di OVF

È possibile includere le specifiche di OVF negli oggetti del modello cloud di Cloud Assembly, come mappe delle immagini e componenti macchina di vCenter. Se l'immagine contiene un file OVF, è possibile individuarne il contenuto senza aprire il file. Passare il puntatore del mouse su OVF per visualizzarne i dettagli, tra cui nome e posizione. Per ulteriori informazioni sul formato del file OVF, vedere [vcenter ovf: property](#). Per visualizzare i dettagli di OVF, la mappatura dell'immagine deve trovarsi sul server Web.



Per informazioni correlate alla visualizzazione dei dettagli OVF utilizzando un link OVF nel campo di mappatura, vedere l'articolo esterno [Modello cloud da un OVA](#).

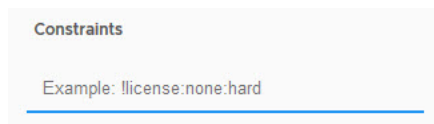
Utilizzo delle immagini condivise e più recenti di una raccolta di immagini di Microsoft Azure

Quando si creano mappature delle immagini per Microsoft Azure, è possibile selezionare immagini in una raccolta di immagini di Azure condivisa nella sottoscrizione. Vengono raccolti i dati delle immagini nel menu a discesa che vengono rese disponibili in base alla regione selezionata.

Anche se le immagini condivise possono essere utilizzate in più sottoscrizioni, non possono essere elencate nel menu a discesa di mappatura delle immagini nelle sottoscrizioni. Vengono raccolti solo i dati delle immagini di una sottoscrizione specifica, che vengono elencate nell'elenco delle mappature delle immagini. Per utilizzare un'immagine di una raccolta di immagini in una sottoscrizione diversa, specificare l'ID immagine nella mappatura delle immagini e utilizzare tale mappatura nel modello cloud.

Utilizzo di vincoli e tag per perfezionare la selezione delle immagini

Per perfezionare ulteriormente la selezione delle immagini in un modello cloud, è possibile aggiungere uno o più vincoli per specificare le limitazioni basate su tag del tipo di immagine che può essere distribuito. L'esempio di **vincoli** forniti visualizzati quando si crea o si modifica una configurazione di mappatura dell'immagine è `!license:none:hard`. L'esempio illustra una limitazione basata su tag in cui l'immagine può essere utilizzata solo se il tag `license:none` *non* è presente nel modello cloud. Se si aggiungono tag come `license:88` e `license:92`, è possibile utilizzare l'immagine specificata solo se i tag `license:88` e `license:92` *sono* presenti nel modello cloud.



Utilizzo di uno script di configurazione cloud per controllare la distribuzione

È possibile utilizzare uno script di configurazione cloud in una mappa dell'immagine, un modello cloud o entrambi per definire le caratteristiche del sistema operativo personalizzato da utilizzare in una distribuzione di Cloud Assembly. Ad esempio, a seconda che il modello cloud venga distribuito in un cloud pubblico o in un cloud privato, è possibile applicare all'immagine specifiche autorizzazioni dell'utente, autorizzazioni del sistema operativo o altre condizioni. Uno script di configurazione del cloud utilizza il formato `cloud-init` per le immagini basate su Linux o il formato `cloudbase-init` per le immagini basate su Windows. Cloud Assembly supporta lo strumento [cloud-init](#) per i sistemi Linux e lo strumento [cloudbase-init](#) per Windows.

Per le macchine Windows, è possibile utilizzare qualsiasi formato di script di configurazione cloud supportato da `cloudbase-init`.

La risorsa macchina nel codice del modello cloud di esempio seguente utilizza un'immagine che contiene uno script di configurazione cloud, il cui contenuto è visibile nella voce `image`.

```
resources:
  demo-machine:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      image: MyUbuntu16
      https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ami-ubuntu-16.04-1.10.3-00-15269239.ova
      cloudConfig: |
        ssh_pwauth: yes
        chpasswd:
          list: |
            ${input.username}:${input.password}
          expire: false
        users:
          - default
          - name: ${input.username}
            lock_passwd: false
            sudo: ['ALL=(ALL) NOPASSWD:ALL']
            groups: [wheel, sudo, admin]
            shell: '/bin/bash'
        runcmd:
          - echo "Defaults:${input.username} !requiretty" >> /etc/sudoers.d/${input.username}
```

La valutazione dinamica delle proprietà funziona quando si utilizza `cloudConfig` direttamente in un modello cloud, ma non è supportata per `cloudConfig` in una mappa dell'immagine.

Nel codice del modello cloud, utilizzare l'impostazione `image` per fare riferimento a un'immagine definita come mappatura dell'immagine. È possibile utilizzare l'impostazione `imageRef` per identificare un modello che contiene uno snapshot (per i cloni collegati), un modello di immagine o un file OVF del modello della libreria di contenuti.

Che cosa succede quando una mappatura dell'immagine e un modello cloud contengono uno script di configurazione cloud

Quando un modello cloud che contiene uno script di configurazione cloud utilizza una mappatura dell'immagine che contiene uno script di configurazione cloud, entrambi gli script vengono combinati. L'azione di unione elabora innanzitutto il contenuto dello script di mappatura dell'immagine e poi il contenuto dello script del modello cloud, tenendo in considerazione la possibilità che gli script siano in formato `#cloud-config` o meno.

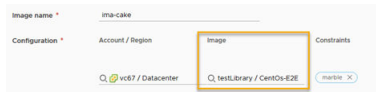
- Per gli script che si trovano nel formato `#cloud-config`, l'unione combina il contenuto di ciascun modulo (ad esempio `runcmd`, `users` e `write_files`) come segue:
 - Per i moduli in cui il contenuto è un elenco, gli elenchi di comandi dalla mappatura dell'immagine e dal modello cloud vengono uniti, escludendo i comandi che sono identici in entrambi gli elenchi.

- Per i moduli in cui il contenuto è un dizionario, i comandi vengono uniti e il risultato è una combinazione di entrambi i dizionari. Se la stessa chiave esiste in entrambi i dizionari, la chiave del dizionario dello script di mappatura dell'immagine viene mantenuta e la chiave dal dizionario dello script del modello cloud viene ignorata.
- Per i moduli in cui il contenuto è una stringa, i valori dei contenuti dello script di mappatura dell'immagine vengono mantenuti e i valori dei contenuti dello script del modello cloud vengono ignorati.
- Per gli script che sono in un formato diverso da `#cloud-config` o quando uno script è in formato `#cloud-config` e l'altro non lo è, entrambi gli script vengono combinati in modo che lo script di mappatura dell'immagine venga eseguito per primo e lo script del modello cloud venga eseguito quando lo script di mappatura dell'immagine è terminato.

Per informazioni correlate, vedere [Unione di sezioni di dati utente](#).

Aggiunta di un'immagine da una libreria dei contenuti di vCenter

Quando una libreria di contenuti locale o di un autore si trova in un vCenter gestito dall'organizzazione di vRealize Automation, le immagini dei modelli della libreria di contenuti vengono visualizzate nel menu a discesa delle immagini. Le immagini elencate includono immagini dei modelli di macchine virtuali e OVF nelle librerie di contenuti di vCenter locali o degli autori. Le immagini delle librerie di contenuti dei sottoscrittori non vengono visualizzate nel menu a discesa. Il modello da cui è stata clonata una macchina virtuale viene visualizzato nella sezione dei dettagli della macchina dell'interfaccia utente delle distribuzioni della macchina.



Nota Se la libreria di contenuti dell'autore vCenter è gestita da vRealize Automation, le informazioni sull'autore vengono visualizzate nella griglia di selezione della mappatura dell'immagine nel seguente formato: *publisher_content_library_name / content_item_name*

Per assegnare un'autorizzazione per una libreria di contenuti, un amministratore deve concedere l'autorizzazione all'utente come autorizzazione globale. Per informazioni correlate, vedere [Ereditarietà gerarchica delle autorizzazioni per le librerie di contenuti](#) in *Amministrazione delle macchine virtuali di vSphere* nella [documentazione di VMware vSphere](#).

Se la libreria di contenuti dell'autore vCenter non è gestita da vRealize Automation, le informazioni sul sottoscrittore vengono visualizzate nella griglia di selezione della mappatura dell'immagine nel seguente formato: *subscriber_content_library_name / content_item_name*

Ad esempio, nello scenario seguente solo gli elementi della libreria di contenuti dell'iscritto sono visibili nell'elenco di mappatura delle immagini vRealize Automation:

- Per un vCenter denominato VC-1, esiste una libreria di contenuti di un iscritto in VC e in vRealize Automation viene creato un account cloud associato a VC-1.
- Per un vCenter denominato VC-2, esiste una libreria di contenuti di un editore in VC a cui è sottoscritta la libreria di contenuti dell'iscritto a VC-1. Tuttavia, in vRealize Automation non è presente alcun account cloud associato a VC-2.

Poiché VC-1 è associato a un account cloud vRealize Automation, la libreria di contenuti dell'iscritto è disponibile in vRealize Automation. Il suo contenuto viene raccolto e visualizzato nell'elenco delle mappature delle immagini vRealize Automation. Tuttavia, poiché VC-2 non è associato a un account cloud, vRealize Automation non conosce la propria libreria di contenuti dell'editore. Per visualizzare gli elementi della libreria di contenuti dell'editore nell'elenco di mappatura dell'immagine è necessario associare un account cloud a vCenter VC-2.

Quando si distribuisce un modello cloud che contiene la mappatura di un'immagine del modello di macchina virtuale, vRealize Automation tenta di accedere all'immagine mappata nella libreria di contenuti più vicina al datastore, e quindi più vicina all'host, della macchina da sottoporre a provisioning. Ciò può includere una libreria di contenuti locale nonché una libreria di contenuti di un autore o un sottoscrittore.

Quando si distribuisce un modello cloud che contiene la mappatura di un'immagine del modello OVF, si accede alle immagini OVF come specificato nella riga della mappatura dell'immagine se l'immagine si trova in una libreria di contenuti locale o un sottoscrittore locale di una libreria di contenuti di un autore remota specificata.

Per informazioni relative alla creazione e all'utilizzo delle librerie dei contenuti di vCenter, vedere [Utilizzo delle librerie dei contenuti](#) nella [documentazione di prodotto di vSphere](#) e nel post di blog [Come utilizzare le librerie dei contenuti in vRealize Automation 8 e vRealize Automation Cloud](#).

Ulteriori informazioni sulla configurazione e l'utilizzo degli script di configurazione cloud

Per ulteriori informazioni sull'utilizzo degli script di configurazione cloud nei modelli cloud, vedere [Inizializzazione della macchina in Cloud Assembly](#).

Vedere anche gli articoli del blog di VMware sulla [personalizzazione di vSphere con cloud-init durante l'utilizzo di vRealize Automation 8 o Cloud](#) e sulla [personalizzazione delle distribuzioni di Cloud Assembly con cloud-init](#).

Come aggiungere profili di rete in vRealize Automation

Un profilo di rete di vRealize Automation descrive il comportamento della rete da distribuire.

Ad esempio, potrebbe essere necessario che una rete sia rivolta a Internet anziché solo interna.

Le reti e i relativi profili sono specifici del cloud.

Selezionare **Infrastruttura > Configura > Profili di rete** e fare clic su **Nuovo profilo di rete**.

Ulteriori informazioni sui profili di rete in vRealize Automation

Un profilo di rete definisce un gruppo di reti e impostazioni di rete disponibili per un account cloud in una particolare regione o data center in vRealize Automation.

In genere, è possibile definire i profili di rete per supportare un ambiente di distribuzione di destinazione, ad esempio un piccolo ambiente di test in cui una rete esistente dispone solo dell'accesso in uscita o un grande ambiente di produzione con bilanciamento del carico che richiede un set di criteri di protezione. Si pensi a un profilo di rete come a una raccolta di caratteristiche di rete specifiche del carico di lavoro.

Contenuto di un profilo di rete

Un profilo di rete contiene informazioni specifiche per un tipo di account cloud e una regione denominati in vRealize Automation, incluse le seguenti impostazioni:

- Regione o account cloud denominati e tag di funzionalità opzionali per il profilo di rete.
- Reti esistenti denominate e relative impostazioni.
- Criteri di rete che definiscono su richiesta e altri aspetti del profilo di rete.
- Inclusione facoltativa di bilanciamenti del carico esistenti.
- Inclusione facoltativa di gruppi di sicurezza esistenti.

È possibile determinare la funzionalità di gestione IP di rete in base al profilo di rete.

I tag di funzionalità dei profili di rete vengono abbinati ai tag dei vincoli nei modelli cloud per consentire di controllare la selezione della rete. Inoltre, tutti i tag assegnati alle reti raccolte dal profilo di rete vengono abbinati anche ai tag nel modello cloud per consentire di controllare la selezione della rete quando il modello cloud viene distribuito.

I tag di funzionalità sono facoltativi. I tag di funzionalità vengono applicati a tutte le reti nel profilo di rete, ma solo se le reti vengono utilizzate come parte del profilo di rete. Per i profili di rete che non contengono tag di funzionalità, la corrispondenza dei tag si verifica solo sui tag di rete. Le impostazioni di rete e sicurezza definite nel profilo di rete corrispondente vengono applicate quando il modello cloud viene distribuito.

Quando si utilizza l'IP statico, l'intervallo di indirizzi è gestito da vRealize Automation. Per DHCP, gli indirizzi di inizio e fine IP sono gestiti dal server DHCP indipendente, non da vRealize Automation. Quando si utilizza l'allocazione di indirizzi di rete DHCP o misti, il valore di utilizzo della rete è impostato su zero. Un intervallo allocato della rete su richiesta si basa sulla dimensione CIDR e subnet specificata nel profilo di rete. Per supportare l'assegnazione statica e dinamica nella distribuzione, l'intervallo allocato viene suddiviso in due intervalli, uno per l'allocazione statica e un altro per l'allocazione dinamica.

Reti

Le reti, definite anche subnet, sono suddivisioni logiche di una rete IP. Una rete raggruppa un account cloud, un indirizzo IP o un intervallo e tag di rete per controllare come e dove eseguire il provisioning di una distribuzione del modello cloud. I parametri di rete nel profilo definiscono il modo in cui le macchine nella distribuzione possono comunicare tra loro tramite il layer IP 3. Le reti possono disporre di tag.

È possibile aggiungere reti al profilo di rete, modificare gli aspetti delle reti utilizzate dal profilo di rete e rimuovere le reti dal profilo di rete.

Quando si aggiunge una rete al profilo di rete, è possibile selezionare le reti disponibili da un elenco filtrato di reti vSphere e NSX. Se il tipo di rete è supportato per il tipo di account cloud, è possibile aggiungerlo al profilo di rete.

In una distribuzione basata su VCF, i segmenti di rete NSX vengono creati in locale nella rete NSX-T e non vengono creati come reti globali.

■ Dominio di rete o Zona di trasporto

Un dominio di rete o una zona di trasporto è il commutatore virtuale distribuito (dvSwitch) per vSphere vNetwork Distributed PortGroups (dvPortGroup). Una *zona di trasporto* è un concetto di NSX esistente simile a termini quali *dvSwitch* o *dvPortGroup*.

Quando si utilizza un account cloud di NSX, il nome dell'elemento nella pagina è **Zona di trasporto**. In caso contrario, è **Dominio di rete**.

Per i commutatori standard, il dominio di rete o la zona di trasporto è lo stesso del commutatore. Il dominio di rete o la zona di trasporto definisce i limiti delle subnet all'interno di vCenter.

Una zona di trasporto controlla quali host sono raggiungibili da un commutatore logico di NSX. Può estendersi in uno o più cluster di vSphere. Le zone di trasporto controllano quali cluster e macchine virtuali possono partecipare all'uso di una determinata rete. Le subnet che appartengono alla stessa zona di trasporto di NSX possono essere utilizzate per gli stessi host delle risorse della macchina.

- **Dominio**

Rappresenta il nome di dominio per la macchina. Il nome del dominio viene passato alla specifica di personalizzazione della macchina vSphere.

- **Gateway predefinito IPv4 CIDR e IPv4**

I componenti della macchina vSphere nel modello cloud supportano l'assegnazione di IPv4, IPv6 e IP dual stack per le interfacce di rete. Ad esempio, 192.168.100.14/24 rappresenta l'indirizzo IPv4 192.168.100.14 e il relativo prefisso di routing associato 192.168.100.0 o, in modo equivalente, la subnet mask 255.255.255.0, che ha 24 bit 1 iniziali. Il blocco di IPv4 192.168.100.0/22 rappresenta i 1024 indirizzi IP da 192.168.100.0 a 192.168.103.255.

- **Gateway predefinito IPv6 CIDR e IPv6**

I componenti della macchina vSphere nel modello cloud supportano l'assegnazione di IPv4, IPv6 e IP dual stack per le interfacce di rete. Ad esempio, 2001:db8::/48 rappresenta il blocco di indirizzi IPv6 da 2001:db8:0:0:0:0:0:0 a 2001:db8:0:ffff:ffff:ffff:ffff:ffff.

Il formato IPv6 non è supportato per le reti su richiesta.

- **Server DNS e Domini di ricerca DNS**

- **IP pubblico di supporto**

Selezionare questa opzione per contrassegnare la rete come pubblica. I componenti di rete in un modello cloud con una proprietà `network type: public` vengono associati alle reti contrassegnate come pubbliche. Si verifica una maggiore corrispondenza durante la distribuzione del modello cloud per determinare la selezione della rete.

- **Valore predefinito per la zona**

Selezionare questa opzione per contrassegnare la rete come predefinita per la zona cloud. Durante la distribuzione del modello cloud, le reti predefinite vengono preferite rispetto ad altre reti.

- **Origine**

Identifica l'origine della rete.

- **Tag**

Specifica una o più etichette assegnate alla rete. I tag sono facoltativi. La corrispondenza dei tag influisce sulle reti disponibili per le distribuzioni dei modelli cloud.

I tag di rete esistono nell'elemento di rete stesso, indipendentemente dal profilo di rete. I tag di rete si applicano a ogni occorrenza della rete a cui sono stati aggiunti e a tutti i profili di rete che contengono tale rete. Le reti possono essere integrate in un numero qualsiasi di profili di rete. Indipendentemente dalla residenza del profilo di rete, un tag di rete è associato a tale rete ovunque venga utilizzata.

Quando si distribuisce un modello cloud, i tag di vincolo nei componenti di rete di un modello cloud vengono abbinati ai tag di rete, inclusi i tag della funzionalità del profilo di rete. Per i profili di rete che contengono tag di funzionalità, i tag di funzionalità vengono applicati a tutte le reti disponibili per tale profilo di rete. Le impostazioni di rete e sicurezza definite nel profilo di rete corrispondente vengono applicate quando il modello cloud viene distribuito.

Criteri di rete

Utilizzando i profili di rete, è possibile definire le subnet per i domini di rete esistenti che contengono indirizzi IP statici, DHCP o una combinazione di impostazioni di indirizzi IP statici e DHCP. È possibile definire le subnet e specificare le impostazioni degli indirizzi IP utilizzando la scheda **Criteri di rete**.

Quando si utilizza NSX-V, NSX-T o VMware Cloud on AWS, le impostazioni dei criteri di rete vengono utilizzate quando un modello cloud richiede `networkType: outbound` o `networkType: private` o quando una rete NSX richiede `networkType: routed`.

In base all'account cloud associato, è possibile utilizzare i criteri di rete per definire le impostazioni per i tipi di rete `outbound`, `private` e `routed` e per i gruppi di sicurezza su richiesta. È inoltre possibile utilizzare i criteri di rete per controllare le reti `existing` quando è associato un bilanciamento del carico a tale rete.

Le reti in uscita consentono l'accesso unidirezionale alle reti upstream. Le reti private non consentono alcun accesso esterno. Le reti instradate consentono il traffico est/ovest tra le reti instradate. Le reti pubbliche e quelle esistenti nel profilo vengono utilizzate come reti sottostanti o upstream.

Le opzioni per le seguenti selezioni su richiesta sono descritte nella guida su schermo **Profili di rete** e riepilogate di seguito.

- **Non creare una rete su richiesta o un gruppo di sicurezza su richiesta**

È possibile utilizzare questa opzione quando si specifica un tipo di rete `existing` o `public`. I modelli cloud che richiedono una rete `outbound`, `private` o `routed` non corrispondono a questo profilo.

- **Crea una rete su richiesta**

È possibile utilizzare questa opzione quando si specifica un tipo di rete `outbound`, `private` o `routed`.

Amazon Web Services, Microsoft Azure, NSX, vSphere e VMware Cloud on AWS supportano questa opzione.

- **Crea un gruppo di sicurezza su richiesta**

È possibile utilizzare questa opzione quando si specifica un tipo di rete `outbound` o `private`.

Se il tipo di rete è `outbound` o `private`, viene creato un nuovo gruppo di sicurezza per i modelli cloud con corrispondenze.

Amazon Web Services, Microsoft Azure, NSX e VMware Cloud on AWS supportano questa opzione.

Le impostazioni dei criteri di rete possono essere specifiche per il tipo di account cloud. Queste impostazioni sono descritte nella guida su schermo e riepilogate di seguito:

- **Dominio di rete o Zona di trasporto**

Un dominio di rete o una zona di trasporto è il commutatore virtuale distribuito (dvSwitch) per vSphere vNetwork Distributed PortGroups (dvPortGroup). Una *zona di trasporto* è un concetto di NSX esistente simile a termini quali *dvSwitch* o *dvPortGroup*.

Quando si utilizza un account cloud di NSX, il nome dell'elemento nella pagina è **Zona di trasporto**. In caso contrario, è **Dominio di rete**.

Per i commutatori standard, il dominio di rete o la zona di trasporto è lo stesso del commutatore. Il dominio di rete o la zona di trasporto definisce i limiti delle subnet all'interno di vCenter.

Una zona di trasporto controlla quali host sono raggiungibili da un commutatore logico di NSX. Può estendersi in uno o più cluster di vSphere. Le zone di trasporto controllano quali cluster e macchine virtuali possono partecipare all'uso di una determinata rete. Le subnet che appartengono alla stessa zona di trasporto di NSX possono essere utilizzate per gli stessi host delle risorse della macchina.

- **Subnet esterna**

Una rete su richiesta con accesso in uscita richiede una subnet esterna con accesso in uscita. La subnet esterna viene utilizzata per fornire l'accesso in uscita se richiesto nel modello cloud. Non controlla il posizionamento della rete. Ad esempio, la subnet esterna non influisce sul posizionamento di una rete privata.

- **CIDR**

La notazione CIDR è una rappresentazione compatta di un indirizzo IP e del relativo prefisso di routing associato. Il valore CIDR specifica l'intervallo di indirizzi di rete da utilizzare durante il provisioning per creare le subnet. Questa impostazione CIDR nella scheda **Criteri di rete** accetta la notazione IPv4 che termina con /nn e contiene valori compresi tra 0-32.

- **Dimensioni subnet**

Questa opzione consente di specificare le dimensioni della rete su richiesta, utilizzando la notazione IPv4, per ogni rete isolata in una distribuzione che utilizza questo profilo di rete. L'impostazione delle dimensioni della subnet è disponibile per la gestione degli indirizzi IP interni o esterni.

Il formato IPv6 non è supportato per le reti su richiesta.

- **Router logico distribuito**

Ad esempio, per una rete instradata su richiesta, è necessario specificare una rete logica distribuita quando si utilizza un account cloud di NSX-V.

Un DLR (Distributed Logical Router) viene utilizzato per instradare il traffico est/ovest tra reti instradate su richiesta in NSX-V. Questa opzione è visibile solo se il valore dell'account/regione per il profilo di rete è associato a un account cloud di NSX-V.

■ **Assegnazione intervallo IP**

L'opzione è disponibile per gli account cloud che supportano NSX o VMware Cloud on AWS, incluso vSphere.

L'impostazione dell'intervallo IP è disponibile quando si utilizza una rete esistente con un punto di integrazione IPAM esterno.

È possibile selezionare una delle tre opzioni seguenti per specificare un tipo di assegnazione dell'intervallo IP per la rete di distribuzione:

■ **Statico e DHCP**

Predefinito e consigliato. Questa opzione mista utilizza le impostazioni **CIDR** e **Intervallo di subnet** allocate per configurare il pool di server DHCP affinché supporti la metà dell'allocazione dello spazio degli indirizzi utilizzando il metodo DHCP (dinamico) e la metà dell'allocazione dello spazio di indirizzi IP utilizzando il metodo statico. Utilizzare questa opzione quando alcune macchine connesse a una rete su richiesta richiedono indirizzi IP statici assegnati e alcune richiedono indirizzi IP dinamici. Vengono creati due intervalli IP.

Questa opzione è più efficace nelle distribuzioni con macchine connesse a una rete su richiesta, in cui ad alcune delle macchine vengono assegnati IP statici e ad altre macchine IP dinamicamente assegnati da un server DHCP di NSX e distribuzioni in cui il VIP di bilanciamento del carico è statico.

■ **DHCP (dinamico)**

Questa opzione utilizza il CIDR allocato per configurare un pool di IP in un server DHCP. Tutti gli indirizzi IP per questa rete vengono assegnati dinamicamente. Viene creato un singolo intervallo IP per ogni CIDR allocato.

■ **Statico**

Questa opzione utilizza il CIDR allocato per allocare staticamente gli indirizzi IP. Utilizzare questa opzione quando non è necessario configurare un server DHCP per questa rete. Viene creato un singolo intervallo IP per ogni CIDR allocato.

■ **Blocchi IP**

L'impostazione dei blocchi IP è disponibile quando si utilizza una rete su richiesta con un punto di integrazione IPAM esterno.

Utilizzando questa impostazione, è possibile aggiungere un blocco o un intervallo IP denominato al profilo di rete dal provider IPAM esterno integrato. È inoltre possibile rimuovere un blocco IP aggiunto dal profilo di rete. Per informazioni su come creare un'integrazione IPAM esterna, vedere [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#).

L'IPAM esterno è disponibile per i seguenti tipi di account cloud o regione:

- vSphere
- vSphere con NSX-T
- vSphere con NSX-V
- **Risorse di rete - Rete esterna**

Le reti esterne sono denominate anche reti esistenti. Queste reti sono state raccolte in base ai dati e rese disponibili per la selezione.

- **Risorse di rete - Router logico di livello 0**

NSX-T utilizza il router logico di livello 0 come gateway per le reti esterne alla distribuzione NSX. Il router logico di livello 0 configura l'accesso in uscita per le reti su richiesta.

- **Risorse di rete - Cluster edge**

Il cluster edge specificato fornisce servizi di routing. Il cluster edge viene utilizzato per configurare l'accesso in uscita per le reti su richiesta e i bilanciamenti del carico. Identifica il cluster edge o il pool di risorse in cui deve essere distribuita l'appliance edge.

- **Risorse di rete - Datastore edge**

Identifica il datastore edge specificato utilizzato per eseguire il provisioning dell'appliance edge. Questa impostazione si applica solo a NSX-V.

I tag possono essere utilizzati per specificare quali reti sono disponibili per il modello cloud.

Bilanciamenti del carico

È possibile aggiungere bilanciamenti del carico al profilo di rete. I bilanciamenti del carico elencati sono disponibili in base ai dati raccolti dalle informazioni dell'account cloud di origine.

Se un tag in uno qualsiasi dei bilanciamenti del carico nel profilo di rete corrisponde a un tag in un componente del bilanciamento del carico nel modello cloud, il bilanciamento del carico viene considerato durante la distribuzione. I bilanciamenti del carico in un profilo di rete corrispondente vengono utilizzati quando viene distribuito un modello cloud.

Per ulteriori informazioni, vedere [Utilizzo delle impostazioni del bilanciamento del carico nei profili di rete in vRealize Automation](#) e [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Gruppi di sicurezza

Quando viene distribuito un modello cloud, i gruppi di sicurezza nel profilo di rete vengono applicati alle schede NIC delle macchine sottoposte a provisioning. Per un profilo di rete specifico di Amazon Web Services, i gruppi di sicurezza nel profilo di rete sono disponibili nello stesso dominio di rete (VPC) delle reti elencate nella scheda Reti. Se nella scheda Reti del profilo di rete non è elencata alcuna rete, vengono visualizzati tutti i gruppi di sicurezza disponibili.

È possibile utilizzare un gruppo di sicurezza per definire ulteriormente le impostazioni di isolamento per una rete `private` o `outbound` su richiesta. I gruppi di sicurezza vengono applicati anche alle reti `existing`. È inoltre possibile assegnare gruppi di sicurezza globali.

I gruppi di sicurezza elencati sono disponibili in base ai dati raccolti dalle informazioni dall'account cloud di origine o aggiunte come gruppo di sicurezza su richiesta nel modello cloud di un progetto. Per ulteriori informazioni, vedere [Risorse di sicurezza in vRealize Automation](#).

I gruppi di sicurezza vengono applicati a tutte le macchine della distribuzione connesse alla rete che corrisponde al profilo di rete. Poiché in un modello cloud potrebbero essere presenti più reti, ognuna delle quali corrispondente a un profilo di rete diverso, è possibile utilizzare gruppi di sicurezza differenti per reti diverse.

Nota Oltre a specificare un gruppo di sicurezza, è possibile selezionare anche reti NSX (impostazione predefinita) oppure reti vSphere o entrambe. Quando si distribuisce un modello cloud, vRealize Automation aggiunge il gruppo di sicurezza allocato o specificato alle schede NIC delle macchine connesse alla rete NSX allocata. Solo le schede NIC delle macchine connesse a una rete NSX possono essere aggiunte a un gruppo di sicurezza di NSX. Se la scheda NIC della macchina è connessa a una rete vSphere, la distribuzione del modello non riesce.

L'aggiunta di un'etichetta a un gruppo di sicurezza esistente consente di utilizzare il gruppo di sicurezza in un componente `Cloud.SecurityGroup` del modello cloud. Un gruppo di sicurezza deve avere almeno un tag o non può essere utilizzato in un modello cloud. Per ulteriori informazioni, vedere [Risorse di sicurezza in vRealize Automation](#) e [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Ulteriori informazioni su profili di rete, reti, modelli cloud e tag

Per ulteriori informazioni sulle reti, vedere [Risorse di rete in vRealize Automation](#).

Per esempi di codice del componente di rete di esempio in un modello cloud, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Per i workflow di automazione di rete di esempio, vedere [Automazione della rete con Cloud Assembly e NSX](#).

Per ulteriori informazioni sui tag e sulla strategia di tag, vedere [Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly](#).

Per informazioni sulla denominazione delle schede NIC delle macchine, vedere [Come configurare il nome di un controller dell'interfaccia di rete utilizzando le azioni di estendibilità](#).

Utilizzo delle impostazioni di rete in profili di rete e progettazioni di modelli cloud in vRealize Automation

Le reti e i profili di rete vengono utilizzati in vRealize Automation per consentire di definire il comportamento del provisioning di rete per le distribuzioni.

In vRealize Automation è possibile definire profili di rete specifici del cloud. Vedere [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

Utilizzando le impostazioni di reti e profili di rete, è possibile controllare il modo in cui gli indirizzi IP di rete vengono utilizzati nelle distribuzioni e nei modelli cloud di vRealize Automation.

Supporto di IPv4 e IPv6 nelle reti di vRealize Automation

Le reti di vRealize Automation supportano IPv4 single stack, IPv6 single stack o IPv4 dual stack e IPv6 con dual stack.

IPv6 è supportato per le reti di vSphere esistenti e per le reti di NSX esistenti.

IPv6 non è supportato per i bilanciamenti del carico, le reti su richiesta NSX o i provider IPAM di terze parti esterni come Infoblox.

Supporto dei provider IPAM esterno

Oltre al supporto IPAM interno fornito, è possibile utilizzare un provider IPAM esterna per allocare dinamicamente o in modo statico l'indirizzo IP per le reti, in forma di intervalli IP per le reti esistenti nei progetti di modelli cloud e nelle distribuzioni e di blocchi IP per le reti su richiesta nei progetti di modelli cloud e nelle distribuzioni.

Il supporto per i provider IPAM esterni, ad esempio Infoblox, è disponibile per i punti di integrazione IPAM specifici del fornitore creati tramite la sequenza di menu **Infrastruttura > Connessioni > Aggiungi integrazione > IPAM**.

Le opzioni per la definizione delle informazioni sugli indirizzi del provider IPAM esterna sono disponibili utilizzando l'opzione **Aggiungi intervallo IP IPAM** nella pagina **Criteri di rete > Aggiungi intervallo IP IPAM**.

Per informazioni su come creare un punto di integrazione IPAM esterno, vedere [Come configurare un'integrazione IPAM esterna in vRealize Automation](#). Per un esempio di come creare un punto di integrazione IPAM per un fornitore IPAM specifico, vedere [Tutorial: configurazione dell'integrazione di un provider IPAM esterno specifico del provider per vRealize Automation](#).

Tipi di rete

Un componente di rete in un modello cloud è definito come uno dei seguenti tipi di `networkType`.

Tipo di rete	Definizione
<code>existing</code>	<p>Seleziona una rete esistente configurata nel fornitore di soluzioni cloud sottostante, ad esempio vCenter, Amazon Web Services e Microsoft Azure. Una rete esistente è richiesta dalla rete su richiesta di <code>outbound</code>.</p> <p>È possibile definire un intervallo di indirizzi IP statici in una rete esistente.</p>
<code>public</code>	<p>Le macchine in una rete pubblica sono accessibili da Internet. Un amministratore IT definisce queste reti. La definizione di una rete <code>public</code> è identica a quella di una rete <code>existing</code> per le reti che consentono il traffico di rete nelle reti pubbliche.</p>

Tipo di rete	Definizione
private	<p>Un tipo di rete su richiesta.</p> <p>Limita il traffico di rete in modo che si verifichi solo tra le risorse della rete distribuita. Impedisce il traffico in entrata e in uscita. In NSX, può essere equiparato a NAT su richiesta one-to-many.</p>
outbound	<p>Un tipo di rete su richiesta.</p> <p>Limita il traffico di rete in modo che si verifichi tra le risorse di elaborazione nella distribuzione, ma consente anche il traffico di rete in uscita unidirezionale. In NSX, può essere equiparato a NAT su richiesta one-to-many con IP esterno.</p>
routed	<p>Un tipo di rete su richiesta.</p> <p>Le reti instradate contengono uno spazio degli indirizzi IP instradabili suddiviso tra le subnet disponibili collegate tra loro. 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 una rete esistente.</p> <p>Le reti instradate sono un tipo di rete su richiesta disponibile per le reti NSX-V e NSX-T. Microsoft Azure e Amazon Web Services forniscono questa connettività per impostazione predefinita.</p> <p>Una rete <code>routed</code> è disponibile solo per la specifica del modello cloud in un componente di rete <code>Cloud.NSX.Network</code>.</p>

Per ulteriori informazioni, vedere [Ulteriori informazioni sulle risorse di rete nei modelli cloud di vRealize Automation](#).

Per esempi di modelli cloud compilati che contengono dati dei componenti di rete, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Esempi di scenari di rete

Quando si distribuisce un modello cloud che utilizza la seguente configurazione del profilo di rete seguente, è possibile prevedere il comportamento descritto di seguito.

Scenario o tipo di rete	Nessun profilo di rete disponibile per la zona cloud	Profili di rete disponibili per la zona cloud
Nessuna rete	<p>Se nel modello cloud non viene specificata alcuna rete, viene selezionata una rete casuale dalla stessa regione di provisioning della risorsa di elaborazione.</p> <p>La preferenza viene data alle reti etichettate come predefinite.</p> <p>Se non esistono reti in una regione di provisioning disponibile, il provisioning non riesce.</p>	<p>Viene selezionata una rete da un profilo di rete corrispondente.</p> <p>La preferenza viene data alle reti etichettate come predefinite.</p> <p>Se nessuno dei profili di rete soddisfa i criteri, il provisioning non riesce.</p>
Rete esistente	<p>Se il componente di rete nel modello cloud contiene tag di vincoli, tali vincoli vengono utilizzati per filtrare l'elenco delle reti disponibili. I tag di vincoli nel componente di rete del modello cloud vengono confrontati con i tag di rete e, se disponibili, con i tag di vincoli del profilo di rete.</p> <p>Nell'elenco filtrato delle reti, viene selezionata una singola rete dalla stessa regione di provisioning della risorsa di elaborazione.</p> <p>La preferenza viene data alle reti etichettate come predefinite.</p> <p>Se dopo aver applicato il filtro in base ai vincoli non sono presenti reti nella regione di provisioning, il provisioning non riesce.</p>	<p>Viene selezionata una rete da un profilo di rete corrispondente.</p> <p>La preferenza viene data alle reti etichettate come predefinite.</p> <p>Se nessuno dei profili di rete soddisfa i criteri, il provisioning non riesce.</p> <p>I vincoli di rete possono essere utilizzati per filtrare le reti esistenti nel profilo in base ai tag pre-assegnati.</p>
Rete pubblica	<p>Se la rete dispone di vincoli, tali vincoli vengono utilizzati per filtrare l'elenco delle reti disponibili con l'attributo <code>supports public IP</code> impostato.</p> <p>Nell'elenco filtrato delle reti, viene selezionata una rete casuale dalla stessa regione di provisioning della risorsa di elaborazione.</p> <p>La preferenza viene data alle reti etichettate come predefinite.</p> <p>Se dopo avere applicato il filtro in base ai vincoli non sono presenti reti pubbliche nella regione di provisioning, il provisioning non riesce.</p>	<p>Viene selezionata una rete con l'attributo <code>supports public IP</code> da un profilo di rete corrispondente.</p> <p>La preferenza viene data alle reti etichettate come predefinite.</p> <p>I vincoli di rete possono essere utilizzati per filtrare le reti pubbliche esistenti nel profilo in base ai tag pre-assegnati.</p>

Scenario o tipo di rete	Nessun profilo di rete disponibile per la zona cloud	Profili di rete disponibili per la zona cloud
Rete privata	Il provisioning non riesce perché le reti private richiedono informazioni da un profilo di rete.	Vengono creati una nuova rete o un nuovo gruppo di sicurezza in base alle impostazioni nel profilo di rete corrispondente. I tag dei vincoli di rete possono essere utilizzati per filtrare i profili di rete e le reti.
Rete in uscita	Il provisioning non riesce perché le reti in uscita richiedono informazioni da un profilo di rete.	Vengono creati una nuova rete o un nuovo gruppo di sicurezza in base alle impostazioni nel profilo di rete corrispondente. I tag dei vincoli di rete possono essere utilizzati per filtrare i profili di rete e le reti.
Rete instradata su richiesta	Il provisioning non riesce perché le reti instradate richiedono informazioni da un profilo di rete.	Per NSX-V è necessaria la selezione DLR (Distributed Logical Router). Per NSX-T e VMware Cloud on AWS è necessario che le impostazioni su richiesta siano simili a quelle delle reti private e delle reti in uscita.
Esempio di caso d'uso di Wordpress con reti pubbliche o esistenti	Il provisioning si verifica come descritto per una rete esistente o una rete pubblica.	Vedere le descrizioni sopra indicate per il comportamento della rete esistente e della rete pubblica. Vedere Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly .
Esempio di caso d'uso di Wordpress con reti pubbliche o esistenti e reti private o in uscita	Il provisioning non riesce perché la rete richiede informazioni da un profilo di rete.	Vedere le descrizioni precedenti per una rete privata e una rete in uscita. Vedere Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly .
Esempio di caso d'uso di Wordpress con bilanciamento del carico	Il provisioning non riesce perché un bilanciamento del carico richiede informazioni da un profilo di rete. Il provisioning può verificarsi quando sono presenti bilanciamenti del carico esistenti.	Viene creato un nuovo bilanciamento del carico in base alla configurazione del profilo di rete. È possibile specificare un bilanciamento del carico esistente attivato nel profilo di rete. Il provisioning non riesce se si richiede un bilanciamento del carico esistente, ma nessuno di essi soddisfa i vincoli nel profilo di rete. Vedere Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly .

Utilizzo delle impostazioni dei gruppi di sicurezza in profili di rete e progettazioni di modelli cloud in vRealize Automation

È possibile definire e modificare le impostazioni dei gruppi di sicurezza in profili di rete e in progettazioni di modelli cloud.

È possibile utilizzare le funzionalità dei gruppi di sicurezza in diversi modi:

- Gruppo di sicurezza esistente specificato in un profilo di rete

È possibile aggiungere un gruppo di sicurezza esistente a un profilo di rete. Quando una progettazione di modelli cloud utilizza tale profilo di rete, le relative macchine vengono raggruppate come membri del gruppo di sicurezza. Questo metodo non richiede l'aggiunta di una risorsa del gruppo di sicurezza a una progettazione di modelli cloud. In questa configurazione, è inoltre possibile utilizzare un bilanciamento del carico. Per informazioni correlate, vedere [Ulteriori informazioni sulle risorse di bilanciamento del carico nei modelli cloud di vRealize Automation](#).

- Componente del gruppo di sicurezza associato alla risorsa macchina in una progettazione di modelli cloud

È possibile trascinare e rilasciare una risorsa del gruppo di sicurezza in una progettazione di modelli cloud e associare la risorsa del gruppo di sicurezza a una scheda NIC di una macchina utilizzando i tag di vincolo nella risorsa del gruppo di sicurezza esistente nella progettazione di modelli cloud e nel gruppo di sicurezza esistente nella risorsa raccolta in base ai dati. È inoltre possibile creare questa associazione collegando gli oggetti insieme a una riga di connessione nella tela di progettazione del modello cloud, in modo simile all'associazione delle reti alle macchine nella tela di progettazione.

Quando si trascina e rilascia una risorsa del gruppo di sicurezza nella tela di progettazione del modello cloud, può essere di tipo `existing` o `new`. Se si tratta di un tipo di gruppo di sicurezza `existing`, è necessario aggiungere un valore di vincolo di tag come richiesto. Se si tratta di un tipo di gruppo di sicurezza `new`, è possibile configurare le regole del firewall.

- Un gruppo di sicurezza esistente allocato con vincoli di tag e associato a una scheda NIC di una macchina nel modello cloud

Ad esempio, è possibile associare una risorsa del gruppo di sicurezza a una scheda NIC di una macchina (in una risorsa macchina) nella progettazione di modelli cloud abbinando i tag tra le due risorse.

Come esempio per NSX-T, quando vengono specificati tag nell'endpoint di origine, è possibile utilizzare i tag NSX-T specificati nell'applicazione NSX-T. È quindi possibile utilizzare un tag NSX-T, specificato come vincolo in una risorsa di rete in una progettazione di modelli cloud, in cui la risorsa di rete è connessa a una scheda NIC di una macchina nella progettazione di modelli cloud. I tag NSX-T consentono di raggruppare dinamicamente le macchine utilizzando un tag NSX-T predefinito, raccolto in base ai dati dall'endpoint di origine di NSX-T. Quando si crea il tag NSX-T in NSX-T, utilizzare una porta logica.

- Regole del firewall in una risorsa del gruppo di sicurezza su richiesta in una progettazione di modelli cloud

È possibile aggiungere regole firewall a un gruppo di sicurezza su richiesta nella progettazione di modelli cloud.

Per informazioni sulle regole firewall disponibili, vedere [Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation](#).

Ulteriori informazioni

Per informazioni sulla definizione dei gruppi di sicurezza nei profili di rete, vedere [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

Per informazioni sulla visualizzazione e sulla modifica delle impostazioni dei gruppi di sicurezza nelle pagine delle risorse dell'infrastruttura, vedere [Risorse di sicurezza in vRealize Automation](#).

Per informazioni sulla definizione dei gruppi di sicurezza nelle progettazioni di modelli cloud, vedere [Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation](#).

Per esempi di risorse dei gruppi di sicurezza nelle progettazioni di modelli cloud, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Utilizzo delle impostazioni del bilanciamento del carico nei profili di rete in vRealize Automation

È possibile configurare le impostazioni del bilanciamento del carico nella configurazione del profilo di rete.

È possibile aggiungere un bilanciamento del carico esistente a un profilo di rete utilizzando la scheda **Bilanciamento del carico**.

È possibile aggiungere un bilanciamento del carico a una progettazione di modello cloud associandola a un profilo di rete che contiene uno o più bilanciamenti del carico o direttamente utilizzando una risorsa di bilanciamento del carico nel codice o nella tela di progettazione del modello cloud.

Esempi di inclusione di un VIP di bilanciamento del carico utilizzando il gruppo di sicurezza in un profilo di rete

Sono disponibili due tipi di gruppi di sicurezza che è possibile utilizzare in un profilo di rete, ovvero un gruppo di sicurezza esistente selezionato nella scheda **Gruppi di sicurezza** e un gruppo di sicurezza su richiesta creato utilizzando un criterio di isolamento nella scheda **Criteri di rete**.

Quando un VIP di bilanciamento del carico viene associato a un gruppo di sicurezza in base alle impostazioni del profilo di rete, la configurazione del gruppo di sicurezza viene fornita dal profilo di rete.

Nella tabella seguente sono illustrati alcuni esempi di scenari.

Topologia di progettazione del modello cloud: risorse associate	Configurazione del profilo di rete	Iscrizione al gruppo di sicurezza
Bilanciamento del carico con un solo ramo con VIP nella rete privata e una macchina nella stessa rete privata.	Il profilo di rete selezionato utilizza un criterio di isolamento definito come gruppo di sicurezza su richiesta.	La scheda NIC della macchina e il VIP di bilanciamento del carico vengono aggiunti al gruppo di sicurezza di isolamento.
Bilanciamento del carico con un solo ramo con VIP nella rete privata e una macchina nella stessa rete privata.	Il profilo di rete selezionato utilizza un gruppo di sicurezza esistente e un criterio di isolamento definito come gruppo di sicurezza su richiesta.	La scheda NIC della macchina e il VIP di bilanciamento del carico vengono aggiunti al gruppo di sicurezza di isolamento e al gruppo di sicurezza esistente.
Bilanciamento del carico a due rami con VIP in una rete pubblica e macchina in una rete privata.	Il profilo di rete selezionato utilizza un gruppo di sicurezza esistente e un criterio di isolamento definito come gruppo di sicurezza su richiesta.	La scheda NIC della macchina e il VIP di bilanciamento del carico vengono aggiunti al gruppo di sicurezza di isolamento e al gruppo di sicurezza esistente.
Bilanciamento del carico a due rami con VIP in una rete pubblica e macchina in una rete privata.	Il profilo di rete selezionato utilizza un gruppo di sicurezza esistente.	La scheda NIC della macchina e il VIP di bilanciamento del carico vengono aggiunti al gruppo di sicurezza esistente.
Bilanciamento del carico a due rami. Il VIP si trova nella rete 1 e la macchina nella rete 2.	Due profili di rete: <ul style="list-style-type: none"> ■ Profilo di rete 1: utilizza un gruppo di sicurezza 1 esistente. ■ Profilo di rete 2: utilizza un gruppo di sicurezza 2 esistente. 	Il bilanciamento del carico si trova nel profilo di rete 1 e la macchina si trova nel profilo di rete 2. Il VIP di bilanciamento del carico viene aggiunto al gruppo di sicurezza 1 e la scheda NIC della macchina viene aggiunta al gruppo di sicurezza 2.

Ulteriori informazioni

Per informazioni sull'aggiunta delle risorse di bilanciamento del carico a una progettazione di modello cloud, vedere [Ulteriori informazioni sulle risorse di bilanciamento del carico nei modelli cloud di vRealize Automation](#).

Per esempi di progettazioni di modelli cloud che includono bilanciamenti del carico, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Come configurare un profilo di rete per supportare una rete su richiesta per un'integrazione IPAM esterna in vRealize Automation

È possibile configurare un profilo di rete per supportare blocchi di indirizzi IP per una rete su richiesta quando il profilo di rete viene utilizzato in un modello cloud di vRealize Automation che utilizza l'integrazione IPAM esterna.

Se si utilizza un'integrazione esistente per un determinato provider IPAM esterno, è possibile eseguire il provisioning della rete su richiesta per creare una nuova rete nel sistema IPAM esterno.

Utilizzando questo processo, è possibile configurare un blocco di indirizzi IP invece di fornire un CIDR principale (come avviene quando si utilizza l'IPAM interno di vRealize Automation). Il blocco di indirizzi IP viene utilizzato durante il provisioning della rete su richiesta per segmentare la nuova rete. I dati dei blocchi IP vengono raccolti dal provider IPAM esterno, purché l'integrazione supporti le reti su richiesta. Ad esempio, quando si utilizza un'integrazione IPAM Infoblox, i blocchi IP rappresentano i contenitori di rete Infoblox.

Quando si utilizza un profilo di rete su richiesta e un'integrazione IPAM esterna in un modello cloud, si verificano i seguenti eventi quando il modello cloud viene distribuito:

- Viene creata una rete nel provider IPAM esterno.
- Viene creata una rete anche in vRealize Automation, che riflette la nuova configurazione di rete del provider IPAM, incluse impostazioni come CIDR e le proprietà del gateway.
- L'indirizzo IP della macchina virtuale distribuita viene recuperato dalla rete appena creata.

In questo esempio di rete su richiesta, viene configurato un profilo di rete per consentire a una distribuzione del modello cloud di eseguire il provisioning di una macchina in una rete su richiesta in vSphere utilizzando Infoblox come provider IPAM esterno.

Per informazioni correlate, vedere [Come configurare un profilo di rete per supportare una rete esistente per un'integrazione IPAM esterna in vRealize Automation](#). Entrambi gli esempi di configurazione di rete sono adatti al workflow generale specifico del fornitore per l'integrazione IPAM esterna in [Tutorial: configurazione di VMware Cloud on AWS per vRealize Automation](#).

Prerequisiti

Mentre i seguenti prerequisiti si applicano all'utente che crea o modifica il profilo di rete, il profilo di rete stesso è applicabile quando viene utilizzato da una distribuzione del modello cloud che contiene un'integrazione IPAM. Per ulteriori informazioni sui punti di integrazione IPAM specifici del fornitore, vedere [Come configurare un'integrazione IPAM esterna in vRealize Automation](#).

Questa sequenza di passaggi viene mostrata nel contesto di un workflow di integrazione del provider IPAM. Vedere [Tutorial: configurazione dell'integrazione di un provider IPAM esterno specifico del provider per vRealize Automation](#).

- Verificare di disporre delle credenziali di amministratore del cloud. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Verificare di disporre di un account con il provider IPAM esterno, ad esempio [Infoblox](#) o [Bluecat](#) e di disporre delle credenziali di accesso corrette per l'account dell'organizzazione con il provider IPAM. In questo workflow di esempio, il provider IPAM è Infoblox.
- Verificare di disporre di un punto di integrazione IPAM per il provider IPAM e che il pacchetto IPAM utilizzato per creare l'integrazione IPAM supporti le reti su richiesta. Vedere [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#).

Il pacchetto IPAM Infoblox supporta reti su richiesta, ma se si utilizza un'integrazione IPAM esterna per un provider diverso, verificare che il pacchetto di integrazione IPAM di tale provider supporti le reti su richiesta.

Procedura

1 Per configurare un profilo di rete, fare clic su **Infrastruttura > Configura > Profili di rete**.

2 Fare clic su **Nuovo profilo di rete**.

3 Fare clic sulla scheda **Riepilogo** e specificare le seguenti impostazioni di esempio:

- Specificare una regione o un account cloud di vSphere, ad esempio **vSphere-IPAM-OnDemandA/Datacenter**.

In questo esempio si presuppone l'utilizzo di un account cloud di vSphere non associato a un account cloud di NSX.

- Assegnare un nome al profilo di rete, ad esempio **Infoblox-OnDemandNP**.
- Aggiungere un tag di funzionalità per il profilo di rete, ad esempio **infoblox_ondemandA**.

Prendere nota del valore del tag di funzionalità, poiché sarà necessario utilizzarlo anche come tag di vincolo del modello cloud per fare in modo che l'associazione del profilo di rete venga utilizzata durante il provisioning del modello cloud.

4 Fare clic sulla scheda **Criteri di rete** e specificare le seguenti impostazioni di esempio:

- Dal menu a discesa **Criterio di isolamento**, selezionare **Rete su richiesta**.

Questa opzione consente di utilizzare blocchi IP di un'IPAM esterno. In base all'account cloud, vengono visualizzate nuove opzioni. Ad esempio, quando si utilizza un account cloud di vSphere associato a un account cloud di NSX vengono visualizzate le seguenti opzioni:

- Zona di trasporto
- Router logico di livello 0
- Cluster edge

Per questo esempio, l'account cloud di vSphere non è associato a NSX, quindi viene visualizzata l'opzione di menu **Dominio di rete**.

- Lasciare vuota l'opzione **Dominio di rete**.

5 Fare clic su **Esterno** come **Origine** della gestione degli indirizzi.

6 Fare clic su **Aggiungi blocco IP** per aprire la pagina **Aggiungi blocco IP IPAM**.

7 Dal menu **Provider** nella pagina **Aggiungi blocco IP IPAM**, selezionare un'integrazione IPAM esterna esistente. Ad esempio, selezionare il punto di integrazione *Infoblox_Integration* da [Aggiunta dell'integrazione di un provider IPAM esterno per Infoblox in vRealize Automation](#) nel workflow di esempio.

- 8 Dal menu **Spazio indirizzi**, selezionare uno dei blocchi IP disponibili ed elencati, ad esempio **10.23.118.0/24** e aggiungerlo.

Se il provider IPAM supporta uno spazio di indirizzi, viene visualizzato il menu **Spazio indirizzi**. Per un'integrazione Infoblox, gli spazi degli indirizzi sono rappresentati dalle visualizzazioni di rete di Infoblox.

- 9 Selezionare un valore in **Dimensioni subnet**, ad esempio **/29 (-6 indirizzi IP)**.

- 10 Fare clic su **Crea**.

Risultati

Viene creato un profilo di rete che può essere utilizzato per eseguire il provisioning di una rete su richiesta utilizzando l'integrazione IPAM esterna specificata. Il modello cloud di esempio seguente illustra la distribuzione di una singola macchina in una rete definita da questo nuovo profilo di rete.

```
formatVersion: 1
inputs: {}
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: ubuntu
      flavor: small
      networks:
        - network: '${resource.Cloud_Network_1.id}'
          assignment: static
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      networkType: private
      constraints:
        - tag: infoblox_ondemandA
```

Nota Quando il modello cloud viene distribuito, viene recuperata la prima rete disponibile nel blocco IP specificato, che viene considerata come CIDR della rete. Se si utilizza una rete NSX nel modello cloud, è invece possibile impostare il CIDR della rete manualmente utilizzando la proprietà di rete `networkCidr`, come illustrato di seguito, per impostare un CIDR manualmente e sostituire le impostazioni di blocchi IP e dimensione della subnet specificate nel profilo di rete associato.

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkCidr: 10.10.0.0/16
```


Come configurare un profilo di rete per supportare una rete esistente per un'integrazione IPAM esterna in vRealize Automation

È possibile configurare un profilo di rete per supportare gli intervalli di indirizzi IP per una rete esistente quando il profilo di rete viene utilizzato in un blueprint di vRealize Automation che utilizza l'integrazione IPAM esterna.

In [Configurazione di una rete e di un profilo di rete per l'utilizzo di un IPAM esterno per una rete esistente in vRealize Automation](#) è disponibile un esempio nel contesto di un workflow di esempio specifico del fornitore. Il workflow generale specifico del fornitore per l'integrazione IPAM esterna è disponibile nella sezione [Tutorial: configurazione di VMware Cloud on AWS per vRealize Automation](#).

Per informazioni correlate, vedere [Come configurare un profilo di rete per supportare una rete su richiesta per un'integrazione IPAM esterna in vRealize Automation](#).

Come aggiungere i profili di storage di Cloud Assembly che rappresentano requisiti diversi

Un profilo di storage di Cloud Assembly descrive il tipo di storage da distribuire.

In genere, viene creato un profilo di storage in base a caratteristiche come il livello di servizio o il costo, le prestazioni o lo scopo, come ad esempio il backup.

Selezionare **Infrastruttura > Configura > Profili di storage** e fare clic su **Nuovo profilo di storage**.

Ulteriori informazioni sui profili di storage in vRealize Automation

La regione di un account cloud contiene profili di storage che consentono all'amministratore del cloud di definire lo storage per la regione in vRealize Automation.

Quali sono le attività di un profilo di storage?

I profili di storage includono le personalizzazioni del disco e un mezzo per identificare il tipo di storage per i tag di funzionalità. I tag vengono quindi combinati con i vincoli di richiesta del servizio di provisioning per creare lo storage desiderato al momento della distribuzione.

I profili di storage sono organizzati in regioni specifiche del cloud. Un account cloud potrebbe avere più regioni, con più profili di storage inclusi in ogni regione.

Il posizionamento indipendente dal fornitore è possibile. Ad esempio, è possibile avere tre account di fornitore diversi e una regione in ciascuno. Ogni regione include un profilo di storage con funzionalità contrassegnata come *rapida*. Al momento del provisioning, una richiesta contenente un tag di vincolo permanente *rapido* è in cerca di una funzionalità *rapida* corrispondente, indipendentemente dal cloud del fornitore che fornisce le risorse. Una corrispondenza quindi applica le impostazioni del profilo di storage associato durante la creazione dell'elemento di storage distribuito.

Nota Storage del cloud differenti possono avere caratteristiche di prestazioni diverse, ma sono comunque considerati l'offerta *rapida* da parte dell'amministratore che li ha aggiunti.

I tag di funzionalità aggiunti ai profili di storage non devono identificare le destinazioni effettive delle risorse. Al contrario, descrivono i tipi di storage. Per ulteriori informazioni sulle risorse effettive, vedere [Risorse di storage in vRealize Automation](#).

Tipo di provisioning predefinito

Il tipo di provisioning del profilo di storage stabilisce solo un comportamento predefinito. L'impostazione non influisce necessariamente sul posizionamento e potrebbe essere sostituita da una proprietà nel modello cloud.

Ad esempio, è possibile impostare il profilo di storage per il thin provisioning. Nella maggior parte dei casi, le richieste creano storage con thin provisioning per impostazione predefinita. Tuttavia, se la proprietà `provisioningType` del modello cloud è impostata su `eager-zero`, il modello cloud sovrascrive il valore predefinito di thin.

Nota Quando si desidera un controllo esatto, è consigliabile aggiungere tag di funzionalità e vincolo etichettati per il tipo di provisioning desiderato.

Per il comportamento predefinito del tipo di provisioning, una proprietà del modello cloud sostituisce l'impostazione predefinita di un profilo di storage e l'impostazione predefinita di un profilo di storage sostituisce un'impostazione predefinita di un criterio di storage di vCenter.

Allocazione del disco con macchine

In un progetto con più zone cloud che appartengono a diversi account cloud, un disco segue la macchina anche se non è collegato alla macchina. Questo comportamento tiene unite le risorse per evitare errori quando si decide di collegare il disco in un secondo momento.

Ad esempio, la progettazione seguente non funzionerà. Il modello cloud tenta di utilizzare i vincoli di posizione per separare il disco, ma la distribuzione restituisce un errore `No matching placement`.

Se è necessario posizionare un disco in un altro account cloud, utilizzare una distribuzione separata per distribuire il disco.

```
resources:
  Machine1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu
      flavor: small
      constraints:
        - tag: 'location:siteA'
  Disk1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      constraints:
        - tag: 'location:siteB'
```

First Class Disk e dischi standard

Utilizzando l'opzione **Tipo di disco** nella pagina del profilo di storage oppure utilizzando l'API di vRealize Automation, è possibile creare un profilo di storage per supportare lo storage su disco FCD (First Class Disk) o su disco standard. Infatti, l'opzione First Class Disk crea un profilo di storage di vSphere.

■ First Class Disk

I First Class Disk possono esistere indipendentemente da una macchina virtuale di vSphere. Un First Class Disk dispone anche di funzionalità di gestione del ciclo di vita che possono funzionare indipendentemente da una macchina virtuale. I First Class Disk sono disponibili per vSphere versione 6.7 2 e successive e sono attualmente implementati in vRealize Automation come funzionalità solo API.

Per informazioni sullo storage su FCD incluse le funzionalità disponibili nell'API di vRealize Automation e i collegamenti alla documentazione dell'API stessa, vedere [Cosa è possibile fare con lo storage FCD \(First Class Disk\) in vRealize Automation](#).

■ Disco standard

Lo storage su disco standard viene creato e gestito come componente integrato di una macchina virtuale.

Per informazioni sullo storage su disco standard, vedere [Cosa è possibile fare con lo storage su disco standard in vRealize Automation](#) e [Cosa è possibile fare con lo storage su disco persistente in vRealize Automation](#).

Crittografia del disco lato server Azure

Per le risorse di Azure, se si sceglie di supportare la crittografia in un profilo di storage del disco gestito, selezionare anche la crittografia del disco con una chiave associata. Le chiavi e la crittografia disponibili corrispondono ai set di crittografia del disco configurati in Azure per la posizione.

Microsoft Azure

Search resources, services, and docs (G+)

Home >

Disk Encryption Sets

+ Add Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter for any field... Subscription == R&D Resource group == all Location == all Add filter

Showing 1 to 100 of 305 records.

Name	Resource group	Location	Key
MyDES	DiskEncryptionSets	West US	WestUSKey...
MyDES1	DiskEncryptionSets	West US	WestUSKey...
MyDES10	DiskEncryptionSets	West US	WestUSKey...
MyDES100	DiskEncryptionSets	West US	WestUSKey...
MyDES101	DiskEncryptionSets	West US	WestUSKey...

Account / region * AzureAcc / West US

Name * SP-with-des

Description

Storage type * Managed disks

Disk type * Standard HDD

OS disk caching * Read only

Data disk caching * Read only

Supports encryption ☒

Encryption set Search for encryption set

Capability tags

CREATE CANCEL

MyDES

WestUSKeyForDisk

MyDES1

WestUSKeyForDisk

MyDES10

WestUSKeyForDisk

MyDES100

WestUSKeyForDisk

MyDES101

WestUSKeyForDisk

EncryptDiskWestUS

EncryptDiskWestUS

EncryptDiskWestUS

EncryptDiskWestUS

EncryptDiskWestUS

Come utilizzare le schede dei prezzi in vRealize Automation

Le schede dei prezzi di Cloud Assembly consentono agli amministratori del cloud di definire e assegnare il criterio dei prezzi per l'impatto monetario delle singole distribuzioni al fine di gestire meglio le risorse.

Nota Affinché i prezzi funzionino in ambienti multi-tenant, è necessario disporre di un'istanza vRealize Operations Manager separata per ogni tenant vRealize Automation.

Le schede dei prezzi definiscono le tariffe per un criterio dei prezzi. Il criterio dei prezzi può quindi essere assegnato a progetti specifici per definire un prezzo totale. Dopo aver creato un endpoint vRealize Operations Manager o CloudHealth, è disponibile una scheda dei prezzi predefinita con un costo uguale alla configurazione del prezzo nella scheda **Infrastruttura > Schede dei prezzi**. È possibile creare schede dei prezzi che si applicano solo ai progetti o alle zone cloud. Per impostazione predefinita, tutte le nuove scheda dei prezzi vengono applicate ai progetti.

Nota Se si modifica l'impostazione **Tutte le schede dei prezzi vengono applicate a**, tutte le assegnazioni di schede dei prezzi esistenti vengono eliminate. Inoltre, se l'endpoint vRealize Operations Manager viene eliminato da Cloud Assembly, vengono eliminate anche tutte le schede dei prezzi e le assegnazioni.

Il prezzo di una distribuzione nel tempo viene visualizzato sia nella scheda della distribuzione che nel progetto come prezzo da inizio mese, che viene azzerato all'inizio di ogni mese. Le suddivisioni dei costi dei componenti sono disponibili nei dettagli della distribuzione. La fornitura di queste informazioni a livello di distribuzione informa l'amministratore del cloud, ma aiuta anche i membri a comprendere l'impatto che il loro lavoro potrebbe avere sui budget e sullo sviluppo a lungo termine.

È possibile scegliere di visualizzare le informazioni sui prezzi da utenti in Cloud Assembly e Service Broker selezionando il pulsante **Visualizza informazioni sui prezzi**. Se lasciato disabilitato, le informazioni sui prezzi vengono nascoste agli utenti di Cloud Assembly e Service Broker.

Come viene calcolato il prezzo

Il prezzo iniziale visualizzato a livello di distribuzione per le risorse di elaborazione e storage si basa sulle percentuali di benchmark standard del settore, successivamente calcolate nel tempo. La tariffa viene applicata agli host e il servizio calcola le tariffe di CPU e memoria. Il server ricalcola il prezzo ogni 6 ore.

Nuovi criteri, assegnazioni e prezzi iniziali sono valutati durante il successivo ciclo di raccolta dati. Per impostazione predefinita, il ciclo di raccolta dati viene eseguito ogni 5 minuti. Potrebbero essere necessarie fino a 6 ore affinché i nuovi criteri o le modifiche vengano aggiornati in progetti e distribuzioni.

Come stimare il prezzo di tutti i progetti e le distribuzioni

Prima di distribuire un elemento del catalogo, è possibile utilizzare il prezzo iniziale come stima del prezzo per la distribuzione. Per visualizzare il prezzo in Cloud Assembly, è necessario disporre di un endpoint di integrazione vRealize Operations Manager configurato con il prezzo abilitato e il valore predefinito di valuta.

Daily Price Estimate



Guest OS and one time prices are excluded in this estimate.



price-service-f309c00

\$0.54



Cloud_vSphere_Machine_1

\$0.53

Compute

\$0.39

Storage

\$0.03

Additional charges

\$0.11



Cloud_vSphere_Disk_1

\$0.01

Storage

\$0.01

CLOSE

Per una stima del prezzo iniziale, la dimensione del disco di avvio per macchina virtuale è sempre 8 GB.

Il prezzo iniziale di una distribuzione è una stima del prezzo giornaliera, in base all'allocazione di una risorsa, per un determinato elemento del catalogo prima che venga distribuito. Dopo aver distribuito un elemento del catalogo, è possibile visualizzare il prezzo da inizio mese come aggregazione del prezzo iniziale nelle schede **Distribuzione** e **Infrastruttura > Progetti**. I prezzi iniziali sono supportati per le risorse del cloud privato, ad esempio macchina vSphere e disco vSphere, elementi del catalogo di Cloud Assembly ed elementi indipendenti dal cloud con vCenter configurato per il cloud privato.

Nota I prezzi iniziali non sono supportati per le risorse del cloud pubblico o per le risorse del cloud privato non macchina o disco vSphere.

Per stimare il costo della distribuzione, dal catalogo selezionare un elemento del catalogo e fare clic su **Richiedi > Calcola**. Se il prezzo è accettabile, fare clic su **Invia**.

È possibile utilizzare le schede dei prezzi del progetto per stimare il prezzo totale di tutti i progetti.

Per stimare il costo di un progetto, nella pagina Infrastruttura - Scheda dei prezzi, accanto all'impostazione **Tutte le schede dei prezzi vengono applicate a**, fare clic su **Modifica** e selezionare **Progetti**.

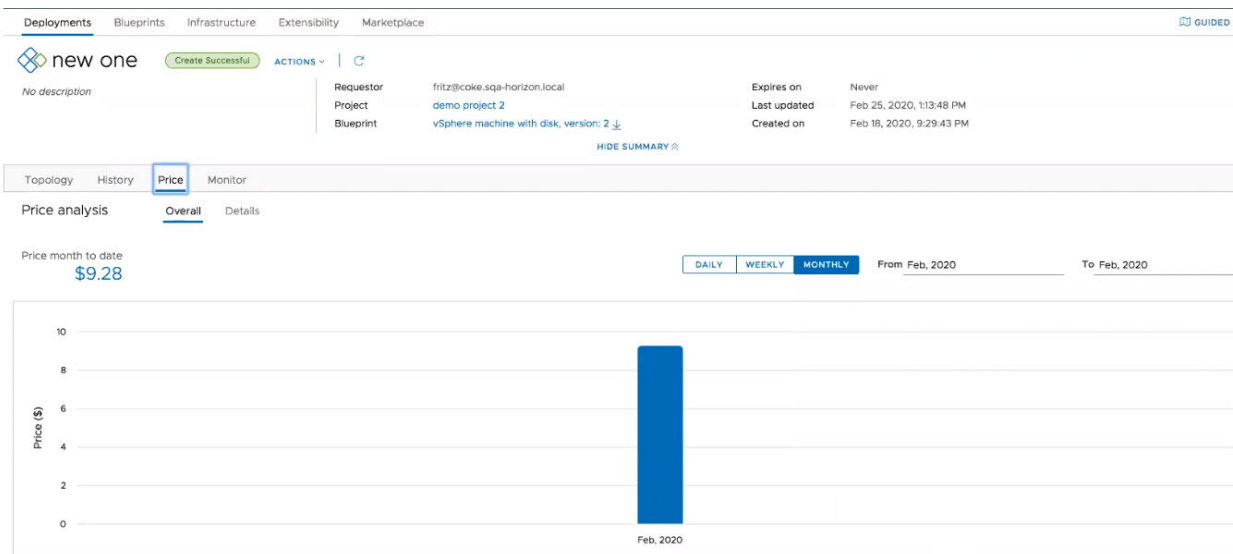
Se si modifica l'impostazione **Tutte le schede dei prezzi vengono applicate a**, tutte le assegnazioni di schede dei prezzi esistenti vengono eliminate. Creare le assegnazioni e le schede dei prezzi utilizzando un approccio basato sui costi.

Come creare le schede dei prezzi per vSphere e VMC

È possibile creare e assegnare una scheda dei prezzi a progetti o zone cloud, in base alla strategia di prezzi determinata dall'amministratore del cloud per le distribuzioni di cloud privato.

Le schede dei prezzi possono essere personalizzate in base ai parametri selezionati dall'utente. Dopo aver configurato una scheda dei prezzi, è possibile assegnarla a uno o più progetti e zone cloud determinati dalla strategia di prezzi.

È possibile aggiornare manualmente il server dei prezzi in qualsiasi momento nella pagina Endpoint vROPs, **Infrastruttura > Integrazioni > Endpoint vROPs > .** Nella sezione vCenter Server, fare clic su **Sincronizza**. Quando si esegue l'aggiornamento manuale del server dei prezzi utilizzando l'opzione **Sincronizza**, il prezzo viene ricalcolato per tutti i progetti nell'organizzazione. In base al numero di progetti posseduti dall'organizzazione, l'elaborazione di questo processo potrebbe essere intensa e richiedere tempo.



Dopo aver creato e assegnato una scheda dei prezzi, è possibile visualizzare la cronologia dei prezzi delle distribuzioni e dei progetti. Per visualizzare la cronologia dei prezzi, passare alla distribuzione e fare clic su **Prezzo**. L'analisi dei prezzi fornisce una panoramica e una visualizzazione dettagliata del prezzo di distribuzione insieme al valore del prezzo da inizio mese. È possibile modificare la rappresentazione grafica per visualizzare i prezzi della distribuzione come valori giornalieri, settimanali o mensili. Inoltre, è possibile specificare un intervallo di date o un mese esatto per la cronologia dei prezzi.

Per visualizzare la ripartizione dei prezzi in base al costo, fare clic su **Dettagli**.

I prezzi sono determinati dai tipi di componenti di cui è stato calcolato il costo.

Tabella 4-1. Tipi di componenti di cui è stato calcolato il costo

Tipo di componente del blueprint	Nome servizio/tipo di oggetto	Tipo di risorsa del blueprint	Commenti
Indipendente dal cloud	Macchina	Cloud.Machine	Se una macchina indipendente è configurata con vSphere, è possibile visualizzare il costo della distribuzione.
	Disco	Cloud.Volume	Se un disco indipendente è collegato a una macchina virtuale configurata con vSphere, è possibile visualizzare il costo della distribuzione.
vSphere	Macchina vSphere	Cloud.vSphere.Machine	Distribuito utilizzando un blueprint specifico del cloud.
	Disco vSphere	Cloud.vSphere.Disk	Distribuito utilizzando un blueprint specifico del cloud collegato a una macchina virtuale.
VMware Managed Cloud (VMC)	Macchina vSphere	Cloud.vSphere.Machine	VMC supporta solo le schede dei prezzi basate su tariffe (le schede dei prezzi basate sui costi non sono supportate).
	Disco vSphere	Cloud.vSphere.Disk	

Prerequisiti

Prima di poter creare o assegnare schede dei prezzi, è necessario configurare e attivare i prezzi e configurare la valuta in vRealize Operations per lavorare con vRealize Automation . Quando si configura vRealize Operations con vRealize Automation , assicurarsi che entrambe le applicazioni siano impostate sullo stesso fuso orario. Per configurare il fuso orario in vRealize Operations, attivare SSH e accedere a ciascun nodo di vRealize Operations, modificare il file `$ALIVE_Base/user/conf/analytics/advanced.properties` e aggiungere `timeZoneUsedInMeteringCalculation =<time zone>`.

Affinché i prezzi funzionino in ambienti multi-tenant, è necessario disporre di un'istanza di vROPs separata per ogni tenant vRA.

È necessario configurare un endpoint vRealize Operations prima di poter configurare le schede dei prezzi. Per configurare l'endpoint vRealize Operations, passare a **Infrastruttura > Connessioni > Integrazioni > Aggiungi integrazione**.

Nota Quando vengono aggiunti più endpoint vRealize Operations, questi non devono monitorare lo stesso vCenter.

Procedura

- 1 Passare a **Infrastruttura > Schede dei prezzi > Nuova scheda dei prezzi**.
- 2 Nella scheda Riepilogo, immettere un nome e una descrizione per la scheda dei prezzi. Una volta definito il criterio nella scheda dei prezzi, la tabella Panoramica viene compilata con le tariffe della scheda dei prezzi.

Nota La valuta viene determinata dal valore selezionato in vRealize Operations.

- 3 Facoltativo. Selezionare la casella di controllo **Impostare come predefinito per i progetti non assegnati?** per assegnare questa scheda dei prezzi a tutti i progetti non assegnati per impostazione predefinita.

4 Fare clic su **Prezzi** e configurare i dettagli del criterio dei prezzi.

Tabella 4-2. Configurazione dei criteri dei prezzi

Parametro	Descrizione
Addebiti di base	<p>Immettere un nome e una descrizione per il criterio. Selezionare Basato su costo o tariffa.</p> <ul style="list-style-type: none"> ■ Costo: il costo è definito in vRealize Operations. Se questa opzione è selezionata, è necessario un fattore di moltiplicazione. Ad esempio, se si seleziona 1,1 come fattore, il costo viene moltiplicato per 1,1 determinando un aumento del 10% del costo calcolato. L'equazione del prezzo che utilizza il costo è: $\text{costo} \times \text{fattore di moltiplicazione} = \text{Prezzo}$ ■ Tariffa: se questa opzione è selezionata, è necessario utilizzare valori assoluti per determinare il costo. L'equazione del prezzo che utilizza la tariffa è: $\text{Tariffa} = \text{Prezzo}$. Selezionare un intervallo di tariffe dall'elenco a discesa per specificare la modalità di addebito. <p>Nella sezione Addebiti di base, è possibile definire il costo o la tariffa per la CPU, la memoria, lo storage e altri costi vari.</p>
Sistemi operativi guest	<p>È possibile definire un addebito per il sistema operativo guest facendo clic su Aggiungi addebito.</p> <p>Immettere il nome del sistema operativo guest e definire il metodo di addebito e la tariffa di base.</p> <ul style="list-style-type: none"> ■ Ricorrente: immettere una tariffa di base e definire l'intervallo ricorrente come periodo di addebito. Il valore della tariffa assoluta è obbligatorio e viene aggiunto al prezzo complessivo. ■ Una tantum: definire l'addebito della tariffa di base una tantum. Il valore assoluto è obbligatorio e viene aggiunto come prezzo una tantum. ■ Fattore tariffa: è necessario un fattore di moltiplicazione applicato alla categoria di addebito selezionata. Ad esempio, se si seleziona Addebito CPU e un fattore tariffa pari a 2. La CPU del sistema operativo guest viene addebitata con un valore di costo raddoppiato rispetto a quello standard. <p>È possibile aggiungere più sistemi operativi guest con addebiti diversi facendo clic su Aggiungi addebito e configurando un criterio di addebito aggiuntivo.</p> <hr/> <p>Nota I costi iniziali per i sistemi operativi guest non vengono mostrati nella pagina di riepilogo, anche se fanno parte del criterio.</p>

Tabella 4-2. Configurazione dei criteri dei prezzi (continua)

Parametro	Descrizione
Tag	<p>È possibile definire un addebito di tag facendo clic su Aggiungi addebito.</p> <p>Selezionare il nome del tag e definire il metodo di addebito e la tariffa di base.</p> <ul style="list-style-type: none"> ■ Ricorrente: immettere una tariffa di base e definire l'intervallo ricorrente come periodo di addebito. Il valore della tariffa assoluta è obbligatorio e viene aggiunto al prezzo complessivo. ■ Una tantum: definire l'addebito della tariffa di base una tantum. Il valore assoluto è obbligatorio e viene aggiunto come prezzo una tantum. ■ Fattore tariffa: è necessario un fattore di moltiplicazione applicato alla categoria di addebito selezionata. <p>Selezionare la modalità di addebito del tag in base allo stato di accensione.</p> <p>È possibile aggiungere più tag con addebiti diversi facendo clic su Aggiungi addebito e configurando un criterio di addebito aggiuntivo.</p> <hr/> <p>Nota Gli addebiti aggiuntivi nel prezzo finale calcolato includono i tag nelle macchine virtuali e non includono i tag in dischi e reti.</p>
Proprietà personalizzate	<p>È possibile definire un addebito per la proprietà personalizzata facendo clic su Aggiungi addebito.</p> <p>Immettere il nome e il valore della proprietà, quindi definire il metodo di addebito e la tariffa di base.</p> <ul style="list-style-type: none"> ■ Ricorrente: immettere una tariffa di base e definire l'intervallo ricorrente come periodo di addebito. Il valore della tariffa assoluta è obbligatorio e viene aggiunto al prezzo complessivo. ■ Una tantum: definire l'addebito della tariffa di base una tantum. Il valore assoluto è obbligatorio e viene aggiunto come prezzo una tantum. ■ Fattore tariffa: è necessario un fattore di moltiplicazione applicato alla categoria di addebito selezionata. <p>Selezionare la modalità di addebito della proprietà personalizzata in base allo stato di accensione.</p> <p>È possibile aggiungere più proprietà personalizzate con addebiti diversi facendo clic su Aggiungi addebito e configurando un criterio di addebito aggiuntivo.</p>
Addebiti complessivi	<p>Definire qualsiasi addebito aggiuntivo che si desidera aggiungere al criterio dei prezzi. È possibile aggiungere addebiti una tantum o ricorrenti.</p>

Gli addebiti una tantum non vengono visualizzati nella stima del prezzo di un elemento del catalogo o nella scheda Riepilogo. Viene mostrata solo la stima del prezzo giornaliero per un determinato elemento del catalogo.

- 5 Fare clic sulla scheda **Assegnazioni**, quindi fare clic su **Assegna progetti**. Selezionare uno o più progetti a cui assegnare la schede dei prezzi.

Nota Per impostazione predefinita, le schede dei prezzi vengono applicate ai progetti. Nella scheda **Infrastruttura > Schede dei prezzi**, è possibile scegliere di applicare le schede dei prezzi alle zone cloud. Se sono state selezionate zone cloud, fare clic su **Assegna zone cloud** nella scheda Assegnazioni.

- 6 Fare clic su **Crea** per salvare e creare il criterio dei prezzi.

Risultati

Il nuovo criterio dei prezzi viene visualizzato nella pagina Schede dei prezzi. Per visualizzare o modificare i dettagli e la configurazione dei criteri, fare clic su **Apri**.

Come utilizzare i tag per gestire le distribuzioni e le risorse di Cloud Assembly

I tag sono componenti critici di Cloud Assembly che determinano il posizionamento delle distribuzioni tramite la corrispondenza di funzionalità e vincoli. È necessario comprendere e implementare i tag in modo efficace per un utilizzo ottimale di Cloud Assembly.

Fondamentalmente, i tag sono etichette che vengono aggiunte agli elementi di Cloud Assembly. È possibile creare qualsiasi tag appropriato per l'organizzazione e l'implementazione. I tag offrono però molte più funzionalità delle etichette, perché controllano come e dove Cloud Assembly utilizza risorse e infrastrutture per creare servizi distribuibili. I tag supportano inoltre la governance all'interno di Cloud Assembly.

Struttura dei tag

Dal punto di vista della struttura, i tag devono seguire la convenzione di coppia `name:value`, ma per il resto la loro creazione è in gran parte in formato libero. In Cloud Assembly, tutti i tag vengono visualizzati in modo simile e la loro funzionalità è determinata dal contesto.

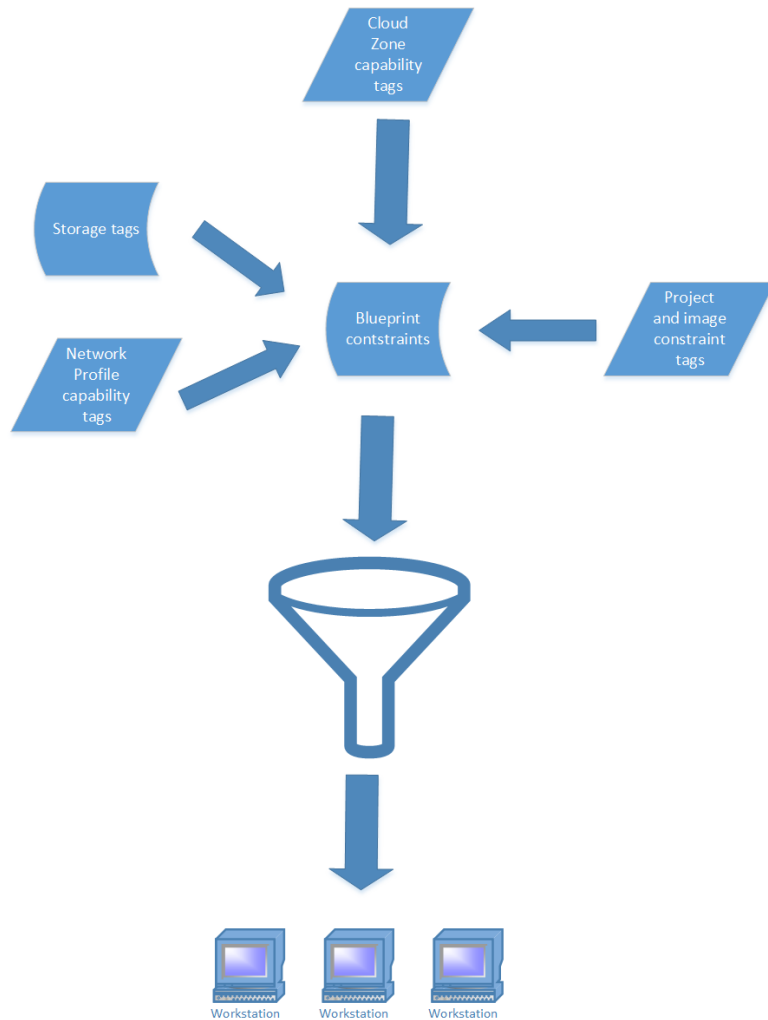
Ad esempio, i tag nelle risorse dell'infrastruttura funzionano in genere come tag di funzionalità perché Cloud Assembly li utilizza per associare le risorse alle distribuzioni. In secondo luogo, identificano anche le risorse.

Funzione dei tag

La funzione primaria dei tag consiste nell'esprimere le funzionalità e i vincoli utilizzati da Cloud Assembly per definire le distribuzioni. Il contesto determina la funzione dei tag. I tag posizionati nelle zone cloud, nei profili di rete e di storage e nelle singole risorse dell'infrastruttura fungono da tag di funzionalità e definiscono le funzionalità desiderate per l'infrastruttura utilizzata nelle

distribuzioni. I tag posizionati nei modelli cloud fungono da vincoli che definiscono le risorse per le distribuzioni. Inoltre, gli amministratori del cloud possono posizionare i tag di vincolo nei progetti per esercitare una forma di governance rispetto a tali progetti. Questi tag di vincolo vengono aggiunti ad altri vincoli espressi nei modelli cloud.

Durante il provisioning, Cloud Assembly associa queste funzionalità ai vincoli, espressi anche come tag, nei modelli cloud per definire la configurazione della distribuzione. Queste funzionalità e vincoli basati su tag sono la base per la configurazione della distribuzione in Cloud Assembly. Ad esempio, è possibile utilizzare i tag per rendere l'infrastruttura disponibile solo nelle risorse PCI in una determinata regione.



A livello secondario, i tag facilitano anche la ricerca e l'identificazione degli elementi di storage e di rete, nonché delle altre risorse dell'infrastruttura.

Ad esempio, si supponga di configurare zone cloud e di disporre di molte risorse di elaborazione. Se alle risorse di elaborazione sono stati applicati i tag appropriati, è possibile utilizzare la funzione di ricerca nella scheda Risorsa di elaborazione della pagina Zona cloud per filtrare le risorse associate a tale zona cloud specifica.

Inoltre, la pagina Gestione tag di Cloud Assembly e le pagine di configurazione delle risorse contengono funzioni di ricerca che permettono di individuare gli elementi in base ai nomi dei tag. L'utilizzo di tag logici e leggibili per questi elementi è fondamentale per facilitare questa funzione di ricerca e identificazione.

Per ulteriori informazioni ed esempi di utilizzo dei tag, guardare i seguenti video di YouTube:

<https://youtu.be/4zNQ33RyQio>

Tag esterni

Cloud Assembly può contenere anche tag esterni. Questi tag vengono importati automaticamente dagli account cloud associati a un'istanza di Cloud Assembly. Questi tag possono essere importati da vSphere, AWS, Azure o altri prodotti software esterni. Quando vengono importati, questi tag sono disponibili per l'uso in modo analogo ai tag creati dall'utente.

Gestione dei tag

È possibile utilizzare la pagina Gestione tag in Cloud Assembly per monitorare e gestire la libreria di tag. In questa pagina è anche possibile creare tag. La pagina Gestione tag è inoltre l'unica pagina in cui è possibile visualizzare e identificare i tag esterni.

Key	Value
a	
AAA	sofiaaaa
aktag1	vafl
alex	kris
AppID	ABC
AppID	XYZ
applicationtier	tango-machine
Application Tier	tango-machine
Application Tier	
astoyanov-rp	
Atos-Tagging-Category	Atos-Storage-Tag
AutomaticCleanExpirationTime	2019-01-08T08:45:33.127Z

Strategia dei tag

Per ridurre al minimo la confusione, prima di creare i tag in Cloud Assembly, è utile definire una strategia e convenzioni di assegnazione dei tag appropriate, in modo che tutti gli utenti che creano e utilizzano i tag comprendano il loro significato e il modo in cui devono essere utilizzati. Vedere [Creazione di una strategia di assegnazione dei tag](#).

Creazione di una strategia di assegnazione dei tag

È necessario pianificare e implementare con attenzione una strategia di assegnazione dei tag appropriata in base alla struttura IT e agli obiettivi dell'organizzazione per massimizzare la funzionalità di Cloud Assembly e ridurre al minimo la potenziale confusione.

I tag sono utili per diversi scopi comuni, ma la strategia di assegnazione dei tag deve essere adattata alle esigenze, alla struttura e agli obiettivi della distribuzione.

Procedure consigliate per l'assegnazione dei tag

Alcune caratteristiche generali di una strategia di assegnazione dei tag efficace:

- Progettare e implementare una strategia coerente per l'assegnazione dei tag, correlata alla struttura della propria azienda e comunicare questo piano a tutti gli utenti interessati. Una strategia deve supportare le esigenze della distribuzione, utilizzare un linguaggio chiaro e leggibile ed essere comprensibile per tutti gli utenti interessati.
- Per i tag utilizzare nomi e valori semplici, chiari e significativi. Ad esempio, i nomi dei tag per gli elementi di storage e di rete devono essere chiari e coerenti, in modo che gli utenti possano facilmente capire cosa stanno selezionando o esaminare le assegnazioni dei tag per una risorsa distribuita.
- Sebbene sia possibile creare tag utilizzando un nome senza alcun valore, è consigliabile creare un valore applicabile per ciascun nome di tag, poiché ciò rende l'utilizzo del tag chiaro per gli altri utenti.
- Evitare la creazione di etichette duplicate o estranee. Ad esempio, è possibile creare solo tag negli elementi di storage relativi ai problemi di storage.

Implementazione dell'assegnazione dei tag

Definire le considerazioni primarie per una strategia di assegnazione dei tag di base. L'elenco seguente include le considerazioni tipiche da valutare durante la definizione della strategia. Tenere presente che queste considerazioni sono solo rappresentative e non sono definitive. È possibile che esistano altre considerazioni molto pertinenti per i propri casi d'uso. La strategia deve essere appropriata per i casi d'uso specifici.

- Numero di ambienti diversi in cui viene eseguita la distribuzione. In genere vengono creati tag che rappresentano ciascun ambiente.
- Struttura e uso delle risorse di elaborazione per supportare le distribuzioni.
- Numero di regioni o posizioni diverse in cui viene eseguita la distribuzione. In genere si creano tag a livello di profilo che rappresentano ciascuna delle regioni o posizioni diverse.
- Numero di opzioni di storage disponibili per le distribuzioni e come si desidera caratterizzarle. Queste opzioni devono essere rappresentate da tag.
- Classificare le opzioni di rete e creare tag per tutte le opzioni applicabili.

- Variabili tipiche della distribuzione. Ad esempio, numero di ambienti diversi in cui viene eseguita la distribuzione. In genere, molte organizzazioni dispongono almeno di ambienti di test, sviluppo e produzione. È consigliabile creare e coordinare tag dei vincoli e tag di funzionalità della zona cloud corrispondenti, in modo da poter configurare facilmente le distribuzioni in uno o più di questi ambienti.
- Coordinare i tag nelle risorse di rete e di storage in modo che abbiano un senso logico nel contesto dei profili di rete e di storage in cui vengono utilizzati. I tag delle risorse possono essere utilizzati come livello di controllo più preciso sulla distribuzione delle risorse.
- Coordinare i tag di funzionalità della zona cloud e del profilo di rete e altri tag di funzionalità con i tag di vincolo. In genere, l'amministratore creerà innanzitutto i tag di funzionalità per le zone cloud e i profili di rete, quindi altri utenti potranno progettare modelli cloud con vincoli che corrispondono a questi tag di funzionalità.

Dopo aver compreso gli aspetti importanti da valutare per l'organizzazione, è possibile pianificare i nomi dei tag appropriati che si riferiscono a questi aspetti in modo logico. Creare quindi una bozza della strategia e renderla disponibile per tutti gli utenti con privilegi per la creazione o la modifica dei tag.

Come utile approccio di implementazione, è possibile iniziare assegnando tag alle singole risorse dell'infrastruttura di elaborazione. Come indicato, utilizzare categorie logiche per i nomi dei tag che si riferiscono alla risorsa specifica. Ad esempio, è possibile contrassegnare le risorse di storage come livello1, livello2 e così via. È inoltre possibile contrassegnare le risorse di elaborazione in base al loro sistema operativo, come Windows, Linux e così via.

Dopo aver assegnato tag alle risorse, è possibile prendere in considerazione l'approccio alla creazione di tag per le zone cloud, nonché i profili di storage e i profili di rete più adatti alle proprie esigenze.

Utilizzo di tag di funzionalità in Cloud Assembly

In Cloud Assembly i tag di funzionalità consentono di definire le funzionalità di distribuzione dei componenti dell'infrastruttura. Insieme ai vincoli, fungono da base per la logica di posizionamento in vRealize Automation.

È possibile creare tag di funzionalità su risorse di elaborazione, zone cloud, immagini e mappe di immagini, nonché su reti e profili di rete. Le pagine per la creazione di queste risorse contengono opzioni per la creazione di tag di funzionalità. In alternativa, è possibile utilizzare la pagina Gestione tag in Cloud Assembly per creare tag di funzionalità. I tag di funzionalità nelle zone cloud e nei profili di rete influiscono su tutte le risorse all'interno di tali zone o profili. I tag di funzionalità nei componenti di storage e di rete influiscono solo sui componenti in cui sono applicati.

In genere, i tag di funzionalità possono definire caratteristiche quali la posizione di una risorsa di elaborazione, un tipo di adattatore per una rete o un livello per una risorsa di storage. Possono inoltre definire la posizione o il tipo dell'ambiente e tutte le altre considerazioni commerciali. Come per la strategia di tag globale, è consigliabile organizzare i tag di funzionalità in modo logico in base alle esigenze aziendali.

Cloud Assembly corrisponde ai tag di funzionalità delle zone cloud con vincoli sui modelli cloud al momento della distribuzione. Pertanto, quando si creano e si utilizzano tag di funzionalità, è necessario comprendere e pianificare la creazione di vincoli dei modelli cloud, in modo che la corrispondenza si verifichi come previsto.

Ad esempio, la sezione della zona cloud nell'[Parte 1: configurazione dell'infrastruttura Cloud Assembly di esempio](#) incluso nella documentazione, descrive come creare tag dev e test per le zone OurCo-AWS-US-East e OurCo AWS-US-West. Nel tutorial, questi tag indicano che la zona OurCo-AWS-US-East è un ambiente di sviluppo e la zona OurCo-AWS-US_ West è un ambiente di test. Se si creano tag di vincolo analoghi in modelli cloud, questi tag di funzionalità consentono di indirizzare le distribuzioni agli ambienti desiderati.

Ereditarietà dei tag

Cloud Assembly utilizza l'ereditarietà dei tag per propagare selettivamente i tag negli account cloud in altre risorse correlate. In particolare, quando si creano tag in un account cloud, vengono applicati anche a tutti i profili di storage e le risorse di elaborazione che corrispondono a tale account cloud.

Nota Il comportamento di propagazione dei tag non si applica ai profili di storage. vRealize Automation non selezionerà automaticamente il vincolo per i profili di storage. Gli utenti devono aggiungere manualmente il tag di vincolo necessario affinché venga selezionato e applicato ai profili di storage.

L'esempio seguente illustra come funziona l'ereditarietà dei tag.

Risorse di elaborazione

- Cluster1 con tag cluster-1
- Cluster2 con tag cluster-2
- Cluster3 con tag cluster-3

```
Vm resource:
  properties:
    constraints:
      - tag: 'cluster-01'
```

Profili di storage

- Profilo 1 per Datastorecluster1 con tag storage-01
- Profilo 2 per Datastorecluster2 con tag storage-02
- Profilo 3 per Datastorecluster3 con tag storage-03

```
vm-resource:
  properties:
    storage:
      constraints:
        - tag: 'storage-01'
```

Account cloud

Account cloud di vSphere con tutti e tre i tag: cluster-1, cluster-2 e cluster-3

Durante il consolidamento dei tag nei profili di storage e nelle risorse di elaborazione, Cloud Assembly considera anche i tag a livello dell'account cloud. Di conseguenza, i tag effettivi in tutti i profili di storage e le risorse di elaborazione sono cluster-1, cluster-2 e cluster-3, e questo è il motivo per cui quando viene fornito uno di questi tag, come mostrato nell'esempio precedente, tutti i profili di storage e le risorse di elaborazione diventano idonei per il posizionamento e la macchina può pervenire a qualsiasi host delle risorse di elaborazione.

È consigliabile ridurre al minimo i risultati imprevisti e l'ingombro dei tag; qualsiasi tag deve essere applicato solo a livello di account cloud se tale tag è una funzionalità appropriata per tutte le risorse di elaborazione e di storage subordinate.

Utilizzo dei tag di vincolo in Cloud Assembly

I tag aggiunti ai progetti e ai modelli cloud fungono da tag di vincolo quando vengono utilizzati per abbinare i tag di funzionalità alle risorse dell'infrastruttura, ai profili e alle zone cloud. Nel caso dei modelli cloud, Cloud Assembly utilizza questa funzionalità corrispondente per allocare risorse per le distribuzioni.

Cloud Assembly consente di utilizzare i tag di vincolo in due modi principali. Il primo quando si configurano progetti e immagini. È possibile utilizzare i tag come vincoli per associare le risorse al progetto o all'immagine. Il secondo è in modelli cloud in cui i tag specificati come vincoli vengono utilizzati per selezionare le risorse per le distribuzioni. I vincoli applicati in entrambi questi modi vengono uniti nei modelli cloud per creare un set di requisiti di distribuzione che definiscono le risorse disponibili per una distribuzione.

Come funzionano i tag di vincolo nei progetti

Quando si configurano le risorse di Cloud Assembly, gli amministratori del cloud possono applicare i tag di vincolo nei progetti. In questo modo, gli amministratori possono applicare vincoli di governance direttamente a livello del progetto. Tutti i vincoli aggiunti a questo livello vengono applicati a ogni modello cloud richiesto per il progetto applicabile e questi tag di vincolo hanno la precedenza su altri tag.

Se i tag di vincolo nel progetto sono in conflitto con i tag di vincolo nel modello cloud, i tag del progetto hanno la precedenza, consentendo così all'amministratore del cloud di imporre le regole di governance. Ad esempio, se gli amministratori del cloud creano un tag `location:london` nel progetto, ma uno sviluppatore posiziona un tag `location:boston` nel modello cloud, il primo avrà la precedenza e la risorsa verrà distribuita nell'infrastruttura contenente il tag `location:london`.

Sono disponibili tre tipi di tag di vincolo che gli utenti possono applicare ai progetti: rete, storage ed estendibilità. È possibile applicare tutte le istanze di ogni tipo di tag necessarie. I vincoli del progetto possono essere permanenti o temporanei. Per impostazione predefinita sono permanenti. I vincoli permanenti consentono di imporre rigidamente le restrizioni della distribuzione. Se uno o più vincoli permanenti non sono soddisfatti, la distribuzione non riesce. I vincoli temporanei offrono un metodo per esprimere le preferenze che verranno selezionate se disponibili, ma la distribuzione riesce anche se tali vincoli non vengono soddisfatti.

Come funzionano i tag di vincolo nei modelli cloud

Nei modelli cloud è possibile aggiungere tag di vincolo alle risorse come codice YAML in modo che corrispondano ai tag di funzionalità appropriati creati dall'amministratore del cloud in risorse e zone cloud, nonché nei profili di rete e di storage. Sono inoltre disponibili altre opzioni più complesse per l'implementazione dei tag di vincolo. Ad esempio, è possibile utilizzare una variabile per popolare uno o più tag in una richiesta. In questo modo è possibile specificare uno o più tag al momento della richiesta.

Creare tag di vincolo utilizzando l'etichetta `tag` sotto un'intestazione di vincolo nel codice YAML del modello cloud. I tag di vincolo dei progetti vengono aggiunti ai tag di vincolo creati nei modelli cloud.

Cloud Assembly supporta una semplice formattazione stringa per semplificare l'uso dei vincoli nei file YAML:

```
[!]tag_key[:tag_value][:hard|:soft]
```

Per impostazione predefinita, Cloud Assembly crea un vincolo positivo con imposizione permanente. Il valore del tag è facoltativo, ma consigliato, come nel resto dell'applicazione.

Il seguente esempio di WordPress con MySQL mostra i tag di vincolo YAML che specificano le informazioni sulla posizione delle risorse di elaborazione.

```
name: "wordpressWithMySQL"
components:
  mysql:
    type: "Compute"
    data:
      name: "mysql"
      # ... skipped lines ...
  wordpress:
    type: "Compute"
    data:
      name: "wordpress"
      instanceType: small
      imageType: "ubuntu-server-1604"
      constraints:
        - tag: "!location:eu:hard"
        - tag: "location:us:soft"
        - tag: "!pci"
      # ... skipped lines ...
```

Per ulteriori informazioni sull'utilizzo dei modelli cloud, vedere [Parte 3: progettazione e distribuzione del modello di Cloud Assembly di esempio](#).

Come funzionano vincoli permanenti e temporanei in progetti e modelli cloud

I vincoli dei progetti e dei modelli cloud possono essere permanenti o temporanei. Il frammento di codice precedente mostra esempi di vincoli permanenti e temporanei. Per impostazione predefinita, tutti i vincoli sono permanenti. I vincoli permanenti consentono di imporre rigidamente le restrizioni della distribuzione. Se uno o più vincoli permanenti non sono soddisfatti, la distribuzione non riesce. I vincoli temporanei esprimono le preferenze che vengono applicate se disponibili, ma non causano la mancata riuscita di una distribuzione se non vengono soddisfatti.

Se in un tipo di risorsa specifico è presente una serie di vincoli permanenti e temporanei, i vincoli temporanei possono essere utilizzati anche come mezzi risolutivi. Ovvero, se più risorse soddisfano un vincolo permanente, i vincoli temporanei vengono utilizzati per selezionare la risorsa effettivamente utilizzata nella distribuzione.

Ad esempio, si supponga di creare un vincolo di storage permanente con un tag `location:boston`. Se nessuno storage nel progetto soddisfa questo vincolo, qualsiasi distribuzione correlata non riesce.

Tag standard

Cloud Assembly applica tag standard ad alcune distribuzioni per supportare l'analisi, il monitoraggio e il raggruppamento delle risorse distribuite.

I tag standard sono univoci all'interno di Cloud Assembly. A differenza di altri tag, gli utenti non li utilizzano durante la configurazione della distribuzione e non vengono applicati vincoli. Questi tag vengono applicati automaticamente durante il provisioning sulle distribuzioni AWS, Azure e vSphere. Questi tag vengono archiviati come proprietà personalizzate di sistema e vengono aggiunti alle distribuzioni dopo il provisioning.

Di seguito viene visualizzato l'elenco dei tag standard.

Tabella 4-3. Tag standard

Descrizione	Tag
Organizzazione	<code>org:orgID</code>
Progetto	<code>project:projectID</code>
Richiedente	<code>requester:username</code>
Distribuzione	<code>deployment:deploymentID</code>
Riferimento modello cloud (se applicabile)	<code>blueprint:blueprintID</code>
Nome componente nel blueprint	<code>blueprintResourceName:CloudMachine_1</code>
Vincoli di posizionamento: applicati nel blueprint, nei parametri di richiesta o tramite il criterio IT	<code>constraints:key:value:soft</code>

Tabella 4-3. Tag standard (continua)

Descrizione	Tag
Account cloud	cloudAccount:accountID
Zona o profilo, se applicabile	zone:zoneID, networkProfile:profileID, storageProfile:profileID

In che modo Cloud Assembly elabora i tag

In Cloud Assembly, i tag esprimono le funzionalità e i vincoli che determinano come e dove le risorse vengono allocate alle distribuzioni di cui è stato eseguito il provisioning durante il processo di provisioning.

Cloud Assembly utilizza un ordine e una gerarchia di operazioni specifici nella risoluzione dei tag per creare distribuzioni con provisioning eseguito. La comprensione delle nozioni fondamentali di questo processo consentirà di implementare i tag in modo efficiente per creare distribuzioni prevedibili.

Nell'elenco seguente vengono riepilogate le operazioni di alto livello e la sequenza che Cloud Assembly utilizza per risolvere i tag e definire una distribuzione:

- Le zone cloud sono filtrate da diversi criteri, tra cui disponibilità e profili. A questo punto vengono confrontati i tag nei profili per la regione a cui appartiene la zona.
- I tag di funzionalità della zona e delle risorse di elaborazione vengono utilizzati per filtrare le zone cloud rimanenti in base a vincoli permanenti.
- Fuori dalle zone filtrate, viene utilizzata la priorità per selezionare una zona cloud. Se sono presenti varie zone cloud con la stessa priorità, vengono ordinate in base ai vincoli temporanei corrispondenti, utilizzando una combinazione delle funzionalità della zona cloud e delle risorse di elaborazione.
- Dopo aver selezionato una zona cloud, viene selezionato un host associando una serie di filtri, tra cui i vincoli permanenti e temporanei espressi nei modelli cloud.

Come configurare una struttura di tag semplice

In questo argomento viene descritto un approccio di base e le opzioni per una strategia di tag di Cloud Assembly logica. È possibile utilizzare questi esempi come punto di partenza per una distribuzione effettiva oppure è possibile definire una strategia diversa che soddisfi meglio le proprie esigenze.

In genere, l'amministratore del cloud è il principale responsabile della creazione e della gestione dei tag.

Questo argomento si riferisce al caso d'uso di WordPress descritto altrove nella documentazione di Cloud Assembly per illustrare la modalità di aggiunta dei tag ad alcuni elementi chiave. Descrive anche possibili alternative ed estensioni agli esempi di tag che compaiono nel caso d'uso di WordPress.

Per ulteriori informazioni sul caso d'uso di WordPress, vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).

Il caso d'uso di WordPress descrive come posizionare i tag nelle zone cloud e nei profili di storage e di rete. Questi profili sono come pacchetti di risorse organizzati. I tag inseriti nei profili si applicano a tutti gli elementi all'interno del profilo. È inoltre possibile creare e posizionare tag in risorse di storage e singoli elementi di rete, nonché nelle risorse di elaborazione, ma questi tag si applicano solo alle risorse specifiche in cui sono posizionati. Quando si configurano i tag, in genere è preferibile iniziare applicando tag alle risorse di elaborazione, quindi è possibile aggiungere successivamente tag ai profili e alle zone cloud. Inoltre, questi tag vengono utilizzati per filtrare l'elenco delle risorse di elaborazione per una zona cloud.

Ad esempio, mentre è possibile inserire tag nei profili di storage, come mostrato in questo caso d'uso, è anche possibile inserire tag nei singoli criteri di storage, nei datastore e negli account di storage. I tag di queste risorse consentono di esercitare un controllo più preciso sulle modalità di distribuzione delle risorse di storage. Durante l'elaborazione in preparazione alla distribuzione, questi tag vengono risolti come livello successivo di elaborazione dopo i tag del profilo.

Come esempio della possibile configurazione di uno scenario tipico del cliente, è possibile collocare un tag di `region: eastern` in un profilo di rete. Questo tag si applicherebbe a tutte le risorse all'interno di tale profilo. È quindi possibile inserire un tag di `networktype:pci` su una risorsa di rete PCI all'interno del profilo. Un modello con vincoli eastern e PCI creerebbe distribuzioni che utilizzano questa rete PCI per la regione eastern.

Procedura

- 1 Contrassegnare le risorse dell'infrastruttura di elaborazione in modo logico e appropriato.

È particolarmente importante che le risorse di elaborazione vengano contrassegnate in modo logico in modo da poterle trovare utilizzando la funzione di ricerca nella scheda Risorse di elaborazione della pagina Crea zona cloud. Utilizzando questa funzione di ricerca, è possibile filtrare rapidamente le risorse di elaborazione associate a una zona cloud. Se si assegnano tag a storage e reti a livello di profilo, potrebbe non essere necessario assegnare tag alle singole risorse di storage e di rete.

- a Selezionare **Risorse > Risorse di elaborazione** per visualizzare le risorse di elaborazione importate per l'istanza di Cloud Assembly.
- b Selezionare ciascuna risorsa di elaborazione in base alle esigenze e fare clic su **Tag** per aggiungere un tag alla risorsa. Se necessario, è possibile aggiungere più tag a ciascuna risorsa.
- c Ripetere il passaggio precedente per le risorse di storage e di rete in base alle esigenze.

- 2 Creare tag di funzionalità per zone cloud e profili di rete.

È possibile utilizzare gli stessi tag per le zone cloud e i profili di rete oppure è possibile creare tag univoci per ogni elemento, se necessario per l'implementazione.

Nei profili di rete è possibile collocare tag sull'intero profilo, nonché sulle subnet all'interno del profilo. I tag applicati a livello di profilo si applicano a tutti i componenti, ad esempio le subnet, all'interno di tale profilo. I tag sulle subnet si applicano solo alla subnet specifica su cui sono posizionati. Durante l'elaborazione dei tag, i tag a livello del profilo hanno la precedenza rispetto ai tag a livello di subnet.

Per informazioni sull'aggiunta di tag alle zone cloud o ai profili di rete, vedere le sezioni relative alla zona cloud e alla rete dell'[Parte 1: configurazione dell'infrastruttura Cloud Assembly di esempio](#).

In questo esempio vengono creati tre semplici tag che vengono visualizzati in tutta la documentazione del caso d'uso per i tag di zone cloud e profili di rete di Cloud Assembly. Questi tag identificano l'ambiente per i componenti del profilo.

- `zone:test`
- `zone:dev`
- `zone:prod`

3 Creare tag del profilo di storage per i componenti dello storage.

In genere, i tag di storage identificano il livello di prestazioni degli elementi di storage, come tier1 o tier2, oppure identificano la natura degli elementi di storage, come ad esempio PCI.

Per informazioni sull'aggiunta di tag ai profili di storage, vedere la sezione relativa all'archiviazione dell'[Parte 1: configurazione dell'infrastruttura Cloud Assembly di esempio](#).

- `usage:general`
- `usage:fast`

Risultati

Dopo aver creato una struttura di tag di base, è possibile iniziare a utilizzarla e aggiungere o modificare i tag in modo appropriato per perfezionare ed estendere le funzionalità di tag.

Come utilizzare le risorse in vRealize Automation

Un amministratore del cloud può esaminare le risorse di vRealize Automation esposte tramite la raccolta dati.

L'amministratore del cloud può etichettare le risorse con i tag di funzionalità per determinare dove vengono distribuiti i modelli cloud di vRealize Automation.

Oltre a queste viste disponibili, è possibile gestire varie risorse utilizzando la scheda Risorse. Vedere [Gestione delle risorse in Cloud Assembly](#).

Risorse di elaborazione in vRealize Automation

Un amministratore del cloud può esaminare le risorse di elaborazione esposte tramite la raccolta dati.

L'amministratore del cloud può scegliere di applicare i tag direttamente alle risorse per etichettare le funzionalità a scopo di corrispondenza nel provisioning di vRealize Automation.

Risorse di rete in vRealize Automation

In vRealize Automation, gli amministratori del cloud possono visualizzare e modificare le risorse di rete che sono state raccolte dai dati degli account cloud e delle integrazioni mappate al progetto.

Dopo aver aggiunto un account cloud all'infrastruttura di Cloud Assembly, ad esempio utilizzando la sequenza di menu **Infrastruttura > Connessioni > Account cloud**, la raccolta dati individua le informazioni di rete e sicurezza dell'account cloud. Tali informazioni sono quindi disponibili per l'utilizzo nelle reti, nei profili di rete e in altre definizioni.

Le reti sono i componenti specifici dell'IP di un dominio di rete o zona di trasporto disponibile. Se si è un utente di Amazon Web Services o Microsoft Azure, considerare le reti come subnet.

È possibile visualizzare informazioni sulle reti nel progetto utilizzando la pagina **Infrastruttura > Risorse > Reti**.

La pagina Cloud Assembly **Reti** contiene informazioni quali:

- Reti e bilanciamenti del carico definiti esternamente nel dominio di rete dell'account cloud, ad esempio in vCenter, NSX-T o Amazon Web Services.
- Reti e bilanciamenti del carico che sono stati distribuiti dall'amministratore del cloud.
- Intervalli di IP e altre caratteristiche di rete definite o modificate dall'amministratore del cloud.
- Intervalli di IP del provider IPAM esterno per un particolare spazio di indirizzi in un'integrazione IPAM esterna specifica del provider.

Per ulteriori informazioni sulle reti, vedere le seguenti informazioni, la guida indicazioni per varie impostazioni nella pagina **Reti** e [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

Reti

È possibile visualizzare e modificare le reti e le relative caratteristiche, ad esempio per aggiungere tag o rimuovere il supporto dell'accesso degli IP pubblici. È inoltre possibile gestire le impostazioni di rete, ad esempio valori di tag, DNS, CIDR e gateway. È inoltre possibile definire intervalli di IP nuovi e gestire quelli esistenti in una rete.

Per le reti esistenti è possibile modificare l'intervallo IP e le impostazioni dei tag selezionando la casella di controllo della rete e selezionando **Gestisci intervalli IP** o **tag**. In caso contrario, è possibile selezionare la rete stessa per modificarne le informazioni.

I tag forniscono un mezzo per associare le reti appropriate e, facoltativamente, i profili di rete ai componenti di rete nei modelli cloud. I tag di rete vengono applicati a tutte le istanze di tale rete, indipendentemente dai profili di rete in cui la rete può risiedere. Le reti possono essere integrate in un numero qualsiasi di profili di rete. Indipendentemente dalla residenza del profilo di rete, un tag di rete è associato a tale rete ovunque venga utilizzata. La corrispondenza dei tag di rete viene eseguita con altri componenti nel modello cloud dopo che il modello cloud è stato associato a uno o più profili di rete.

Per le reti globali, le reti esistenti e pubbliche sono supportate per gli account cloud del manager globale e locale di NSX-T e per gli account cloud di vCenter associati ai manager locali. La rappresentazione del manager locale delle reti estese viene definita all'interno di una zona di trasporto. La zona di trasporto è un costrutto del manager locale di NSX-T che definisce l'intervallo delle reti di NSX-T per gli host e i cluster di vCenter Server.

Cloud Assembly enumera le reti esistenti e pubbliche o ne raccoglie i dati. È possibile creare una rete globale aggiungendo una rete esistente o pubblica in un manager globale di NSX-T. La rete globale può quindi essere utilizzata da tutti i manager locali associati. Le reti globali possono estendersi a uno, a tutti o a un sottoinsieme dei manager locali associati.

È possibile eseguire il provisioning di una macchina in una rete globale utilizzando un'assegnazione di IP statici. Il protocollo DHCP non è supportato.

È possibile creare i seguenti tipi di reti globali in un manager globale:

- 1 Overlay: una rete overlay viene associata a un manager locale di livello 0 e 1 e si estende automaticamente a tutti i siti connessi al manager locale di livello 0 e 1. Per ogni manager locale, viene utilizzata la zona di trasporto overlay predefinita.
- 2 VLAN: una rete VLAN si applica a un singolo manager locale e la zona di trasporto può essere selezionata manualmente.

Le reti globali sono elencate nella pagina **Infrastruttura > Risorse** con tutti gli account cloud a cui si applicano.

Le seguenti operazioni giorno 2 sono supportate per le reti globali:

- Riconfigurazione di una rete nella definizione di un modello cloud da una rete globale a una rete locale e viceversa.
- Scalabilità orizzontale/verticale di macchine su reti globali.

Per ulteriori informazioni sull'utilizzo delle reti nei modelli cloud, vedere [Ulteriori informazioni sulle risorse di rete nei modelli cloud di vRealize Automation](#).

Per informazioni sull'aggiornamento delle reti vSphere in vRealize Automation dopo la migrazione di NSX-T da N-VDS a C-VDS, vedere [Aggiornamento delle risorse di rete in vRealize Automation dopo la migrazione da N-VDS a C-VDS in NSX-T](#).

Intervalli IP

Utilizzare un intervallo di IP per definire o apportare modifiche all'indirizzo IP iniziale e finale per una particolare rete dell'organizzazione. È possibile visualizzare e gestire gli intervalli di IP per le reti elencate. Se la rete è gestita da un provider IPAM esterno, è possibile gestire gli intervalli di IP in relazione al punto di integrazione IPAM associato.

Fare clic su **Nuovo intervallo IP** per aggiungere un intervallo di IP aggiuntivo alla rete. È possibile specificare un **intervallo di IP interno** oppure, se è disponibile un'integrazione IPAM valida, è possibile specificare un **intervallo di IP esterno**.

Non è possibile includere il gateway predefinito in un intervallo di IP. L'intervallo di IP della subnet non può includere il valore del gateway della subnet.

Se si utilizza un'integrazione IPAM esterna per un determinato provider IPAM, è possibile utilizzare l'**intervallo di IP esterno** per selezionare un intervallo di IP da un punto di integrazione IPAM esterno disponibile. Questo processo è descritto nel contesto di un workflow di integrazione IPAM esterno complessivo in [Configurazione di una rete e di un profilo di rete per l'utilizzo di un IPAM esterno per una rete esistente in vRealize Automation](#).

Nota Quando un intervallo P di un provider IPAM esterno viene eliminato nell'applicazione IPAM esterna, l'intervallo IP viene eliminato automaticamente durante l'enumerazione in vRealize Automation. L'intervallo IP eliminato non è più visibile o disponibile per l'associazione di rete in vRealize Automation, evitando così intervalli di indirizzi IP orfani.

vRealize Automation consente di applicare e gestire un intervallo di indirizzi IP in più reti di vSphere e NSX. Il supporto dell'intervallo di IP condiviso viene fornito sia per l'IPAM interno sia per quello esterno. È possibile impostare un singolo intervallo di IP in una rete estesa di NSX in modo che le macchine di tale rete possano utilizzare indirizzi IP assegnati dal singolo indirizzo IP anche se sono distribuite in vCenter diversi.

Indirizzi IP

È possibile visualizzare gli indirizzi IP attualmente utilizzati dall'organizzazione e visualizzarne lo stato, ad esempio `available` o `allocated`. Gli indirizzi IP visualizzati sono indirizzi IP gestiti internamente da vRealize Automation o indirizzi IP designati per le distribuzioni che contengono un'integrazione del provider IPAM esterna. I provider di IPAM esterna gestiscono la propria allocazione di indirizzi IP.

Se la rete è gestita internamente da vRealize Automation e non da un provider IPAM esterno, è inoltre possibile rilasciare gli indirizzi IP.

Quando si utilizza l'IPAM interno e si rilasciano indirizzi IP, ad esempio dopo l'eliminazione di una macchina che utilizzava gli indirizzi IP o dopo aver fatto clic su **Rilascia indirizzo IP** per una rete selezionata, si verifica un periodo di attesa tra il rilascio degli indirizzi inutilizzati e quando saranno disponibili per il riutilizzo. Il periodo di attesa, o periodo di timeout del rilascio, consente di svuotare la cache DNS. Gli indirizzi IP possono quindi essere allocati a una nuova macchina. Per impostazione predefinita, il periodo di attesa per il rilascio dell'indirizzo IP è di 30 minuti. È possibile modificare il periodo di attesa facendo clic sull'opzione **Impostazioni** nell'angolo superiore destro della pagina **Reti** e modificando il valore **Timeout rilascio**.

- Durante il periodo del timeout di rilascio, gli indirizzi IP pertinenti vengono elencati come rilasciati. Quando il periodo del timeout di rilascio è scaduto, vengono elencati come disponibili.
- Il sistema controlla ogni 5 minuti i nuovi indirizzi IP rilasciati, quindi anche se il valore del timeout di rilascio è 1 minuto, possono essere necessari da 1 a 6 minuti prima che gli indirizzi IP rilasciati diventino disponibili, a seconda di quando è stato eseguito l'ultimo controllo. L'intervallo di controllo di 5 minuti si applica a tutti i valori diversi da 0.
- Se il valore del timeout di rilascio viene impostato su 0, gli indirizzi IP vengono rilasciati immediatamente e diventano disponibili immediatamente.

- Il valore del timeout di rilascio si applica a tutti gli account cloud dell'organizzazione.

Bilanciamenti del carico

È possibile gestire le informazioni sui bilanciamenti del carico disponibili per gli account cloud di account/regione dell'organizzazione. È possibile aprire e visualizzare le impostazioni configurate per ogni bilanciamento del carico disponibile. È inoltre possibile aggiungere e rimuovere tag per un bilanciamento del carico.

Per ulteriori informazioni sull'utilizzo dei bilanciamenti del carico nei modelli cloud, vedere [Ulteriori informazioni sulle risorse di bilanciamento del carico nei modelli cloud di vRealize Automation](#).

Domini di rete

L'elenco dei domini di rete contiene le reti correlate e non sovrapposte.

Risorse di sicurezza in vRealize Automation

Dopo aver aggiunto un account cloud in Cloud Assembly, la raccolta dati rileva le informazioni sulla rete e la sicurezza dell'account cloud e rende tali informazioni disponibili per l'uso nei profili di rete e altre opzioni.

I gruppi di sicurezza e le regole del firewall supportano l'isolamento di rete. I gruppi di sicurezza vengono raccolti in dati. Le regole del firewall non vengono raccolte in dati.

Utilizzando la sequenza di menu **Infrastruttura > Risorse > Sicurezza**, è possibile visualizzare i gruppi di sicurezza su richiesta che sono stati creati nelle progettazioni di modelli cloud di Cloud Assembly e i gruppi di sicurezza esistenti che sono stati creati nelle applicazioni di origine, ad esempio NSX-T e Amazon Web Services. I gruppi di sicurezza disponibili sono esposti dal processo di raccolta dati.

È possibile utilizzare un tag per associare l'interfaccia della macchina (NIC) a un gruppo di sicurezza in una definizione di modello cloud o in un profilo di rete. È possibile visualizzare i gruppi di sicurezza disponibili e aggiungere o rimuovere tag per i gruppi di sicurezza selezionati. Un autore di modelli cloud può assegnare uno o più gruppi di sicurezza a una scheda NIC della macchina per controllare la sicurezza della distribuzione.

Nella progettazione del modello cloud, il parametro `securityGroupType` nella risorsa del gruppo di sicurezza viene specificato come `existing` per un gruppo di sicurezza esistente o `new` per un gruppo di sicurezza su richiesta.

Gruppi di sicurezza esistenti

I gruppi di sicurezza esistenti vengono visualizzati e classificati nella colonna **Origine** come *Discovered*.

I gruppi di sicurezza esistenti dell'endpoint dell'account cloud sottostante, ad esempio le applicazioni NSX-V, NSX-T o Amazon Web Services, sono disponibili per l'utilizzo.

Un amministratore del cloud può assegnare uno o più tag a un gruppo di sicurezza esistente per consentirne l'utilizzo in un modello cloud. Un autore di modelli cloud può utilizzare una risorsa `Cloud.SecurityGroup` in una progettazione di modelli cloud per allocare un gruppo di sicurezza esistente utilizzando vincoli di tag. Un gruppo di sicurezza esistente richiede che nella progettazione del modello cloud sia specificato almeno un tag di vincolo nella risorsa di sicurezza.

Se si modifica un gruppo di sicurezza esistente direttamente nell'applicazione di origine, ad esempio nell'applicazione NSX di origine anziché in Cloud Assembly, gli aggiornamenti non sono visibili in Cloud Assembly finché non vengono eseguite le esecuzioni di raccolta dati e i dati raccolgono l'account cloud o il punto di integrazione associato da Cloud Assembly. La raccolta dei dati viene eseguita automaticamente ogni 10 minuti.

I gruppi di sicurezza esistenti sono supportati per gli account cloud del manager globale e del manager locale di NSX-T e gli account cloud di vCenter associati ai manager locali. Cloud Assembly enumera i gruppi di sicurezza esistenti, o ne raccoglie i dati, e li collega alle interfacce di rete (NIC) della macchina. È possibile creare un gruppo di sicurezza globale aggiungendo un gruppo di sicurezza esistente in un manager globale di NSX-T. Il gruppo di sicurezza globale può quindi essere utilizzato dai manager locali associati. I gruppi di sicurezza globali possono includere uno, tutti o un sottoinsieme dei manager locali associati.

- I gruppi di sicurezza globali esistenti sono supportati ed enumerati per tutte le regioni definite.
- I gruppi di sicurezza globali sono elencati nella pagina **Infrastruttura > Risorse** con tutti gli account cloud a cui si applicano.
- È possibile associare un'interfaccia della macchina (NIC) a un gruppo di sicurezza globale esistente direttamente in un modello cloud o nel profilo di rete selezionato.
- Le seguenti operazioni giorno 2 sono supportate per i gruppi di sicurezza globali:
 - Riconfigurazione del gruppo di sicurezza in un modello cloud da un gruppo di sicurezza globale a un gruppo di sicurezza locale e viceversa.
 - Scalabilità orizzontale/verticale delle macchine associate ai gruppi di sicurezza globali.

Gruppi di sicurezza su richiesta

I gruppi di sicurezza su richiesta creati in Cloud Assembly, in un modello cloud o in un profilo di rete, vengono visualizzati e classificati nella colonna **Origine** come `Managed by Cloud Assembly`. I gruppi di sicurezza su richiesta creati come parte di un profilo di rete sono classificati internamente come un gruppo di sicurezza di isolamento con regole firewall preconfigurate e non

vengono aggiunti a una progettazione di modelli cloud come risorsa del gruppo di sicurezza. I gruppi di sicurezza su richiesta creati in una progettazione di modelli cloud, che possono contenere regole del firewall esplicite, vengono aggiunti come parte di una risorsa del gruppo di sicurezza classificata come `new`.

Nota È possibile creare regole del firewall per i gruppi di sicurezza su richiesta per NSX-V e NSX-T direttamente in una risorsa del gruppo di sicurezza nel codice di progettazione del modello cloud. La colonna **Applicato a** non contiene gruppi di sicurezza classificati o gestiti da un NSX Distributed firewall (DFW). Le regole del firewall che si applicano alle applicazioni sono per il traffico DFW est/ovest. Alcune regole del firewall possono essere gestite solo nell'applicazione di origine e non possono essere modificate in Cloud Assembly. Ad esempio, le regole ethernet, emergency, infrastructure e environment sono gestite in NSX-T.

I gruppi di sicurezza su richiesta non sono attualmente supportati per gli account cloud del manager globale di NSX-T.

Ulteriori informazioni

Per ulteriori informazioni sull'utilizzo dei gruppi di sicurezza nei profili di rete, vedere [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

Per informazioni sulla definizione delle regole firewall, vedere [Utilizzo delle impostazioni dei gruppi di sicurezza in profili di rete e progettazioni di modelli cloud in vRealize Automation](#).

Per ulteriori informazioni sull'utilizzo dei gruppi di sicurezza in un modello cloud, vedere [Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation](#).

Per gli esempi di codice di progettazione dei modelli cloud che contengono gruppi di sicurezza, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Risorse di storage in vRealize Automation

Un amministratore del cloud può utilizzare le risorse di storage e le relative funzionalità, individuate tramite la raccolta dati di vRealize Automation dagli account cloud associati.

Le funzionalità delle risorse di storage vengono esposte tramite tag che in genere provengono dall'account cloud di origine. Un amministratore del cloud può scegliere di applicare tag aggiuntivi direttamente alle risorse di storage, utilizzando Cloud Assembly. I tag aggiuntivi possono etichettare una funzionalità specifica a scopo di corrispondenza al momento del provisioning.

vRealize Automation supporta le funzionalità disco standard e First Class Disk. First Class Disk è disponibile solo per vSphere.

- [Cosa è possibile fare con lo storage su disco standard in vRealize Automation](#)
- [Cosa è possibile fare con lo storage FCD \(First Class Disk\) in vRealize Automation](#)

Le funzionalità sulle risorse di storage diventano visibili come parte della definizione di un profilo di storage di Cloud Assembly. Vedere [Ulteriori informazioni sui profili di storage in vRealize Automation](#).

I First Class Disk di cui sono stati raccolti i dati vengono visualizzati nella vista **Risorse > Risorse > Volumi**.

Ulteriori informazioni sulle risorse in Cloud Assembly

Cloud Assembly può esporre informazioni aggiuntive sui dati raccolti dalle risorse, ad esempio le schede dei prezzi.

Come funziona la raccolta dati in vRealize Automation

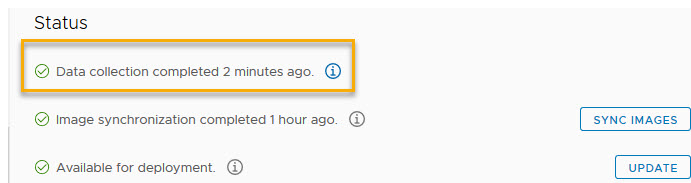
Dopo la raccolta dati iniziale, la raccolta dati delle risorse viene eseguita automaticamente ogni 10 minuti. L'intervallo di raccolta dati non è configurabile e non è possibile avviare manualmente la raccolta dati.

È possibile individuare informazioni sulla raccolta dati delle risorse e sulla sincronizzazione delle immagini per un account cloud esistente nella sezione **Stato** della relativa pagina. A tale scopo, selezionare **Infrastruttura > Connessioni > Account cloud** e quindi fare clic su **Apri** nell'account cloud esistente di propria scelta.

È possibile aprire un account cloud esistente e visualizzarne la versione dell'endpoint associato nella sezione **Stato** della relativa pagina. Se l'endpoint associato è stato aggiornato, la nuova versione dell'endpoint viene rilevata durante la raccolta dei dati e riflessa nella sezione **Stato** nella pagina dell'account cloud.

Raccolta dati delle risorse

La raccolta dati viene eseguita automaticamente ogni 10 minuti. Ogni account cloud viene visualizzato quando la raccolta dati è stata completata.

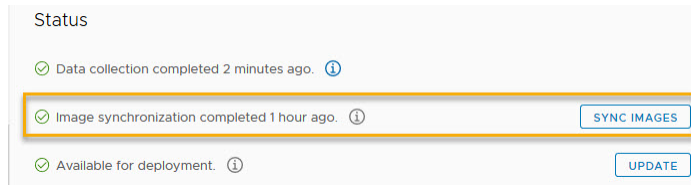


Raccolta dati delle immagini

La sincronizzazione delle immagini avviene ogni 24 ore. È possibile avviare la sincronizzazione delle immagini per alcuni tipi di account cloud. Per avviare la sincronizzazione delle immagini, aprire l'account cloud (**Infrastruttura > Account cloud** quindi selezionare e aprire l'account cloud esistente) e fare clic sul pulsante **Sincronizza immagini**. Non è disponibile alcuna opzione di sincronizzazione delle immagini per gli account cloud di NSX.

Nota Le immagini sono classificate internamente come pubbliche o private. Le immagini pubbliche sono condivise e non sono specifiche di una particolare sottoscrizione oppure organizzazione cloud. Le immagini private non sono condivise e sono specifiche di una sottoscrizione specifica. Le immagini pubbliche e private vengono sincronizzate automaticamente ogni 24 ore. Un'opzione nella pagina Account cloud consente di attivare la sincronizzazione delle immagini private.

La pagina Account cloud viene visualizzata al termine della sincronizzazione delle immagini.



Per semplificare la tolleranza agli errori e l'alta disponibilità nelle distribuzioni, ogni endpoint del data center di NSX-T rappresenta un cluster di tre NSX Manager. Per informazioni correlate, vedere [Creazione di un account cloud di NSX-T in vRealize Automation](#).

Account cloud e piani di onboarding

Quando si crea un account cloud, vengono raccolti i dati di tutte le macchine associate a tale account e le macchine vengono visualizzate nella pagina **Risorse > Risorse > Macchine virtuali**. Se l'account cloud include macchine distribuite all'esterno di Cloud Assembly, è possibile utilizzare un piano di onboarding per consentire a Cloud Assembly di gestire le distribuzioni delle macchine.

Per informazioni sull'aggiunta degli account cloud, vedere [Aggiunta di account cloud a Cloud Assembly](#).

Per informazioni sull'onboarding delle macchine non gestite, vedere [Che cosa sono i piani di onboarding in Cloud Assembly](#).

Aggiornamento delle risorse di rete in vRealize Automation dopo la migrazione da N-VDS a C-VDS in NSX-T

Dopo la migrazione di NSX-T da NSX Virtual Distributed Switch (N-VDS) a Converged VDS (C-VDS), è necessario aggiornare le risorse di rete di vSphere interessate in vRealize Automation per continuare a utilizzare le risorse nelle distribuzioni e nei modelli cloud nuovi ed esistenti.

Dopo la migrazione da N-VDS a C-VDS, è possibile che le reti di vSphere manchino dai profili di rete di vRealize Automation di cui sono membri. Per evitare di perdere queste reti di tipo vSphere e continuare ad allocarle nelle distribuzioni esistenti e nuove, è necessario aggiornare manualmente tutte le reti C-VDS elencate in vRealize Automation Cloud Assembly.

Nota Questa procedura è specifica per le azioni necessarie in vRealize Automation per aggiornare le reti *vSphere* dopo che la migrazione da N-VDS a C-VDS è stata eseguita in NSX-T. Non è necessario eseguire alcuna azione in vRealize Automation per le reti *NSX* dopo la migrazione da N-VDS a C-VDS. Le reti *NSX* non richiedono alcun intervento manuale dopo la migrazione da N-VDS a C-VDS.

Anche se un amministratore di NSX-T può eseguire la migrazione dei tipi di rete NSX-T in VDS (N-VDS) ai tipi di rete Converged VDS (C-VDS) in NSX, questa azione influisce sulle risorse di rete di vSphere esistenti in vRealize Automation. L'amministratore di vRealize Automation può eseguire azioni successive alla migrazione per riconciliare tali risorse in vRealize Automation con le modifiche associate in NSX-T e vCenter Server. Si tenga presente che C-VDS, o semplicemente VDS, viene anche chiamato Virtual Distributed Switch (VDS) di vSphere 7.

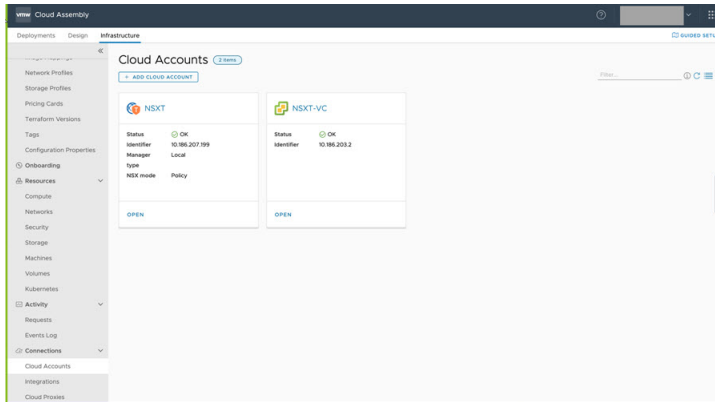
Per informazioni su Converged VDS di NSX-T, vedere gli articoli della Knowledge Base di VMware [NSX-T in VDS \(79872\)](#) e [Migrazione di VMware Cloud on AWS \(VMConAWS\) e VMware Cloud on Dell EMC da N-VDS a VDS \(82487\)](#).

Nota Questo scenario di esempio illustra i passaggi necessari per riconciliare le risorse in un ambiente vRealize Automation dopo la migrazione da N-VDS a C-VDS. È possibile utilizzare questo esempio e la procedura in vRealize Automation 8.5 e versioni successive per riconciliare le modifiche apportate in vCenter Server dopo la migrazione da N-VDS a C-VDS in NSX-T.

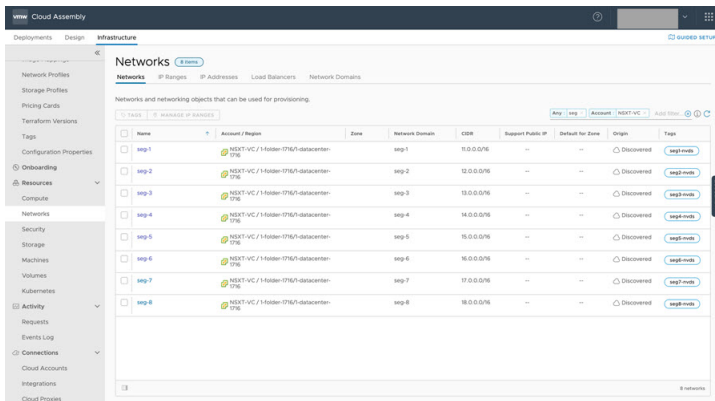
Esempio: risorse di vRealize Automation prima della migrazione

In questo esempio vengono illustrate risorse di NSX-T di esempio in un ambiente di vRealize Automation di esempio prima della migrazione da N-VDS a C-VDS.

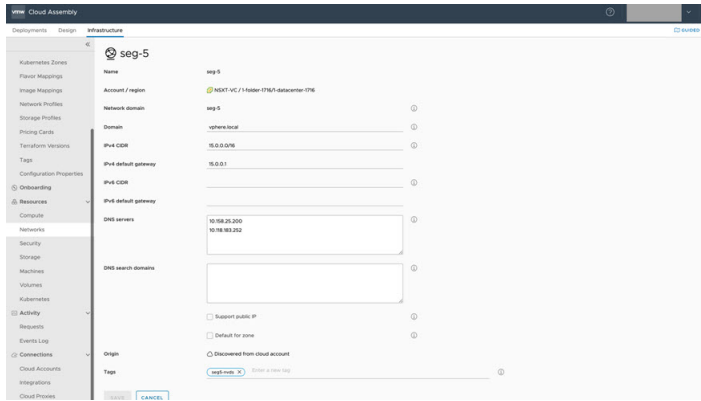
- Questo esempio include account cloud di NSX-T e vCenter come illustrato di seguito.



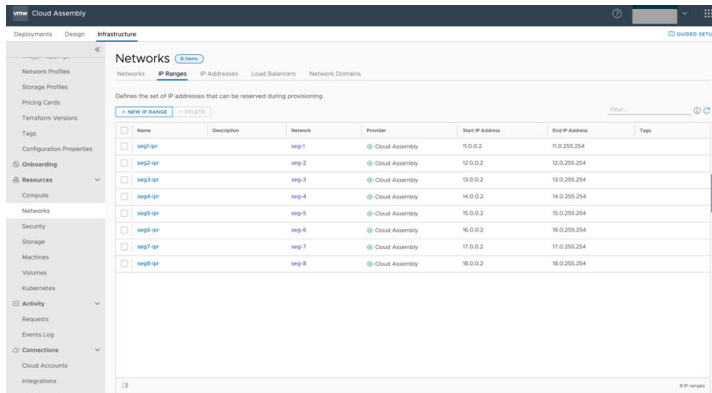
- L'esempio contiene diverse reti vSphere, come illustrato di seguito.



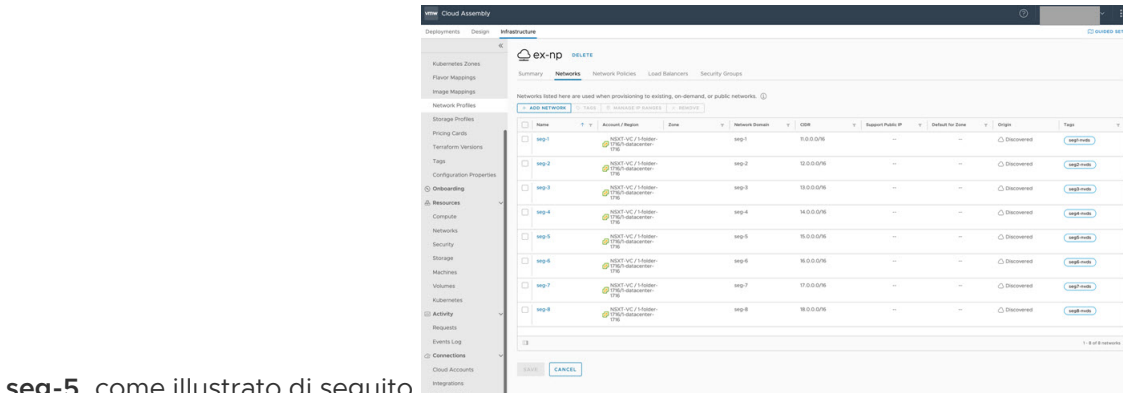
- La configurazione di rete di esempio contiene le impostazioni CIDR e DNS, come illustrato di seguito.



- L'esempio include anche intervalli di IP esistenti, come illustrato di seguito.

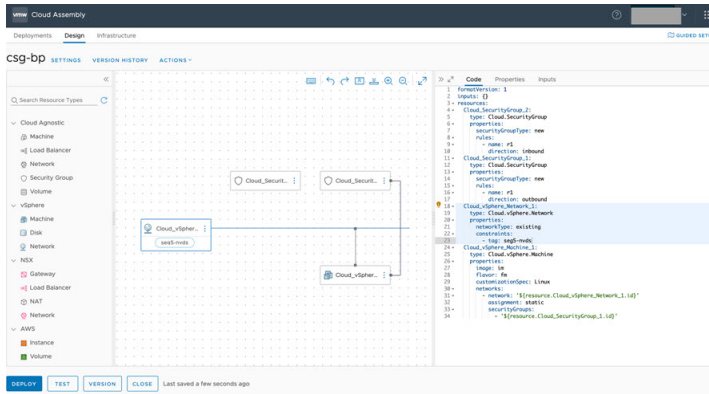


- L'esempio contiene un profilo di rete (**ex-np**) che contiene diverse reti N-VDS (N-VDS), tra cui

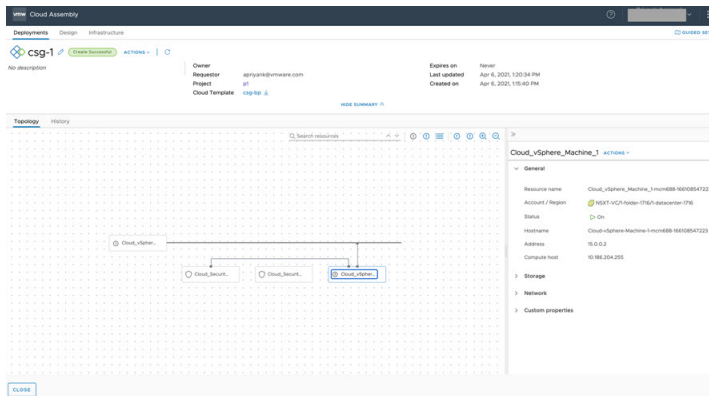


seg-5, come illustrato di seguito.

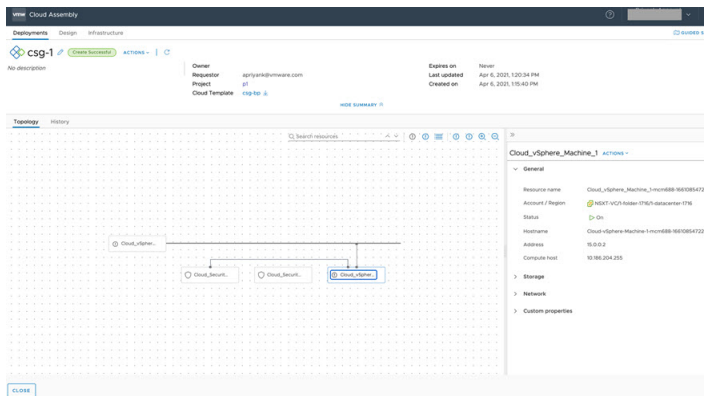
- In questo esempio, il componente di rete **seg5** esistente è illustrato nella seguente sintassi del modello cloud. La rete è contrassegnata come rete N-VDS. In questo esempio verranno illustrati gli aggiornamenti successivi alla migrazione necessari per la rete **seg5**.



- Il modello cloud di esempio genera la distribuzione, come illustrato di seguito.



- Gli indirizzi IP delle macchine di esempio sono visualizzati nella distribuzione di esempio, come illustrato di seguito.



Esempio: passaggio 1 successivo alla migrazione - Eseguire la raccolta dei dati dopo la migrazione da N-VDS a C-VDS e l'enumerazione

Nella sezione precedente, sono state utilizzate schermate per illustrare l'infrastruttura utilizzata in un ambiente di vRealize Automation di esempio per poi concludere con il modello cloud e la distribuzione risultanti.

Dopo aver eseguito la migrazione da N-VDS a C-VDS in NSX-T o dopo che questa migrazione è stata eseguita da un altro amministratore, attendere almeno 10 minuti per consentire a vRealize Automation di eseguire il processo periodico di raccolta ed enumerazione dei dati per recuperare e visualizzare le risorse interessate in vRealize Automation.

Dopo aver atteso il completamento della raccolta dei dati di vRealize Automation, fare clic su **Infrastruttura > Reti** per visualizzare le reti C-VDS disponibili e accedervi. Si noti la rete **seg5**, come illustrato di seguito.

Name	Account / Region	Zone	Network domain	CIDR	Support Public IP	Default for Zone	Origin	Tags
seg 8	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	18.0.0.0/16	--	--	Discovered	seg8
seg 7	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	17.0.0.0/16	--	--	Discovered	seg7
seg 6	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	16.0.0.0/16	--	--	Discovered	seg6
seg 5	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	15.0.0.0/16	--	--	Discovered	seg5
seg 4	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	14.0.0.0/16	--	--	Discovered	seg4
seg 3	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	13.0.0.0/16	--	--	Discovered	seg3
seg 2	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	12.0.0.0/16	--	--	Discovered	seg2
seg 1	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	11.0.0.0/16	--	--	Discovered	seg1
2-switch-380	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	--	--	--	Discovered	
1-switch-383	NSX-T VCF / 1 folder / 1766 / datacenter-176		CVDS-microswitch1-datacenter-4	--	--	--	Discovered	

Esempio: passaggio 2 successivo alla migrazione - Aggiungere CIDR e DNS definiti in precedenza alle reti C-VDS migrate

Modificare una rete C-VDS migrata per aggiungere i dettagli di CIDR e DNS specificati nella definizione di N-VDS precedente alla migrazione e modificare i tag di rete.

- 1 Aggiungere i dettagli di CIDR e DNS specificati nella definizione di N-VDS precedente alla migrazione
- 2 Aggiungere un nuovo tag per il segmento di rete C-VDS **seg-5**, ad esempio *seg5-cvds*.

Si tenga presente che la rete N-VDS originale **seg-5** è stata contrassegnata come *seg5-nvds*, come indicato nelle schermate precedenti. La modifica dei dettagli dei tag della risorsa è richiesta dalla riconfigurazione della rete. vRealize Automation richiede l'inclusione nel modello cloud per la rete C-VDS di un nome di tag diverso da quello utilizzato nella rete N-VDS originale. L'assegnazione dei tag modificata identifica una modifica nel modello cloud quando si genera una redistribuzione valida.

Esempio: passaggio 3 successivo alla migrazione - Aggiungere informazioni aggiornate sull'intervallo di IPe

È possibile modificare gli intervalli di IP della rete specificando i dettagli degli intervalli di IP indicati nella definizione di N-VDS prima della migrazione, tramite un'API della riga di comando o una sequenza di menu in vRealize Automation.

- Opzione 1: utilizzare l'API per aggiornare i dati dell'intervallo di IP come illustrato nella schermata di esempio seguente.

PATCH : `{{host}}/iaas/api/network-ip-ranges/{{subnet-range-id}}`

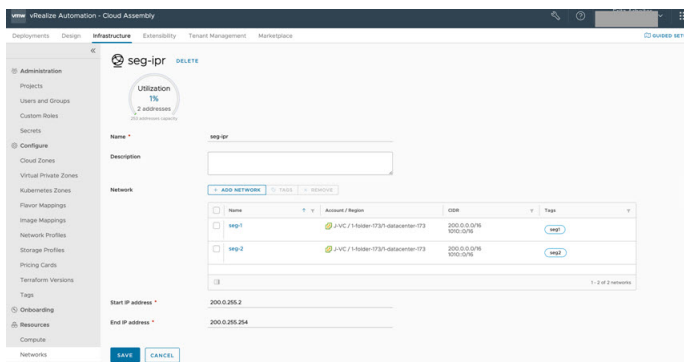
Headers :

- Authorization : Bearer `{{token}}`

Payload :

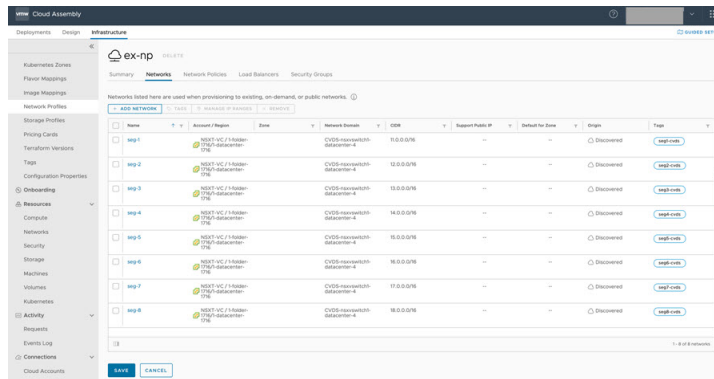
```
{
  "fabricNetworkIds": ["{{subnet-id}}"]
}
```

- Opzione 2: utilizzare l'interfaccia utente per aggiornare i dati dell'intervallo di IP come illustrato nella schermata di esempio seguente.



Esempio: passaggio 4 successivo alla migrazione - Aggiornare i profili di rete per correggere le reti mancanti

Dopo la migrazione, le reti N-VDS vengono riconciliate ed eliminate da vRealize Automation Cloud Assembly dopo la raccolta e l'enumerazione dei dati. Nei profili di rete interessati (ad esempio, **ex-np**) mancano alcune reti. Per correggere il problema delle reti mancanti, aggiornare ciascuna rete N-VDS a rete C-VDS, come illustrato di seguito.

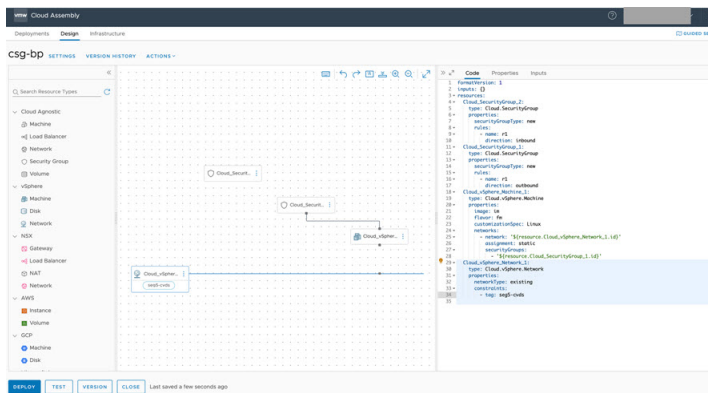


Esempio: passaggio 5 successivo alla migrazione - Aggiornare i vincoli di rete nel modello cloud

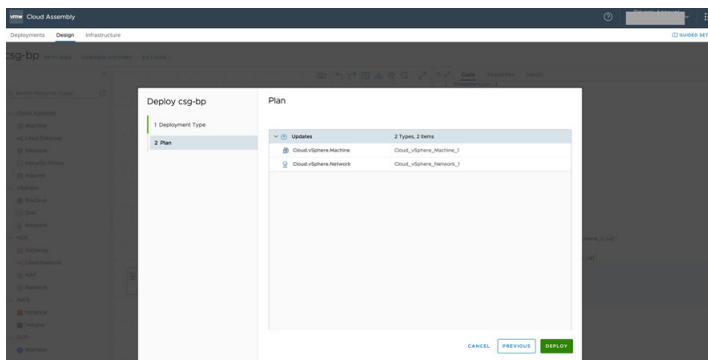
Per le distribuzioni esistenti, è necessario aggiornare i vincoli di rete nel modello cloud in modo che corrispondano alle nuove reti C-VDS nei profili di rete aggiornati. I vincoli di rete aggiornati sono necessari anche per eseguire distribuzioni iterative e riconfigurare le reti dalla rappresentazione vSphere N-VDS originale alla rappresentazione vSphere C-VDS.

Per le nuove distribuzioni vengono utilizzate le risorse C-VDS specificate, quindi questo passaggio non è necessario. Le distribuzioni iterative e la riconfigurazione di rete funzionano semplicemente come previsto.

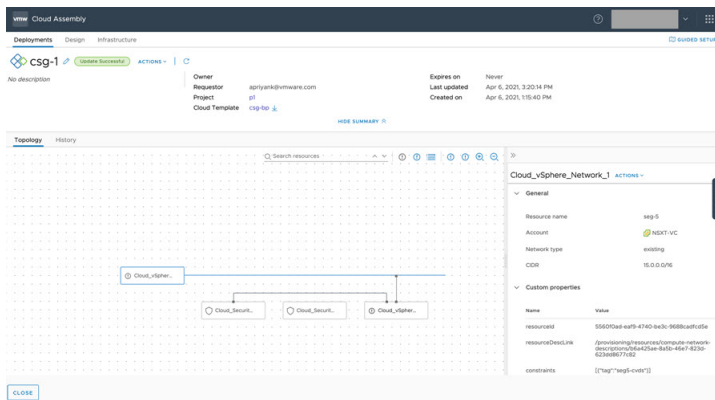
- 1 Per questo esempio, modificare i vincoli di rete nel modello cloud da *seg5-nvds* a *seg5-cvds* come illustrato di seguito.



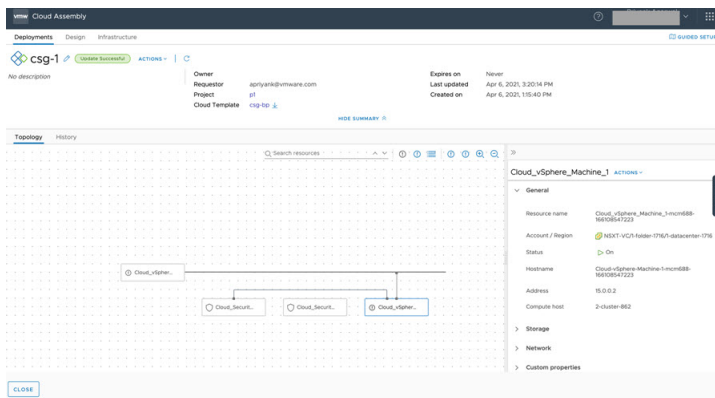
- 2 Eseguire una distribuzione iterativa per riconfigurare la rete come illustrato di seguito.



- 3 Dopo una redistribuzione corretta, si noti che le proprietà personalizzate di rete visualizzano i vincoli aggiornati come illustrato di seguito.



Poiché l'intervallo di IP è stato aggiornato in precedenza con i nuovi dati di C-VDS, l'indirizzo IP della macchina non viene modificato correttamente nella redistribuzione, come illustrato di seguito.



Come utilizzare il dashboard Dettagli per monitorare la capacità delle risorse e informare i proprietari dei progetti in vRealize Automation

Un amministratore del cloud può monitorare e gestire le risorse dell'infrastruttura e le ottimizzazioni della distribuzione all'interno di ogni zona cloud. Visualizzando dettagli in tempo reale e rivedendo le azioni suggerite per le risorse supportate, è possibile aiutare proattivamente i proprietari dei progetti a gestire le proprie capacità delle risorse e ottimizzare le loro distribuzioni.

È possibile utilizzare il dashboard **Dettagli** per esplorare i dati delle metriche per le risorse e le distribuzioni nelle zone cloud all'interno dei progetti gestiti. Tali informazioni, fornite dalla combinazione di vRealize Automation e dell'applicazione vRealize Operations Manager integrata, possono essere utilizzate per apportare le modifiche necessarie alla memoria, alla CPU e così via o condivise con i membri del team in modo da informarli meglio e consentire loro di apportare le eventuali modifiche necessarie.

Il dashboard Dettagli consente di contattare alcuni o tutti i proprietari di progetti che hanno distribuzioni nella zona cloud che contengono capacità di risorse recuperabili. I dettagli della zona cloud mostrano la capacità recuperabile per i progetti e le distribuzioni.

I proprietari del progetto contattati visualizzano la notifica nella pagina **Avvisi** della distribuzione. La notifica conterrà il loro nome e il nome e il collegamento di ogni distribuzione che può essere ottimizzata.

Il dashboard **Dettagli** è disponibile per le zone cloud di vSphere e VMware Cloud on AWS, a condizione che gli account cloud siano configurati in vRealize Automation e in vRealize Operations Manager e che siano monitorati in vRealize Operations Manager.

Prerequisiti

- Rivedere [Ottimizzazione di distribuzione e gestione delle risorse utilizzando metriche di vRealize Operations Manager in vRealize Automation](#).
- Verificare di disporre delle credenziali di amministratore del cloud di vRealize Automation e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud di vRealize Automation. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Configurare l'integrazione di vRealize Automation con vRealize Operations Manager.
- Configurare l'adattatore di vRealize Automation in vRealize Operations Manager.

Informazioni su vRealize Operations Manager e sulle metriche di capacità delle risorse raccolte

vRealize Operations Manager raccoglie le metriche di capacità per le stesse risorse dell'infrastruttura utilizzate dall'utente e dai team supportati in vRealize Automation. Integrando vRealize Automation con vRealize Operations Manager, i dati metrici di vRealize Operations Manager vengono resi disponibili e visualizzati per ogni progetto gestito in un dashboard **Dettagli** in ciascuna zona cloud.

I dati del progetto vengono analizzati nel dashboard vRealize Automation dall'applicazione vRealize Operations Manager integrata. Nel dashboard **Dettagli** vengono visualizzate le seguenti informazioni:

- Percentuale di utilizzo della CPU rispetto alla capacità
- Percentuale di utilizzo della memoria rispetto alla capacità
- Percentuale di utilizzo dello storage rispetto alla capacità
- Cronologia della richiesta di memoria e CPU calcolata e richiesta prevista
- Opzione per contattare i proprietari di alcune o tutte le distribuzioni in una zona cloud che può essere ottimizzata recuperando risorse, ad esempio ridimensionando o eliminando macchine. I dati di ottimizzazione vengono calcolati nell'ordine di giorni.

Il dashboard **Dettagli** è disponibile per le risorse di vSphere.

Un widget delle tendenze mostra i componenti di elaborazione di una zona cloud (ad esempio cluster e host), l'utilizzo GHz della CPU relativo alla capacità della CPU e l'utilizzo dei GB di memoria relativi alla capacità di memoria.

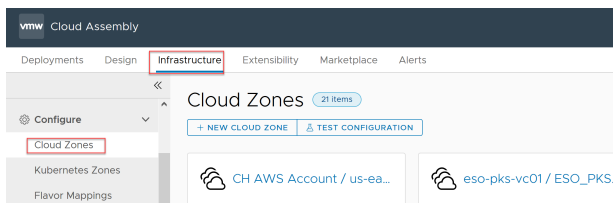
Le informazioni sui ruoli necessari per utilizzare gli avvisi sono disponibili qui: [Ruoli utente personalizzati in vRealize Automation](#).

Per informazioni correlate, vedere [Ottimizzazione di distribuzione e gestione delle risorse utilizzando metriche di vRealize Operations Manager in vRealize Automation](#).

Procedura

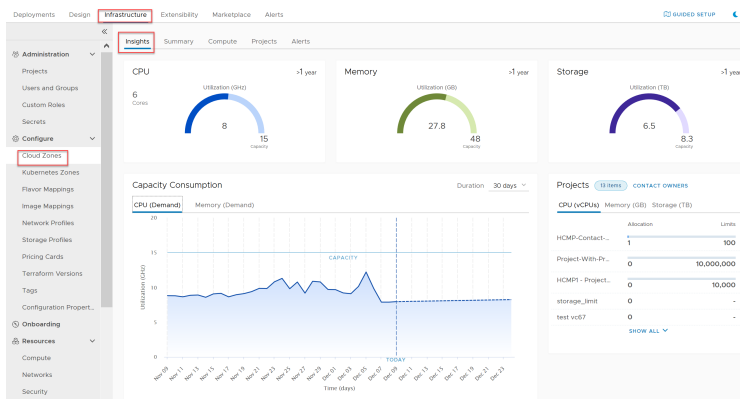
Aprire una zona cloud per individuare le relative metriche di capacità e, facoltativamente, recuperare informazioni sulle distribuzioni del progetto che possono essere ottimizzate. I dati vengono raccolti e forniti dall'applicazione vRealize Operations Manager associata.

- 1 Da Cloud Assembly, fare clic su **Infrastruttura > Configura > Zone cloud** e selezionare una zona cloud.

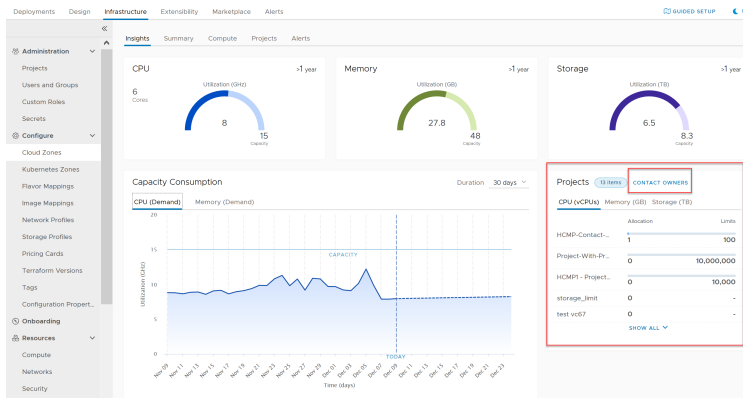


- 2 Fare clic sulla scheda **Dettagli** ed esaminare il dashboard Dettagli.

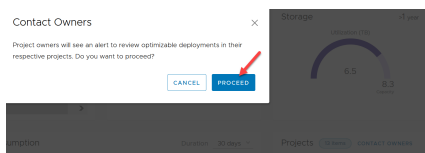
Nell'esempio seguente vengono visualizzate le informazioni su CPU, memoria e capacità di storage per le risorse utilizzate dai progetti nella zona cloud.



- 3 Per informare il proprietario del progetto di tutte le distribuzioni che possono essere ottimizzate, fare clic su **Contatta proprietario** nella sezione **Progetti**. Le notifiche vengono visualizzate nella pagina della scheda **Avvisi**.

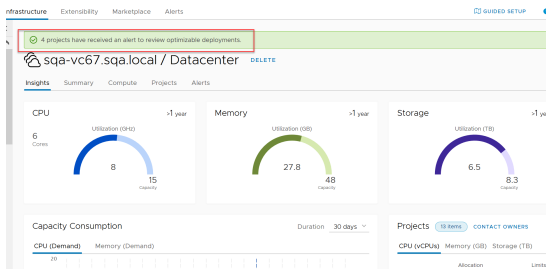


- 4 Per recuperare le informazioni sull'ottimizzazione di tutte le distribuzioni per il progetto, fare clic su **Continua**.

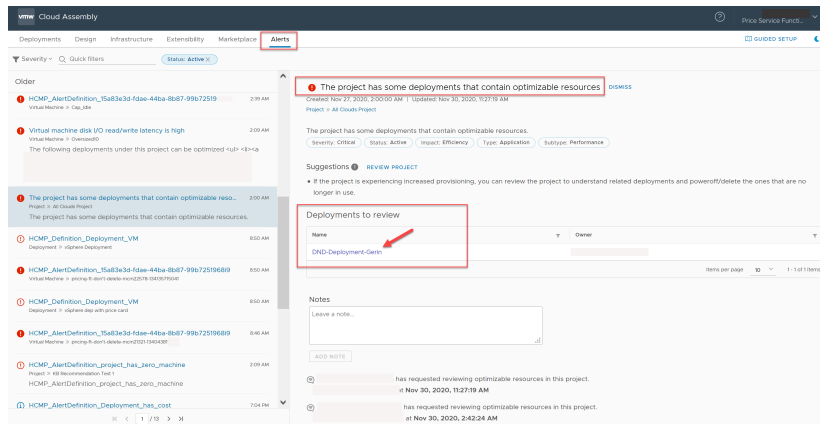


Se il progetto contiene distribuzioni che possono essere ottimizzate, l'informazione viene trasmessa al proprietario del progetto nella scheda **Avvisi** di Cloud Assembly.

- 5 Viene visualizzato un messaggio che indica il numero di distribuzioni che possono essere ottimizzate.



Il proprietario del progetto troverà le informazioni delle notifiche relative a queste risorse e distribuzioni nella scheda **Avvisi** di Cloud Assembly. Per questo esempio, le informazioni della notifica includono il nome e un collegamento a ogni distribuzione che può essere ottimizzata, come illustrato nell'esempio seguente:



Passaggi successivi

Utilizzare le informazioni ottenute dal dashboard **Dettagli** per apportare le modifiche necessarie alle risorse gestite. Aprire la pagina **Avvisi** per ottenere informazioni aggiuntive, azioni suggerite e collegamenti alle distribuzioni che possono essere ottimizzate. Vedere [Come utilizzare Avvisi per gestire capacità, prestazioni e disponibilità delle risorse in vRealize Automation](#).

Come utilizzare Avvisi per gestire capacità, prestazioni e disponibilità delle risorse in vRealize Automation

In qualità di amministratore del cloud, è necessario sapere quando la capacità, le prestazioni o la disponibilità di vRealize Automation stanno diventando aspetti problematici, in modo da poter reagire preventivamente e prima che gli utenti comincino a esaurire le risorse.

È possibile visualizzare una serie di avvisi fornito dall'applicazione vRealize Operations Manager associata. Gli avvisi sono disponibili per gli oggetti risorsa di vSphere e VMware Cloud on AWS. Utilizzare le informazioni contenute negli avvisi per modificare le risorse e le distribuzioni gestite o condividere tali informazioni con il team in modo che possa modificare gli oggetti che gestisce.

Nota Per esaminare ed agire sulle distribuzioni dei progetti che si intende ottimizzare, vedere [Come utilizzare gli avvisi per ottimizzare le distribuzioni in vRealize Automation](#).

Gli avvisi sono al momento disponibili solo per gli oggetti risorsa di vSphere e VMware Cloud on AWS. La scheda **Avvisi** è disponibile solo se è configurato l'accesso a vRealize Operations Manager.

I valori di soglia degli avvisi di vRealize Automation sono impostati in vRealize Operations Manager. Alcuni avvisi di vRealize Automation attualmente sono predefiniti. Anche le notifiche degli avvisi sono impostate in vRealize Operations Manager. Per informazioni sull'impostazione delle definizioni degli avvisi e sulla configurazione delle notifiche, consultare la vRealize Operations Manager [documentazione di prodotto](#).

Prerequisiti

- Rivedere [Ottimizzazione di distribuzione e gestione delle risorse utilizzando metriche di vRealize Operations Manager in vRealize Automation](#).

- Verificare di disporre delle credenziali di amministratore del cloud di vRealize Automation e di aver abilitato l'accesso HTTPS sulla porta 443. Vedere [Credenziali necessarie per l'utilizzo di account cloud in vRealize Automation](#).
- Verificare di disporre del ruolo utente di amministratore del cloud di vRealize Automation. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Configurare l'integrazione di vRealize Automation con vRealize Operations Manager.
- Configurare l'adattatore di vRealize Automation in vRealize Operations Manager.
- Configurare i ruoli necessari per gestire gli avvisi. Vedere [Ruoli utente personalizzati in vRealize Automation](#).

Le funzionalità del ruolo includono:

- Gli amministratori del cloud possono gestire gli avvisi della zona cloud.
- Gli amministratori di progetto possono gestire gli avvisi del progetto.
- Gli amministratori di Service Broker possono gestire gli avvisi di distribuzione.

Informazioni su vRealize Operations Manager e avvisi delle risorse

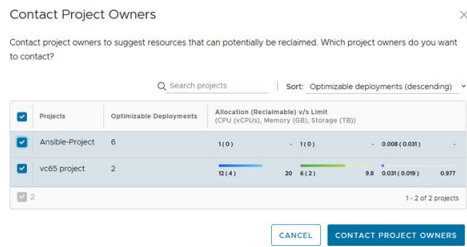
vRealize Operations Manager raccoglie metriche di integrità, utilizzo e altre per le stesse risorse e distribuzioni dell'infrastruttura gestite in vRealize Automation. Integrando vRealize Automation con vRealize Operations Manager, i dati monitorati vengono resi disponibili in vRealize Automation utilizzando la scheda **Avvisi** nel menu principale di Cloud Assembly.

I dati degli avvisi forniti da vRealize Operations Manager includono problematiche relative a integrità e soglie di rischio per modelli cloud, distribuzioni, organizzazioni e progetti. Contengono inoltre informazioni sulle distribuzioni che possono essere ottimizzate, in base al proprietario contattato da un'azione intrapresa nella scheda **Dettagli** della zona cloud. Vedere [Come utilizzare il dashboard Dettagli per monitorare la capacità delle risorse e informare i proprietari dei progetti in vRealize Automation](#).

I dettagli dell'avviso per ogni distribuzione includono:

- Nome progetto
- Nome della distribuzione (e collegamento alla distribuzione) contenente risorse che possono essere ottimizzate
- Azioni suggerite
- Potenziali risparmi sui costi da recupero ed ottimizzazione
- Numero totale di CPU virtuali utilizzate dalla distribuzione
- Quantità totale di memoria RAM utilizzata dalla distribuzione
- Quantità totale di storage utilizzato dalla distribuzione
- Macchine virtuali nella distribuzione consigliate per il recupero e l'ottimizzazione, inclusi il nome delle risorse, le macchine inattive, le macchine spente, le macchine sovradimensionate e sottodimensionate, le macchine sottoutilizzate e gli snapshot delle macchine

Utilizzando l'opzione **Contatta proprietari del progetto** nel dashboard Dettagli della zona cloud, è possibile visualizzare un riepilogo di tutti i progetti che hanno capacità recuperabile (CPU, memoria e storage) nella zona cloud e fornire un avviso per alcuni o tutti i proprietari del progetto.



Procedura

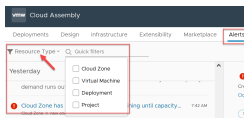
È possibile visualizzare le informazioni sulle soglie degli avvisi relativi alle risorse gestite utilizzando le opzioni di filtro nella pagina **Avvisi**. I dati degli avvisi sono forniti dall'applicazione vRealize Operations Manager associata. Le azioni suggerite vengono fornite per ogni avviso.

È inoltre possibile selezionare una distribuzione dalla sezione **Distribuzioni da esaminare** per aprire e ottimizzare la distribuzione. Vedere [Come utilizzare gli avvisi per ottimizzare le distribuzioni in vRealize Automation](#).

- 1 Dall'interno del servizio Cloud Assembly, fare clic sulla scheda **Avvisi** nel menu principale.

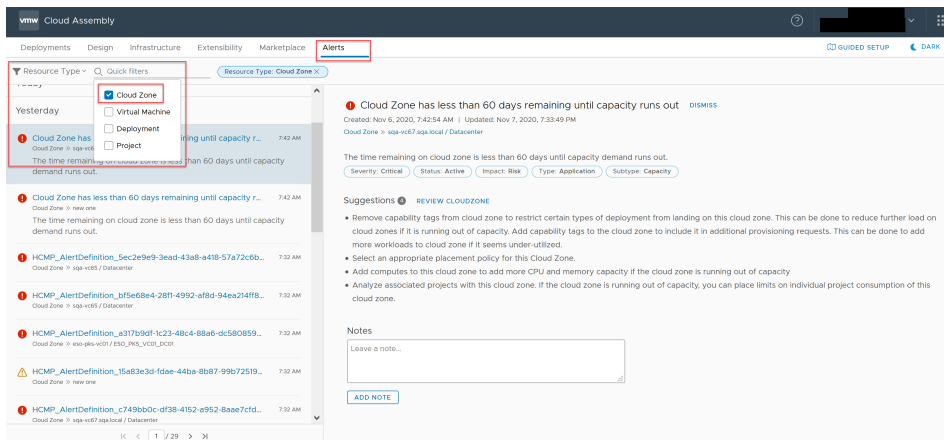


- 2 Per controllare il modo in cui vengono visualizzati gli avvisi, sperimentare con i filtri disponibili. Selezionare ad esempio l'opzione **Risorse** dal menu a discesa dei filtri.



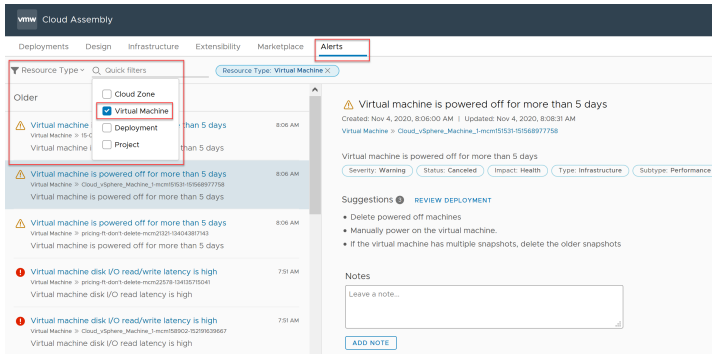
- 3 Per visualizzare gli avvisi e le azioni suggerite per tali avvisi, utilizzare le opzioni di filtro rapido nel pannello del selettore.

- Visualizzare gli avvisi relativi alle risorse della zona cloud.



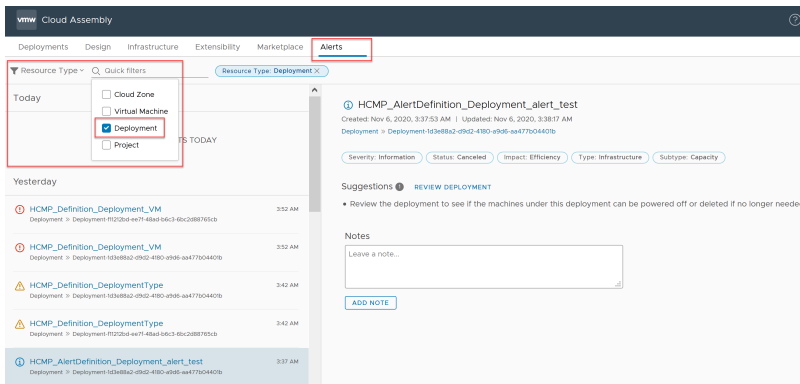
vRealize Operations Manager è in grado di monitorare tempo rimanente, capacità residua, capacità recuperabile e così via.

- Visualizzare gli avvisi relativi alle risorse della macchina virtuale.



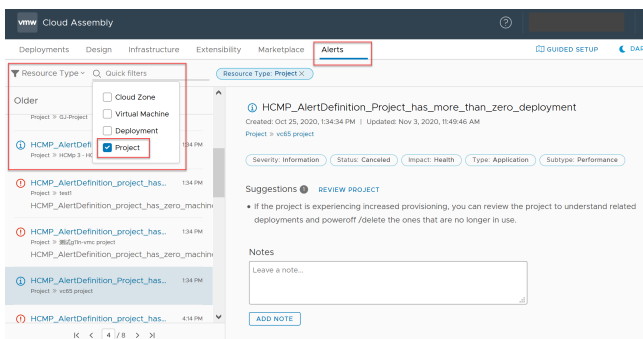
La maggior parte degli avvisi della macchina virtuale riguarda lo stato accesa/spenta, la latenza e così via.

- Visualizzare gli avvisi relativi alle risorse di distribuzione.



Gli avvisi di distribuzione riguardano le risorse recuperabili e il giusto dimensionamento.

- Visualizzare gli avvisi relativi alle risorse del progetto.



Gli avvisi del progetto riguardano le risorse recuperabili e i limiti di allocazione.

- 4 Esplorare gli altri tipi di filtro e le relative opzioni di filtro rapido per controllare ulteriormente l'elenco degli avvisi.
 - Utilizzare i filtri rapidi Integrità, Rischio ed Efficienza della sezione **Impatto**.
 - Utilizzare i filtri rapidi Critico, Immediato, Avviso e Informazioni della sezione **Gravità**.
 - Utilizzare i filtri rapidi Attivo, Annullato e Ignorato della sezione **Stato**.
 - Utilizzare i filtri Disponibilità, Prestazioni e Capacità della sezione **Sottotipo**.
 - Utilizzare i filtri rapidi Applicazione, Hardware, Infrastruttura, Storage e Rete della sezione **Tipo**.
- 5 Eseguire le azioni necessarie in base ai dati degli avvisi e ai suggerimenti.

Passaggi successivi

Per ulteriori informazioni sulle altre azioni disponibili, vedere [Come utilizzare gli avvisi per ottimizzare le distribuzioni in vRealize Automation](#).

È inoltre possibile visualizzare i **Dettagli** delle capacità per le risorse basate sulla zona cloud nei progetti gestiti. Per informazioni sull'utilizzo dei dati dei **Dettagli** forniti da vRealize Operations Manager in vRealize Automation, vedere [Come utilizzare il dashboard Dettagli per monitorare la capacità delle risorse e informare i proprietari dei progetti in vRealize Automation](#).

Come utilizzare gli avvisi per ottimizzare le distribuzioni in vRealize Automation

L'amministratore del cloud o il proprietario del progetto può monitorare e gestire le risorse della macchina per ottenere la migliore ottimizzazione possibile utilizzando i dati ottenuti da vRealize Operations Manager e visualizzati in vRealize Automation.

Quando si connette vRealize Automation a vRealize Operations Manager, è possibile accedere a informazioni raccolte dai dati sulle risorse dei progetti che si gestiscono. Avvisi e dettagli vengono forniti per informare di vari problemi relativi ai progetti che si gestiscono e consentono di comunicare facilmente suggerimenti sull'ottimizzazione e dati di supporto raccolti da vRealize Operations Manager ai proprietari dei progetti in modo semplice ed efficiente, senza mai dover uscire dall'applicazione vRealize Automation. Ad esempio, è possibile visualizzare la capacità delle risorse recuperabili, con risparmi sui costi specifici per ogni distribuzione in una zona cloud. Quando una zona cloud contiene più distribuzioni che possono essere ottimizzate, è possibile informare alcuni o tutti i proprietari del progetto e della distribuzione.

Gli avvisi di ottimizzazione delle distribuzioni possono essere generati dal dashboard Dettagli. Vedere [Come utilizzare il dashboard Dettagli per monitorare la capacità delle risorse e informare i proprietari dei progetti in vRealize Automation](#). È possibile contattare i proprietari del progetto affinché possano aprire una distribuzione denominata da ottimizzare da un collegamento fornito

nella pagina **Avvisi**. Anche i proprietari dei progetti possono aprire direttamente le proprie distribuzioni e utilizzare la scheda **Ottimizza** per eseguire le attività di ottimizzazione disponibili. Le azioni che il proprietario di un progetto può eseguire includono il recupero delle risorse eliminando le distribuzioni non critiche e interrompendo il provisioning in una zona cloud.

Nota Per ulteriori informazioni sulle altre azioni di correzione delle risorse che è possibile eseguire, vedere [Come utilizzare Avvisi per gestire capacità, prestazioni e disponibilità delle risorse in vRealize Automation](#).

Prerequisiti

Vedere [Come utilizzare Avvisi per gestire capacità, prestazioni e disponibilità delle risorse in vRealize Automation](#) per le credenziali necessarie e le informazioni di configurazione per accedere ai dati di vRealize Operations Manager in vRealize Automation.

Per richiedere che i proprietari dei progetti vengano avvisati dell'esistenza di distribuzioni ottimizzabili, vedere [Come utilizzare il dashboard Dettagli per monitorare la capacità delle risorse e informare i proprietari dei progetti in vRealize Automation](#).

Informazioni disponibili

Ogni distribuzione contiene una scheda **Ottimizza**. Sono disponibili i seguenti parametri di ottimizzazione:

- Macchine che possono essere razionalizzate: visualizza informazioni e azioni per le macchine sovradimensionate e sottodimensionate nella distribuzione, insieme al risparmio che è possibile ottenere con l'ottimizzazione.
- Macchine sottoutilizzate: visualizza informazioni e azioni per le macchine inattive o spente nella distribuzione, insieme al risparmio che è possibile ottenere con l'ottimizzazione.
- Snapshot di macchine: visualizza informazioni e azioni per gli snapshot delle macchine se le macchine nella distribuzione contengono snapshot, insieme al risparmio che è possibile ottenere con l'ottimizzazione.

In qualità di amministratore, è possibile informare i proprietari dei progetti della presenza di distribuzioni ottimizzabili. Le notifiche vengono visualizzate nella scheda **Avvisi** in Cloud Assembly.

La scheda **Avvisi** è disponibile solo se è configurato l'accesso a vRealize Operations Manager. I proprietari del progetto possono aprire e ottimizzare le proprie distribuzioni per rispondere agli avvisi.

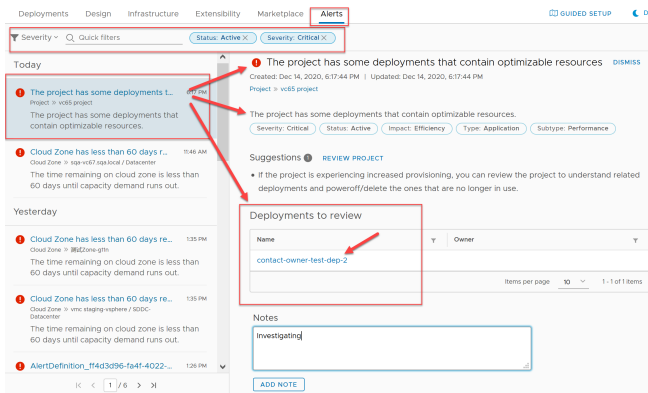
Procedura

È possibile visualizzare le informazioni sulle soglie degli avvisi relativi alle risorse gestite utilizzando le opzioni di filtro nella pagina **Avvisi**. I dati degli avvisi sono forniti dall'applicazione vRealize Operations Manager associata. Le azioni suggerite vengono fornite per ogni avviso. In questo esempio, il proprietario del progetto apre la propria distribuzione da un collegamento fornito in una notifica di avviso. La scheda **Ottimizza** della distribuzione visualizza i parametri della macchina disponibili per l'ottimizzazione.

- 1 In qualità di proprietario del progetto o amministratore, fare clic sulla scheda **Avvisi** nel menu principale.



- 2 Individuare un avviso che contenga informazioni su una distribuzione ottimizzabile e fare clic sul nome della distribuzione in **Distribuzioni da esaminare** per aprire la distribuzione e visualizzare la relativa scheda **Ottimizza**.



- 3 Quando la distribuzione viene aperta, fare clic sulla scheda **Ottimizza**.



- 4 Se sono presenti macchine sottoutilizzate, esaminare i dati e intervenire sulle macchine inattive e spente. Una distribuzione sottodimensionata può essere spenta o eliminata.
- 5 Se sono presenti macchine che possono essere razionalizzate, esaminare i dati e intervenire su qualsiasi macchina sovradimensionata o sottodimensionata nella distribuzione.
- 6 Se una o più macchine della distribuzione contengono uno snapshot, è possibile eliminare o esportare ogni snapshot.
- 7 Al termine del processo, verificare che la distribuzione sia stata ottimizzata come desiderato e chiudere la distribuzione.

Passaggi successivi

Per ulteriori informazioni sulle altre azioni disponibili, vedere [Come utilizzare Avvisi per gestire capacità, prestazioni e disponibilità delle risorse in vRealize Automation](#).

È inoltre possibile visualizzare i **Dettagli** delle capacità per le risorse basate sulla zona cloud nei progetti gestiti. Per informazioni sull'utilizzo dei dati dei **Dettagli** forniti da vRealize Operations Manager in vRealize Automation, vedere [Come utilizzare il dashboard Dettagli per monitorare la capacità delle risorse e informare i proprietari dei progetti in vRealize Automation](#).

Cosa è possibile fare con lo storage su disco standard in vRealize Automation

I dischi standard possono essere persistenti o non persistenti.

vRealize Automation supporta due categorie di storage: disco standard e FCD (First Class Disk). First Class Disk è disponibile solo per vSphere.

■ vSphere

vSphere supporta dischi standard dipendenti (predefiniti), persistenti indipendenti e non persistenti indipendenti. Per informazioni correlate, vedere [Cosa è possibile fare con lo storage su disco persistente in vRealize Automation](#).

Quando si elimina una macchina virtuale vengono eliminati anche i relativi dischi dipendenti e non persistenti indipendenti.

Quando si elimina una macchina virtuale, i suoi dischi persistenti indipendenti non vengono eliminati.

È possibile creare uno snapshot di dischi dipendenti e non persistenti indipendenti. Non è possibile creare uno snapshot di un disco persistente indipendente.

■ EBS di Amazon Web Services (AWS)

È possibile collegare un volume EBS a un'istanza di elaborazione AWS oppure scollegare un volume EBS da un'istanza di elaborazione AWS.

Quando si elimina una macchina virtuale, il relativo volume EBS collegato viene scollegato ma non eliminato.

■ VHD di Microsoft Azure

I dischi collegati sono sempre persistenti.

Quando si elimina una macchina virtuale, è possibile specificare se rimuovere i relativi dischi di storage collegati.

■ Google Cloud Platform (GCP)

I dischi collegati sono sempre persistenti.

I dischi persistenti sono posizionati in maniera indipendente dalle istanze della macchina virtuale, in modo da poter scollegare o spostare i dischi persistenti per conservare i dati anche dopo l'eliminazione delle istanze.

Quando si elimina una macchina virtuale, il relativo disco collegato viene scollegato ma non eliminato.

Per informazioni correlate, vedere [Ulteriori informazioni sui profili di storage in vRealize Automation](#).

Cosa è possibile fare con lo storage su disco persistente in vRealize Automation

I dischi persistenti consentono di eliminare accidentalmente dati preziosi.

In un modello cloud, in un volume, è possibile aggiungere la proprietà `persistent: true` affinché il disco venga preservato in seguito alle eliminazioni di Cloud Assembly o Service Broker. I dischi persistenti non vengono rimossi durante l'eliminazione della distribuzione né durante le operazioni giorno 2 di eliminazione o rimozione del disco.

Per questo motivo, i dischi persistenti possono rimanere nell'infrastruttura anche dopo l'eliminazione di una distribuzione o l'eliminazione del disco. Per rimuoverli, è possibile utilizzare le tecniche seguenti.

- Trasmettere esplicitamente il contrassegno purge come parametro di query utilizzando l'API DELETE.
- Eliminarli direttamente dall'endpoint cloud.

Si noti che non sono disponibili interfacce utente di Cloud Assembly o Service Broker per rimuoverli.

Cosa è possibile fare con lo storage FCD (First Class Disk) in vRealize Automation

Un First Class Disk (FCD) fornisce la gestione del ciclo di vita dello storage su dischi virtuali come Disk-as-a-Service o come storage su disco simile a EBS, permettendo di creare e gestire dischi indipendentemente dalle macchine virtuali di vSphere.

vRealize Automation supporta due categorie di dischi di storage: disco standard e FCD (First Class Disk). La funzionalità First Class Disk è supportata solo per vSphere. vRealize Automation attualmente offre la funzionalità First Class Disk solo tramite API.

Un First Class Disk dispone di funzioni per la gestione del ciclo di vita che operano in modo indipendente da una macchina virtuale. Una delle differenze tra un First Class Disk e un disco persistente indipendente consiste nella possibilità di utilizzare un First Class Disk per creare e gestire snapshot indipendenti da una macchina virtuale.

È possibile creare un nuovo profilo di storage di vRealize Automation per supportare le funzionalità di First Class Disk o disco standard. Vedere [Ulteriori informazioni sui profili di storage in vRealize Automation](#) e [Risorse di storage in vRealize Automation](#).

È inoltre possibile aggiungere un elemento `First Class Disk Cloud.vSphere.Disk` nei modelli cloud e nelle distribuzioni di vRealize Automation per supportare First Class Disk di vSphere. I First Class Disk di cui sono stati raccolti i dati vengono pagina **Risorse > Risorse > Volumi**.

In vCenter, i First Class Disk vengono denominati anche *IVD (Improved Virtual Disk)* o *dischi virtuali gestiti*.

Funzionalità

Utilizzando funzionalità API di vRealize Automation è possibile:

- Creare, elencare ed eliminare un First Class Disk.
- Ridimensionare un First Class Disk.
- Collegare e scollegare un First Class Disk.
- Creare e gestire snapshot di First Class Disk.
- Convertire un disco standard esistente in un First Class Disk.

Gli scenari seguenti non sono supportati:

- Provisioning delle macchine virtuali da snapshot in un cluster di datastore.
- Proprietà e condivisione di blocchi di storage basati su dispositivo per utenti e tenant.
- Creazione e ripristino degli snapshot della macchina virtuale.
- Collegamento dello storage in più macchine virtuali e cluster.

Le relative informazioni sull'API correlate alla creazione e alla gestione dello storage First Class Disk (FCD) utilizzando l'API di vRealize Automation, incluso come definire un profilo di storage per utilizzare le funzionalità First Class Disk, sono disponibili all'indirizzo code.vmware.com nella pagina [What are the vRealize Automation Cloud APIs and how do I use them](#) o navigando dalle seguenti posizioni:

- La documentazione sull'API correlata a FCD è disponibile nella sezione [First Class Disk \(FCD\)](#) della [guida alla programmazione di Virtual Disk Development Kit](#).
- I collegamenti alla documentazione del caso d'uso dell'API per FCD in vRealize Automation sono disponibili nella pagina della [documentazione dell'API di vRealize Automation](#) corrispondente alla versione di vRealize Automation in uso.

Considerazioni e limitazioni

Al momento, le considerazioni e le limitazioni di First Class Disk sono le seguenti:

- First Class Disk è disponibile solo per macchine virtuali vSphere.
- Per utilizzare i First Class Disk è necessario vSphere 6.7 aggiornamento 2 o versioni successive.
- Il provisioning di FCD (First Class Disk) nei cluster di datastore non è supportato.
- Il collegamento multiplo dei volumi non è supportato per i First Class Disk.
- I First Class Disk con snapshot non possono essere ridimensionati.
- I First Class Disk con snapshot non possono essere eliminati.

- La gerarchia di snapshot dei First Class Disk può essere costruita solo utilizzando l'opzione API `createdAt`.
- La versione minima dell'hardware della macchina virtuale necessaria per collegare un First Class Disk è vmx-13 (compatibile con ESX 6.5).

Configurazione delle risorse tenant multi-provider con vRealize Automation

Negli ambienti con più tenancy, i clienti possono gestire l'allocazione delle risorse in base al tenant utilizzando le zone private virtuali (VPZ, Virtual Private Zone).

In vRealize Automation 8.x, i clienti possono configurare ambienti multi-tenancy utilizzando VMware Lifecycle Manager e Workspace ONE Access. Questi strumenti permettono agli utenti di configurare la multi-tenancy e creare e configurare i tenant. Dopo aver configurato i tenant, gli amministratori del provider possono creare zone private virtuali in Cloud Assembly e quindi possono assegnare zone ai tenant utilizzando la funzionalità Cloud Assembly Gestisci tenant.

La multi-tenancy si basa sulla coordinazione e sulla configurazione di tre diversi prodotti VMware, come indicato di seguito:

- Workspace ONE Access: questo prodotto fornisce il supporto dell'infrastruttura per la multi-tenancy e le connessioni al dominio di Active Directory che forniscono la gestione di utenti e gruppi all'interno delle organizzazioni tenant.
- vRealize Suite Lifecycle Manager: questo prodotto supporta la creazione e la configurazione dei tenant per i prodotti supportati, ad esempio vRealize Automation. Inoltre, fornisce alcune funzionalità di gestione dei certificati.
- vRealize Automation: i provider e gli utenti accedono a vRealize Automation per accedere ai tenant in cui creano e gestiscono le distribuzioni.

Quando si configura la multi-tenancy, gli utenti devono avere familiarità con tutti i tre prodotti e la documentazione associata.

Per ulteriori informazioni sull'utilizzo di vRealize Suite Lifecycle Manager e Workspace ONE Access, vedere quanto segue.

Come creare una zona privata virtuale per vRealize Automation

Gli amministratori del provider possono creare una zona privata virtuale (VPZ, Virtual Private Zone) per allocare le risorse dell'infrastruttura ai tenant in un ambiente di vRealize Automation con più organizzazioni. Gli amministratori possono inoltre utilizzare le VPZ per controllare l'allocazione delle risorse nelle distribuzioni con tenant singolo.

È possibile utilizzare le zone private virtuali per allocare risorse come immagini, reti e risorse di storage. Le VPZ funzionano in modo ottimale come zona cloud per singolo tenant, ma sono progettate specificamente per l'utilizzo con distribuzioni con più tenant. Per qualsiasi progetto, è possibile utilizzare le zone cloud o le VPZ, ma non entrambe. Inoltre esiste una relazione uno a uno tra VPZ e tenant. Ad esempio, una VPZ può essere assegnata a un solo tenant alla volta.

Nota È possibile configurare mappature delle immagini e caratteristiche per una VPZ nella pagina Gestione tenant.

È possibile creare una VPZ con o senza NSX. Se si crea una zona senza NSX, vi sono limiti relativi alle funzionalità correlate a NSX negli endpoint vSphere.

- Sicurezza (gruppi, firewall)
- Componenti di rete (NAT)

Prerequisiti

- Abilitare e configurare la multi-tenancy nella distribuzione di vRealize Automation utilizzando VMware Lifecycle Manager e VMware Workspace ONE Access.
- Creare gli amministratori tenant in base alle esigenze della configurazione del tenant.
- Se si desidera utilizzare NSX, è necessario creare un account cloud NSX appropriato nell'organizzazione del provider.

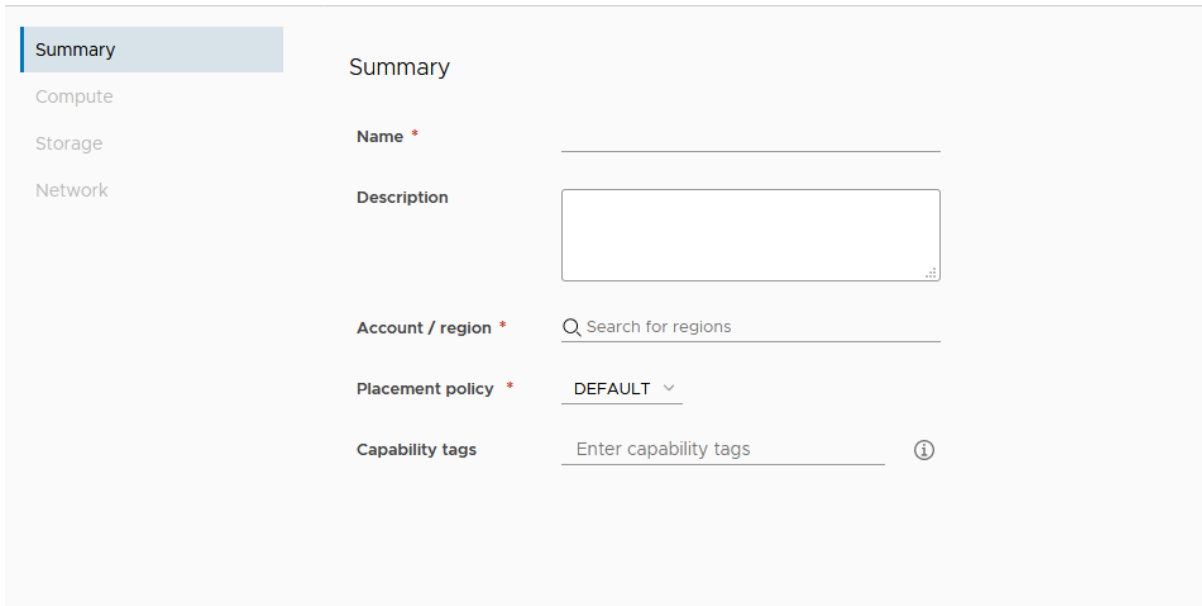
Procedura

- 1 Selezionare **Infrastruttura > Configura > Zone private virtuali**

La pagina della VPZ mostra tutte le zone esistenti e consente di creare zone.

2 Fare clic su **Nuova zona privata virtuale**.

New Virtual Private Zone



Nella parte sinistra della pagina sono presenti quattro selezioni che è possibile utilizzare per configurare le informazioni di riepilogo e i componenti dell'infrastruttura per la zona.

3 Immettere le informazioni di riepilogo per la nuova zona.

- a Aggiungere un nome e una descrizione.
- b Selezionare un account a cui applicare la zona.
- c Selezionare il criterio di posizionamento.

Il criterio di posizionamento determina la selezione dell'host per le distribuzioni all'interno della zona cloud specificata.

- **Default:** distribuisce le risorse di elaborazione tra i cluster e gli host in modo casuale. Questa selezione funziona a livello di singola macchina. Ad esempio, tutte le macchine in una distribuzione specifica vengono distribuite casualmente tra i cluster e gli host disponibili che soddisfano i requisiti.
- **binpack:** inserisce le risorse di elaborazione nell'host più carico che dispone di risorse sufficienti per eseguire la risorsa di elaborazione specificata.
- **spread:** esegue il provisioning delle risorse di elaborazione della distribuzione nel cluster o nell'host con il minor numero di macchine virtuali. Per vSphere, Distributed Resource Scheduler (DRS) distribuisce le macchine virtuali tra gli host. Ad esempio, tutte le macchine richieste in una distribuzione vengono posizionate nello stesso cluster, ma la distribuzione successiva potrebbe selezionare un altro cluster vSphere in base al carico corrente.

4 Selezionare la risorsa di elaborazione per la zona.

Aggiungere risorse di elaborazione appropriate per la zona cloud. Inizialmente la selezione del filtro è Includi elaborazione completa. L'elenco seguente mostra tutte le risorse di elaborazione disponibili, che sono allocate alla zona applicabile. Sono disponibili altre due opzioni per aggiungere risorse di elaborazione a una zona cloud.

- Seleziona manualmente elaborazione: selezionare questa voce di menu se si desidera selezionare le risorse di elaborazione manualmente nell'elenco che segue. Dopo averle selezionate, fare clic su **Aggiungi elaborazione** per aggiungere le risorse alla zona.
- Includi dinamicamente elaborazione in base ai tag: selezionare questa voce di menu per scegliere la risorsa di elaborazione da aggiungere alla zona in base ai tag. Tutte le risorse di elaborazione vengono visualizzate finché non vengono aggiunti tag appropriati. È possibile selezionare o immettere uno o più tag nell'opzione Includi elaborazione con questi tag.

Per entrambe le selezioni di elaborazione, è possibile rimuovere una o più risorse di elaborazione incluse nella pagina selezionando la casella di controllo alla loro destra e facendo clic su **Rimuovi**.

5 Immettere o selezionare i tag nel modo appropriato.

6 Selezionare Storage nel menu a sinistra e scegliere il criterio di storage e le altre configurazioni di storage per la zona.

7 Nel menu a sinistra, selezionare Rete e definire le reti e, facoltativamente, un criterio di rete da utilizzare con questa zona. È inoltre possibile configurare bilanciamenti del carico e gruppi di sicurezza per i criteri di rete selezionati.

Rete	<ul style="list-style-type: none"> ■ Tutte le reti esistenti associate a questa VPZ vengono visualizzate nella tabella della scheda Reti. ■ Fare clic su Aggiungi rete per visualizzare tutte le reti associate alla regione selezionata. Aggiungere una rete da utilizzare con questa zona. ■ Selezionare una rete e fare clic su Tag per aggiungere uno o più tag alla rete specificata. ■ Selezionare Gestisci intervalli IP per specificare l'intervallo di indirizzi IP tramite cui gli utenti possono accedere a questa rete. ■ Se applicabile, fare clic sulla scheda Criteri di rete e selezionare un criterio di isolamento.
Criteri di rete	<p>Se sono configurati, selezionare un criterio di rete da utilizzare con questa zona per applicare un criterio di isolamento per le reti in uscita e private.</p> <ul style="list-style-type: none"> ■ Selezionare un criterio di isolamento, se lo si desidera. ■ Selezionare un router logico di livello 0 e un cluster edge, se lo si desidera.

Bilanciamenti del carico	Fare clic su Aggiungi bilanciamento del carico per configurare i bilanciamenti del carico per gli account cloud della regione o dell'account.
Gruppi di sicurezza	Fare clic su Aggiungi gruppo di sicurezza per utilizzare i gruppi di sicurezza per applicare regole del firewall alle macchine di cui è stato eseguito il provisioning.

Risultati

La zona privata virtuale viene creata con le allocazioni di risorse specificate.

Operazioni successive

Gli amministratori del cloud possono associare la VPZ a un progetto.

- 1 In Cloud Assembly, selezionare **Amministrazione > Progetti**
- 2 Selezionare la scheda Provisioning.
- 3 Fare clic su **Aggiungi zona** e scegliere Aggiungi zona privata virtuale.
- 4 Selezionare la VPZ desiderata nell'elenco.
- 5 È possibile impostare la priorità di provisioning e limitare il numero di istanze, la quantità di memoria disponibile e il numero di CPU disponibili.
- 6 Fare clic su **Aggiungi**.

Gestione delle zone private virtuali per i tenant di vRealize Automation

Gli amministratori del provider possono gestire le zone private virtuali (VPZ) in Cloud Assembly per controllare l'allocazione delle risorse dell'infrastruttura in base al tenant. Utilizzando la pagina Gestione tenant, gli amministratori possono visualizzare i tenant e le zone VPZ e abilitare o disabilitare le VPZ per i tenant.

Per impostazione predefinita, le zone private virtuali non vengono allocate ad alcun tenant. È necessario allocare le VPZ in questa pagina per usarle con i tenant.

Quando vengono create inizialmente, le VPZ sono abilitate per impostazione predefinita. Una VPZ abilitata è pronta per essere allocata e utilizzata con il tenant specificato. Quando le VPZ sono disabilitate, non possono essere utilizzate per il provisioning o allocate a un tenant. Una VPZ può essere disabilitata ma comunque allocata per un tenant.

Quando un amministratore del provider passa alla pagina Gestione tenant, nella pagina vengono visualizzati tutti i tenant disponibili e l'amministratore può selezionarne uno. Dopo la selezione del tenant, nella pagina vengono visualizzate le VPZ attualmente allocate per tale tenant, se presenti. L'amministratore può utilizzare questa pagina per allocare le VPZ al tenant selezionato.

Quando una VPZ è allocata, gli amministratori dei tenant possono aggiungerla ai loro progetti. La VPZ diventa così disponibile per il provisioning da parte degli utenti del tenant. Dopo l'allocazione a un tenant, una VPZ può essere allocata a un altro tenant.

Dopo l'abilitazione, una VPZ è pronta per l'uso nel tenant specificato. Gli amministratori del provider possono disabilitare le VPZ per semplificare la manutenzione o la riconfigurazione del tenant e possono inviare agli utenti una notifica per informarli della disabilitazione. Se si desidera che una VPZ non sia disponibile in un tenant in modo più permanente, è possibile annullarne l'allocazione. Se l'allocazione di una VPZ esistente viene annullata da un tenant per qualche motivo, la VPZ non può essere utilizzata per creare distribuzioni da tale tenant.

Prerequisiti

- Configurare la multi-tenancy e creare le zone private virtuali appropriate per la distribuzione.
- Configurare le mappature delle immagini e caratteristiche globali per la configurazione di VPZ e tenant utilizzando le selezioni del menu della mappatura delle immagini e caratteristiche sul lato sinistro della pagina Gestione tenant in Cloud Assembly. Vedere [Creazione di mappature delle immagini e caratteristiche per i tenant di vRealize Automation](#).

È possibile sovrascrivere queste assegnazioni globali ora o successivamente utilizzando le selezioni delle mappature delle immagini e caratteristiche specifiche del tenant nella parte superiore della pagina Gestione tenant. Vedere [Configurazione delle mappature di immagini e caratteristiche specifiche del tenant per vRealize Automation](#).

Procedura

- 1 In Cloud Assembly selezionare Gestisci tenant.

La pagina Gestione tenant mostra tutti i tenant configurati per l'organizzazione dell'amministratore in una vista scheda.

- 2 Fare clic su un tenant per selezionarlo.
- 3 Fare clic sulla scheda Gestione infrastruttura per visualizzare tutte le VPZ allocate per il tenant.
- 4 Selezionare **Alloca zona privata virtuale** per aprire una finestra di dialogo che includa tutte le zone non attualmente allocate ai tenant. Allocare la zona a un tenant.
- 5 Selezionare una o più zone nella finestra di dialogo e fare clic su **Alloca al tenant**.

Operazioni successive

Dopo l'allocazione delle VPZ, gli amministratori dei tenant possono assegnarle ai progetti.

Gli amministratori del provider possono utilizzare la vista scheda dei tenant per monitorare e gestire lo stato delle VPZ.

- Se si desidera disabilitare un tenant, fare clic su **Disabilita** nella scheda del tenant.
- Per abilitare un tenant, fare clic su **Abilita** nella scheda del tenant.
- Se si desidera annullare l'allocazione di un tenant, fare clic su **Dealloca** nella scheda di tale tenant.

Creazione di mappature delle immagini e caratteristiche per i tenant di vRealize Automation

Gli amministratori del provider possono selezionare o creare mappature delle immagini e caratteristiche globali che possono essere assegnate ai tenant di vRealize Automation.

La mappatura delle immagini e caratteristiche globale consente di impostare rapidamente mappature applicabili a più tenant. È inoltre possibile aggiornare rapidamente queste mappature. La pagina Gestione tenant consente inoltre di creare mappature delle immagini e caratteristiche specifiche del tenant che possono sovrascrivere le configurazioni predefinite.

Nota Le mappature delle immagini e caratteristiche configurate nella pagina Gestione tenant si applicano solo ai tenant così come configurati e non all'organizzazione del provider più ampia.

Prerequisiti

Procedura

- 1 In Cloud Assembly selezionare Gestisci tenant.

La pagina Gestione tenant mostra tutti i tenant configurati per l'organizzazione dell'amministratore in una vista scheda.

- 2 Selezionare Mappatura immagine nel menu a sinistra della pagina Gestione tenant.

La pagina Mappatura immagine mostra tutte le immagini attualmente configurate per i tenant in Cloud Assembly e indica se le mappature sono globali o associate a un tenant specifico.

Create Image Mapping

Account / region *

Q Search for regions

Image Name *

Image *

Q Search for images

Constraints

Example: !license:none:hard

Scope *

Q All tenants

Cloud Configuration

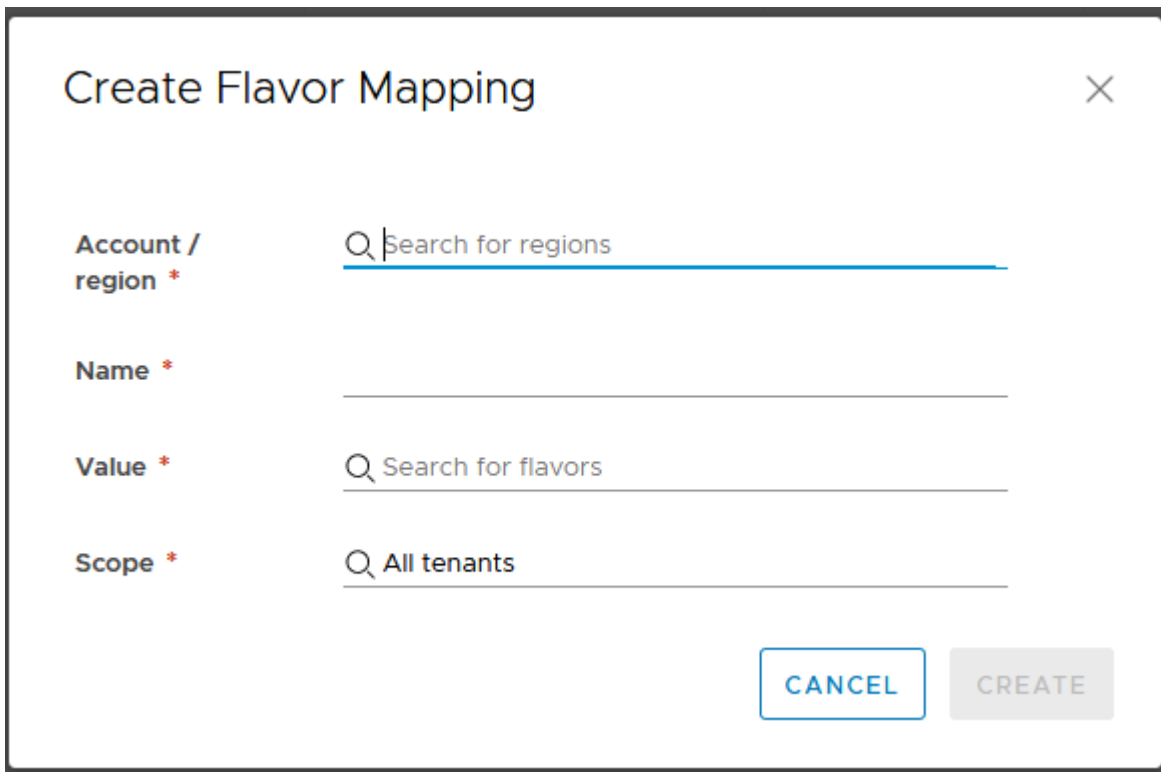
1	
---	--

CANCEL

CREATE

- 3 Selezionare **Aggiungi mappatura immagine** per aggiungere una mappatura immagine da utilizzare con i tenant.
 - a Selezionare l'account/regione a cui applicare la mappatura immagine.
 - b Immettere un nome per la mappatura immagine e selezionare l'istanza o la versione dell'immagine specifica a cui si riferisce.

- c Immettere i tag di vincolo desiderati.
 - d Selezionare l'ambito per la mappatura immagine. L'ambito può essere Tutti i tenant o Globale oppure è possibile selezionare un tenant specifico a cui applicare la mappatura immagine.
- 4 Se desiderato, è possibile utilizzare uno script di configurazione cloud per definire le caratteristiche del sistema operativo personalizzato per le distribuzioni.
- Ad esempio, a seconda che il modello cloud venga distribuito in un cloud pubblico o in un cloud privato, è possibile applicare all'immagine specifiche autorizzazioni dell'utente, autorizzazioni del sistema operativo o altre condizioni. Uno script di configurazione del cloud utilizza il formato `cloud-init` per le immagini basate su Linux o il formato `cloudbase-init` per le immagini basate su Windows. Vedere [Ulteriori informazioni sulle mappature dell'immagine in vRealize Automation](#) per ulteriori informazioni.
- 5 Fare clic **Crea** per creare la mappatura immagine.
- 6 Selezionare **Aggiungi mappatura caratteristica** per aggiungere una mappatura caratteristiche da utilizzare con i tenant.



The image shows a 'Create Flavor Mapping' dialog box with a close button (X) in the top right corner. It contains four input fields, each with a magnifying glass icon and a placeholder text:

- Account / region ***: Placeholder text is 'Search for regions'.
- Name ***: Placeholder text is empty.
- Value ***: Placeholder text is 'Search for flavors'.
- Scope ***: Placeholder text is 'All tenants'.

At the bottom right, there are two buttons: 'CANCEL' (outlined in blue) and 'CREATE' (grayed out).

- a Selezionare l'account/regione a cui verrà applicata la mappatura caratteristiche.
- b Immettere un nome per la mappatura caratteristiche che si sta creando.

- c Selezionare i parametri Dimensione per la mappatura caratteristiche che si sta creando.

È possibile specificare il numero di processori e la quantità di memoria per questa caratteristica.

- d Selezionare l'ambito per la mappatura caratteristiche. L'ambito può essere Tutti i tenant o Globale oppure è possibile selezionare un tenant specifico a cui applicare la mappatura caratteristiche. Tutti i tenant vale per tutti i tenant nell'organizzazione dell'amministratore del provider.

7 Fare clic **Crea** per creare la mappatura caratteristiche.

Risultati

Dopo aver creato le mappature globali, queste verranno visualizzate nelle schede Mappatura caratteristiche o Mappatura tenant nella pagina Gestione tenant per i tenant applicabili.

Operazioni successive

In questa pagina è possibile modificare o eliminare le mappature delle immagini e caratteristiche globali. Per modificare una mappatura, selezionarla e apportare le modifiche desiderate.

Configurazione delle mappature di immagini e caratteristiche specifiche del tenant per vRealize Automation

Cloud Assembly consente di configurare le mappature delle immagini e delle caratteristiche globali disponibili per tutte le zone private virtuali all'interno dell'organizzazione. In alternativa, è possibile sostituire le impostazioni globali e configurare mappature delle immagini e delle caratteristiche specifiche del tenant in base alle proprie distribuzioni.

In genere, un amministratore del cloud configura le mappature delle immagini e delle caratteristiche globali utilizzando i collegamenti di navigazione nella parte sinistra della pagina Gestione tenant. Queste mappature vengono applicate su scala aziendale per tutti i tenant. In alcuni casi, può essere necessario creare mappature delle immagini e delle caratteristiche personalizzate specifiche del tenant per determinati tenant e la pagina Gestione tenant supporta questa opzione.

La mappatura delle immagini e delle caratteristiche viene visualizzata nelle rispettive schede della pagina Gestione tenant. Fare clic su una delle mappature delle immagini e delle caratteristiche esistenti per modificarle. Per eliminare la mappatura di un'immagine o di una caratteristica, selezionare la mappatura e quindi fare clic su **Elimina**.

Prerequisiti

- Abilitare la multi-tenancy e configurare i tenant per la distribuzione.
- Creare le zone private virtuali appropriate.

Procedura

- 1** Selezionare Gestione tenant nel menu principale di Cloud Assembly.

- 2 Selezionare il tenant per cui si desidera configurare la mappatura personalizzata delle immagini o delle caratteristiche.
- 3 Selezionare il collegamento Mappatura immagine nella parte superiore della pagina, quindi fare clic su **Aggiungi mappatura immagine**.
Viene visualizzata la finestra di dialogo Crea mappatura immagine.
- 4 Assicurarsi che l'account o la regione specificati siano corretti e aggiungere un nome per la mappatura nella casella di testo **Nome immagine**.
- 5 Selezionare l'immagine della macchina sottostante da utilizzare nel menu a discesa **Immagine**.
- 6 Aggiungere tag di vincolo, se applicabili per l'utilizzo dell'immagine.
- 7 Selezionare l'**Ambito** appropriato per l'immagine.
 - Fare clic sul pulsante di opzione Disponibile solo per questo tenant se si desidera che la mappatura immagine possa essere utilizzata solo dal tenant selezionato.
 - Fare clic sul pulsante di opzione Condiviso tra tenant se si desidera che la mappatura immagine possa essere utilizzata da altri tenant.
- 8 Fare clic su **Crea** per salvare la mappatura immagine come è stata configurata.
- 9 Selezionare il collegamento Mappatura caratteristiche nella parte superiore della pagina e quindi fare clic su **Aggiungi mappatura caratteristica** per creare una mappatura caratteristica.
Viene visualizzata la finestra di dialogo Crea mappatura caratteristica.
- 10 Assicurarsi che l'account o la regione specificati siano corretti e aggiungere un nome per la mappatura nella casella di testo **Nome**.
- 11 Specificare le impostazioni relative a CPU e memoria nel campo **Valore**.
- 12 Selezionare l'**Ambito** appropriato per l'immagine.
 - Fare clic sul pulsante di opzione Disponibile solo per questo tenant se si desidera che la mappatura immagine possa essere utilizzata solo dal tenant selezionato.
 - Fare clic sul pulsante di opzione Condiviso tra tenant se si desidera che la mappatura immagine possa essere utilizzata da altri tenant.
- 13 Fare clic su **Crea** per salvare la mappatura caratteristiche come è stata configurata.

Risultati

Le mappature delle immagini e delle caratteristiche specifiche del tenant vengono configurate come specificato.

Creazione di sottoscrizioni di estendibilità per provider o tenant

Gli amministratori del provider e del tenant possono creare sottoscrizioni di estendibilità per accedere ai workflow di vRealize Orchestrator. I workflow di vRealize Orchestrator vengono attivati in base agli eventi, se è presente una sottoscrizione per alcuni argomenti di evento che corrisponde a una fase specifica del ciclo di vita dell'applicazione.

Le caratteristiche di una sottoscrizione di estendibilità variano a seconda che la sottoscrizione venga creata da un amministratore del provider o da un amministratore del tenant.

- L'amministratore del tenant può creare una sottoscrizione ma non può specificare l'ambito dell'organizzazione. Tale sottoscrizione verrà attivata solo per gli eventi attivati dal tenant.
- L'amministratore del provider può creare una sottoscrizione e specificare l'ambito del provider. La sottoscrizione si comporterà come una sottoscrizione tenant o un ambiente non multi-tenant. Verrà attivata in base agli eventi provenienti dal provider.
- Il provider può creare una sottoscrizione e specificare l'ambito del tenant. La sottoscrizione viene attivata in base agli eventi provenienti da qualsiasi tenant. Non viene attivata dagli eventi provenienti dal provider.

Le sottoscrizioni attivano i workflow di vRealize Orchestrator in base a eventi specifici. Non richiamano le azioni di estendibilità. Al momento è supportata una sola istanza di vRealize Orchestrator per ogni organizzazione del provider specifica. Per ulteriori informazioni su eventi, argomenti degli eventi e sottoscrizioni, vedere [Terminologia dell'estendibilità](#).

Prerequisiti

Configurare i tenant e le zone private virtuali nel modo appropriato per la propria distribuzione.

Procedura

1 In vRealize Automation, passare alla pagina Sottoscrizioni e fare clic su **Nuova sottoscrizione**.

2 Immettere un **nome** e una **descrizione** per la sottoscrizione.

3 Assicurarsi che il pulsante di opzione Abilita sottoscrizione sia attivato.

Se non si desidera che la sottoscrizione sia immediatamente attiva, è possibile lasciare il pulsante disattivato.

4 Se si è un amministratore del provider, selezionare l'**Ambito organizzazione** appropriato.

Le opzioni dell'ambito dell'organizzazione sono Provider e Tenant. Se si seleziona Tenant, l'ambito del progetto è costituito da tutti i progetti e non può essere modificato. Se si seleziona Provider, è possibile specificare l'ambito del progetto selezionandolo nella parte inferiore della pagina Sottoscrizioni.

5 Selezionare l'**Argomento dell'evento** a cui si desidera effettuare la sottoscrizione.

6 Selezionare uno o più workflow.

Risultati

I provider e i tenant possono visualizzare gli eventi restituiti per una distribuzione specifica nella pagina Eventi in Cloud Assembly. I risultati visualizzati dipendono dal proprio ruolo e dall'ambito dell'organizzazione.

- Se l'ambito dell'organizzazione è Provider, i provider visualizzeranno gli eventi in base alle loro azioni nella stessa organizzazione del provider.

- Se l'ambito dell'organizzazione è Tenant, i tenant potranno visualizzare gli eventi, mentre il provider non potrà visualizzarli. Gli eventi si trovano sempre nell'organizzazione dell'autore.
- 1 Selezionare **Estendibilità > Eventi** in Cloud Assembly.
 - 2 Nella casella Cerca della pagina Eventi, immettere l'ID distribuzione di cui si desidera visualizzare gli eventi.

Nella pagina vengono visualizzati gli eventi che corrispondono ai criteri di ricerca.

Utilizzo delle zone private virtuali legacy nelle versioni più recenti di vRealize Automation

Le opzioni di configurazione per le zone private virtuali sono cambiate in Cloud Assembly. È possibile aggiornare o utilizzare zone private virtuali legacy nelle versioni correnti di vRealize Automation.

In vRealize Automation 8.2 gli utenti configuravano le mappature di immagini e caratteristiche all'interno delle zone private virtuali. Nelle versioni più recenti di vRealize Automation, gli utenti creano mappature di immagini e caratteristiche in base al tenant, aumentando l'efficienza e la flessibilità di configurazione soprattutto nelle distribuzioni con un numero elevato di tenant. Sebbene non sia possibile eseguire la migrazione di zone private virtuali legacy create in vRealize Automation 8.2, sono disponibili diverse opzioni per utilizzarle con versioni più recenti di vRealize Automation.

La prima opzione, quella più flessibile, consiste nell'eliminare le mappature di immagini e caratteristiche legacy dalle zone private virtuali precedenti e riconfigurarle con nuove mappature create nella pagina Gestione tenant.

- 1 Selezionare **Infrastruttura > Configura > Zone private virtuali** per aprire la pagina VPZ.
- 2 Selezionare Mappatura immagine per visualizzare la mappatura esistente.
- 3 Selezionare le mappature e fare clic per eliminarle.
- 4 Selezionare Mappatura immagine per visualizzare la mappatura esistente.
- 5 Selezionare le mappature e fare clic per eliminarle.
- 6 Chiudere la pagina VPZ.
- 7 Selezionare Mappatura tenant e selezionare una mappatura globale per i tenant applicabili o creare una mappatura specifica del tenant.

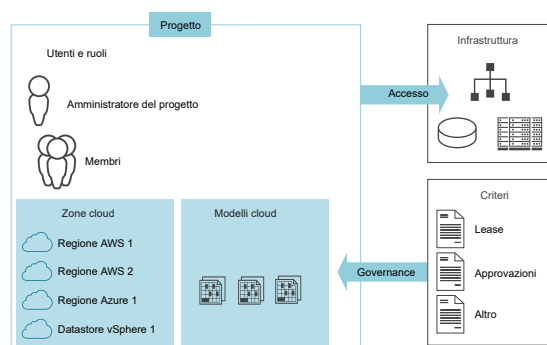
In alternativa, è possibile utilizzare le zone private virtuali legacy con versioni più recenti di vRA nella propria configurazione esistente. Le mappature di immagini e caratteristiche legacy continueranno a funzionare come configurate, ma le relative opzioni di configurazione verranno lette solo nella pagina VPZ. Questa opzione offre meno flessibilità rispetto alla prima opzione.

Aggiunta e gestione di progetti di Cloud Assembly

5

I progetti controllano chi può accedere ai modelli cloud di Cloud Assembly e la posizione di distribuzione dei modelli. È possibile utilizzare i progetti per organizzare e gestire le operazioni che gli utenti possono eseguire e le zone cloud in cui possono distribuire i modelli cloud nell'infrastruttura cloud.

Gli amministratori del cloud configurano i progetti ai quali possono aggiungere utenti e zone cloud. Tutti gli utenti che creano e distribuiscono modelli cloud devono essere membri di almeno un progetto.



Questo capitolo include i seguenti argomenti:

- [Come aggiungere un progetto per il team di sviluppo di Cloud Assembly](#)
- [Ulteriori informazioni sui progetti Cloud Assembly](#)

Come aggiungere un progetto per il team di sviluppo di Cloud Assembly

Si crea un progetto a cui si aggiungono membri e zone cloud in modo che i membri del progetto possano distribuire i propri modelli cloud nelle zone associate. L'amministratore di Cloud Assembly può creare un progetto per un team di sviluppo. Può quindi assegnare un amministratore del progetto oppure operare come amministratore del progetto.

Quando si crea un modello cloud, è necessario selezionare prima il progetto da associare a esso. Deve esistere un progetto prima che sia possibile creare il modello cloud.

Assicurarsi che i progetti supportino le esigenze aziendali del team di sviluppo.

- Il progetto deve fornire le risorse che supportano gli obiettivi del team. Per un esempio di come le risorse dell'infrastruttura e un progetto supportano un modello cloud, vedere [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).
- I membri del progetto richiedono o prevedono che le distribuzioni siano condivise o private. Le distribuzioni condivise sono disponibili per tutti i membri del progetto nella pagina Distribuzioni, non solo per il membro di distribuzione. È possibile modificare lo stato di condivisione della distribuzione in qualsiasi momento.

Quando si condivide la distribuzione con i membri del progetto, i membri possono eseguire la stessa azione giorno 2. Per gestire la capacità dei membri di eseguire le azioni giorno 2, è possibile creare i criteri del giorno 2 in Service Broker. I criteri si applicano alle distribuzioni di Cloud Assembly e Service Broker.

Per ulteriori informazioni sui criteri del giorno 2, vedere [Come autorizzare gli utenti della distribuzione alle azioni giorno 2 utilizzando i criteri](#).

Questa procedura si basa sulla creazione di un progetto iniziale che include solo le configurazioni di base. Poiché il team di sviluppo crea e distribuisce i propri modelli cloud, è possibile apportare modifiche nel progetto. È possibile aggiungere vincoli, proprietà personalizzate e altre opzioni per migliorare l'efficienza della distribuzione. Vedere gli articoli disponibili in [Ulteriori informazioni sui progetti Cloud Assembly](#).

Prerequisiti

- Verificare di aver configurato le zone cloud. Vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).
- Verificare di aver configurato le mappature e i profili per le regioni incluse come zone cloud per questo progetto. Vedere [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#).
- Verificare di disporre delle autorizzazioni necessarie per eseguire questa attività. Vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Determinare chi si sta designando come amministratore del progetto. Per capire quali operazioni può svolgere l'amministratore del progetto in Cloud Assembly, vedere [Che cosa sono i ruoli utente di vRealize Automation](#).
- Se si aggiungono gruppi di Active Directory ai progetti, verificare di aver configurato i gruppi di Active Directory per l'organizzazione. Vedere [Modifica delle assegnazioni dei ruoli di gruppo in vRealize Automation in Amministrazione di vRealize Automation](#). Se i gruppi non sono sincronizzati, non sono disponibili quando si tenta di aggiungerli a un progetto.

Procedura

- 1 Selezionare **Infrastruttura > Amministrazione > Progetti** e fare clic su **Nuovo progetto**.
- 2 Immettere il nome del progetto.

3 Fare clic sulla scheda Utenti.

- a Per rendere le distribuzioni dei membri del progetto accessibili solo per l'utente richiedente, disattivare **Condivisione della distribuzione**. Per assicurarsi che sia possibile assegnare la proprietà di una distribuzione a un altro membro del progetto, verificare che **Condivisione della distribuzione** sia attivata.
- b Aggiungere utenti con ruoli assegnati.

4 Fare clic sulla scheda Provisioning e aggiungere una o più zone cloud.

Aggiungere le zone cloud e le zone private virtuali che contengono le risorse che supportano i modelli cloud distribuiti dagli utenti del progetto.

Per ogni zona, è possibile impostare una priorità per la zona e limitare la quantità di risorse che il progetto può utilizzare. I limiti possibili includono il numero di istanze, memoria e CPU. Solo per le zone cloud di vSphere, è possibile configurare limiti di storage per le risorse distribuite basate sui modelli di macchine virtuali di vSphere. I limiti di storage vengono valutati in base alla richiesta di distribuzione e a quando si apportano modifiche tramite le azioni di ridimensionamento del disco, ridimensionamento del disco di avvio, rimozione del disco e aggiornamento del conteggio. Tali limiti di storage non si applicano ad altri tipi di risorse come AWS, Microsoft Azure o Google Cloud Platform.

Quando si aggiungono le zone e si applicano i limiti, non limitare le risorse del progetto al punto che i membri non possono distribuire i propri modelli cloud.

Quando gli utenti inviano una richiesta di distribuzione, le zone vengono valutate per determinare quali di esse dispongono delle risorse per supportare la distribuzione. Se più di una zona supporta la distribuzione, viene valutata la priorità e il carico di lavoro viene convogliato su quello con la priorità più alta, corrispondente al numero intero più basso.

5 Se la distribuzione dei carichi di lavoro necessari per questo progetto richiede più di due ore, immettere un valore più alto in Timeout.

Il valore predefinito è di due ore.

6 Fare clic su Crea.**7 Per eseguire il test del progetto con le zone cloud del progetto, fare clic su Prova configurazione nella pagina Progetti.**

La simulazione esegue un test di distribuzione ipotetico standardizzato delle risorse della zona cloud del progetto. Se non riesce, è possibile esaminare i dettagli e correggere la configurazione delle risorse.

Operazioni successive

Introduzione ai modelli cloud. Vedere [Capitolo 6 Progettazione delle distribuzioni di Cloud Assembly](#).

Ulteriori informazioni sui progetti Cloud Assembly

I progetti sono il collegamento tra modelli cloud e risorse. Più si comprende il loro funzionamento e utilizzo, più efficace sarà il processo di sviluppo e distribuzione di Cloud Assembly.

Utilizzo dei tag di progetto e delle proprietà personalizzate di Cloud Assembly

In qualità di amministratore, è possibile aggiungere vincoli di governance o proprietà personalizzate a livello di progetto quando i requisiti del progetto sono diversi da quelli dei modelli cloud di Cloud Assembly. Oltre ai tag di vincolo, è possibile aggiungere tag di risorse che vengono aggiunti alle risorse distribuite durante il processo di provisioning, in modo da poter gestire le risorse.

Che cosa sono i tag di risorse del progetto

Un tag di risorse del progetto funziona come un tag di identificazione standardizzato che è possibile utilizzare per gestire le risorse distribuite e garantire la conformità.

I tag di risorse definiti in un progetto vengono aggiunti a tutte le risorse dei componenti distribuite come parte di tale progetto. È quindi possibile utilizzare l'assegnazione di tag standard per gestire le risorse utilizzando altre applicazioni, ad esempio, per monitorare i costi utilizzando CloudHealth e, cosa importante, per garantire la conformità.

Ad esempio, in qualità di amministratore del cloud, si desidera utilizzare un'applicazione come CloudHealth per gestire i costi. È possibile aggiungere il tag `costCenter:eu-cc-1234` a un progetto dedicato allo sviluppo di uno strumento di risorse umane dell'Unione europea. Quando il team del progetto esegue la distribuzione da questo progetto, il tag viene aggiunto alle risorse distribuite. È quindi possibile configurare lo strumento dei costi per identificare e gestire le risorse che includono questo tag. Altri progetti con altri centri di costo avranno valori alternativi da passare con la chiave.

Che cosa sono i tag di vincolo del progetto

Un vincolo di progetto funziona come definizione di governance. Si tratta di un tag di `key:value` che definisce le risorse che la richiesta di distribuzione utilizza o evita nelle zone cloud del progetto.

Il processo di distribuzione cerca i tag delle reti e dello storage che corrispondono ai vincoli del progetto ed esegue la distribuzione in base ai tag corrispondenti.

Il vincolo di estendibilità viene utilizzato per specificare l'istanza integrata di vRealize Orchestrator da utilizzare per i workflow di estendibilità.

Quando si configurano i vincoli di progetto, tenere in considerazione i seguenti formati.

- **key:value** e **key:value:hard**. Utilizzare questo tag in uno dei formati quando il modello cloud deve essere sottoposto a provisioning sulle risorse con il tag di funzionalità corrispondente. Il processo di distribuzione non riesce quando non viene trovato alcun tag corrispondente.

Ad esempio, è necessario effettuare il provisioning di un modello cloud distribuito dai membri di un progetto su una rete conforme a PCI. Si utilizza `security:pci`. Se non viene trovata nessuna rete nelle zone cloud del progetto, la distribuzione non riesce e garantisce che non avvengano distribuzioni non sicure.

- **key:value:soft.** Utilizzare questo tag quando si preferisce una risorsa corrispondente, ma si desidera che il processo di distribuzione proceda senza errori e possa accettare risorse in cui il tag non corrisponde. Ad esempio, si preferisce che i membri del progetto distribuiscano i propri modelli cloud in uno storage meno costoso, ma si desidera che la disponibilità dello storage non interferisca con la loro capacità di distribuzione. Si utilizza `tier:silver:soft`. Se non è disponibile alcuno storage con tag `tier:silver` nelle zone cloud del progetto, il modello cloud viene comunque distribuito in altre risorse di storage.
- **!key:value.** Utilizzare questo tag, con applicazione permanente o temporanea, quando si desidera evitare la distribuzione alle risorse con un tag corrispondente.

È importante sottolineare che i tag di vincolo del progetto hanno una priorità più alta rispetto ai tag di vincolo del modello cloud e li sovrascrivono al momento della distribuzione. Se si dispone di un modello cloud in cui questa operazione non deve mai verificarsi, è possibile utilizzare `failOnConstraintMergeConflict:true` nel modello. Ad esempio, se il progetto ha un vincolo di rete `loc:london`, ma il modello cloud è `loc:mumbai`; tuttavia, per evitare che la posizione del progetto abbia la precedenza, si desidera che la distribuzione non riesca con un messaggio di conflitto di vincoli, aggiungendo una proprietà simile al seguente esempio.

```
constraints:
  - tag: 'loc:mumbai'
failOnConstraintMergeConflict:true
```

Come utilizzare le proprietà personalizzate del progetto

È possibile utilizzare una proprietà personalizzata del progetto per la creazione di report, per attivare e popolare le azioni di estendibilità e il workflow e per sovrascrivere le proprietà a livello del modello cloud.

L'aggiunta di una proprietà personalizzata a una distribuzione consente di utilizzare il valore nell'interfaccia utente o di recuperarla utilizzando l'API in modo da poter generare report.

L'estendibilità può inoltre utilizzare una proprietà personalizzata per una sottoscrizione di estendibilità. Per ulteriori informazioni sull'estendibilità, vedere [Estensione e automazione dei cicli di vita delle applicazioni con l'estendibilità](#).

Un modello cloud potrebbe avere un particolare valore di proprietà che si desidera modificare per un progetto. È possibile fornire un nome e un valore alternativi come proprietà personalizzata.

È inoltre possibile crittografare il valore della proprietà in modo che né l'utente corrente né gli altri utenti possano vedere il valore incluso nella distribuzione. È possibile ad esempio crittografare una password utilizzata da tutti gli utenti nel progetto, ma che si desidera non sia visibile. Dopo aver crittografato il valore e salvato il progetto, non sarà possibile rimuovere la maschera o sostituire il valore. Se si deseleziona la casella di controllo **Crittografato**, il valore verrà rimosso. Sarà necessario immettere nuovamente un valore.

In che modo i criteri di posizionamento a livello di progetto influiscono sull'allocazione delle risorse in vRealize Automation

In qualità di amministratore, è possibile definire il criterio di posizionamento per i progetti in cui più di una zona cloud è idonea come zona di destinazione della distribuzione. Ad esempio, si potrebbe avere un progetto in cui si desidera distribuire i modelli cloud in base alla priorità impostata. In alternativa, è possibile bilanciare le risorse distribuite in più zone in base a quale presenta il miglior rapporto tra macchine virtuali e host.

Considerazioni sull'allocazione

Per un criterio di posizionamento predefinito o spread.

- Se l'utente che esegue la distribuzione dispone dell'autorizzazione necessaria per gestire gli account cloud in modalità di manutenzione, il processo di allocazione può selezionare un account cloud in modalità di manutenzione perché l'utente potrebbe dover eseguire una distribuzione di prova prima di chiudere la finestra di manutenzione.
- Se l'utente non dispone dell'autorizzazione necessaria per gestire gli account cloud, gli account cloud in modalità di manutenzione vengono filtrati al di fuori del processo di allocazione.
- Gli host in modalità di manutenzione vengono conteggiati come parte del rapporto di spread. Per escludere un host in manutenzione dal calcolo del rapporto, è necessario impostare lo stato di alimentazione su Off.

Per un criterio di distribuzione.

- I rapporti vengono calcolati in base agli host. Gli host possono essere autonomi o far parte di un cluster.
- Se un host autonomo è disattivato, non viene conteggiato come parte del rapporto.
- Se un host che fa parte di un cluster è disattivato, lo stato disattivato non viene riflesso nel cluster e l'host viene comunque considerato durante il calcolo del rapporto.

Come impostare il criterio di posizionamento

Se sono presenti più zone cloud in un progetto che sono ugualmente idonee come destinazione per una distribuzione, la richiesta di distribuzione valuta dove posizionarle in base a come è stato configurato il **criterio di posizionamento**.

- 1 Selezionare **Infrastruttura > Progetti** e creare o selezionare un progetto.
- 2 Nel progetto, fare clic sulla scheda **Provisioning**.

3 Selezionare un criterio.

Criterio di posizionamento	Descrizione
Predefinito	<p>Distribuisce le risorse richieste nella prima zona cloud che soddisfa i requisiti.</p> <p>Selezionare Predefinito quando si desidera che i carichi di lavoro vengano distribuiti nell'ordine di priorità ed è indifferente che tutte le risorse vengano utilizzate in un host.</p> <p>Se questa opzione è selezionata, i valori della macchina virtuale e degli host non vengono recuperati.</p>
Spread	<p>Distribuisce le risorse richieste nella zona cloud con il minor numero di macchine virtuali per host.</p> <p>Selezionare Spread quando si desidera distribuire i carichi di lavoro negli host, utilizzando ampiamente le risorse tra gli host.</p> <p>Se questa opzione è selezionata, il numero di macchine virtuali e host viene recuperato dalle risorse della zona cloud e valutato.</p>

4 Fare clic su **Salva**.**Revisione delle modalità di applicazione del criterio**

Dopo aver configurato il criterio di posizionamento a livello di progetto, è possibile visualizzare in un diagramma di provisioning la posizione in cui il sistema prevede di distribuire il modello cloud.

- 1 Selezionare **Progettazione > Modelli cloud** e selezionare o configurare un modello che utilizzi il progetto per il quale è stato selezionato un criterio.
- 2 Fare clic su **Test**.
- 3 Quando il test viene completato correttamente, fare clic su **Diagramma di provisioning** nei risultati del test.

4 Il diagramma sarà simile a uno dei due esempi.

Tipo di criterio

Diagramma di provisioning

Predefinito



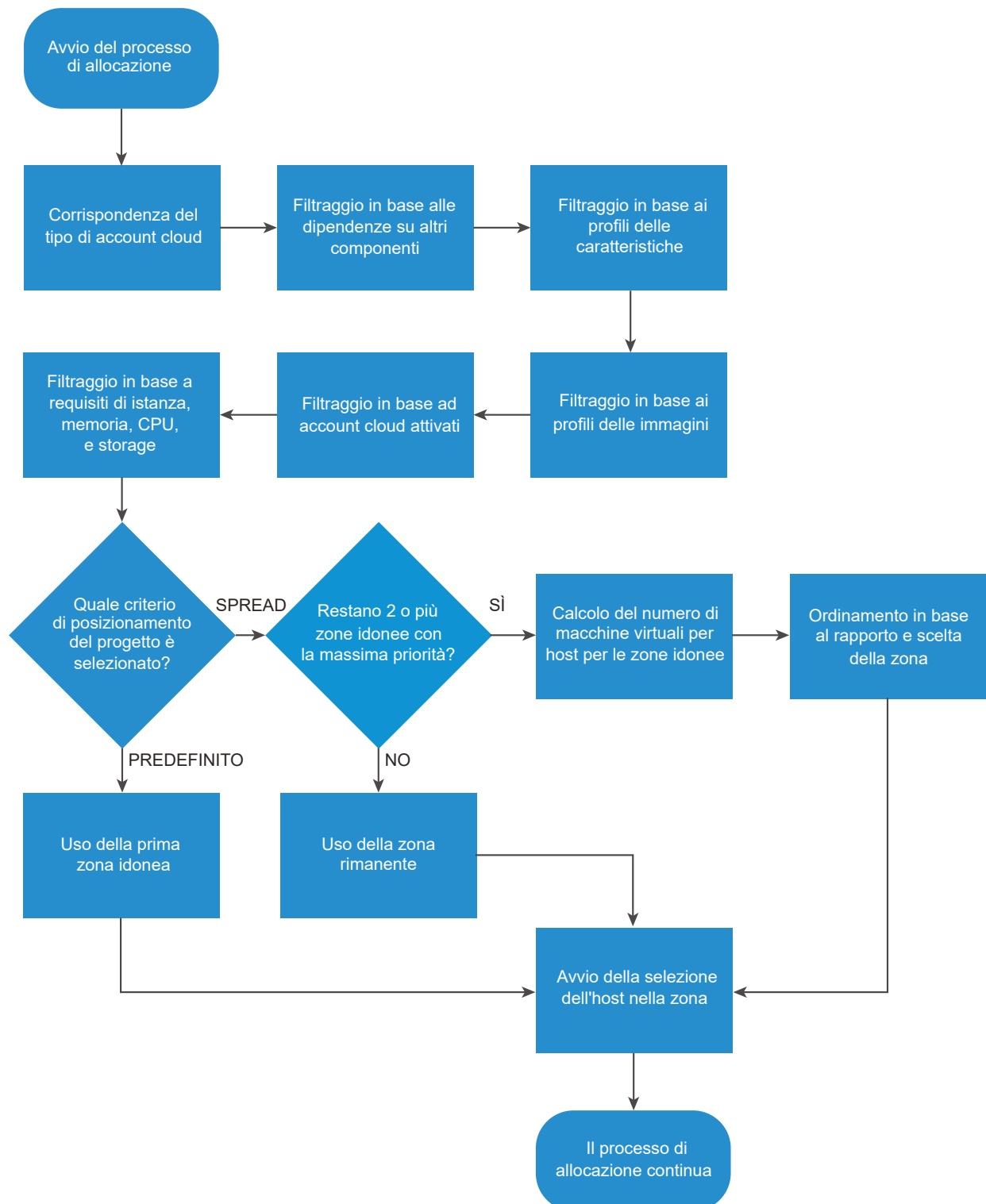
Spread



5 Se si è pronti per eseguire la distribuzione, tornare al modello cloud e fare clic su **Distribuisci**.

Valutazione dei criteri di posizionamento durante il processo di allocazione

Il diagramma seguente consente di comprendere quando il criterio viene valutato durante il processo di allocazione e quando vengono identificati la zona di destinazione e l'host.



Prezzi del progetto in Cloud Assembly

I costi disponibili nei progetti Cloud Assembly consentono di gestire le spese delle risorse associate a interi progetti. Il progetto include anche i singoli costi di distribuzione.

Ansible-Project DELETE

Summary Users Provisioning Kubernetes Provisioning **Price** Integrations

Price Analysis **\$10.81**
Month to date (private cloud only)

Deployment Name	Description	Requestor	Created On	Expiring In	Price
AnsibleTower-Demo		skurad@vmware.com	Jan 26, 2021	Never expires	\$3.07
Check-Delete		skurad@vmware.com	Jan 18, 2021	Never expires	\$3.04
Ansible vSphere		skurad@vmware.com	Jan 19, 2021	Never expires	\$3.01
WT with 2 machines		skurad@vmware.com	Feb 14, 2021	Never expires	\$0.61
Create with templates		skurad@vmware.com	Feb 14, 2021	Never expires	\$0.32
Ansible		skurad@vmware.com	Jan 07, 2021	Never expires	\$0.31
Create with job templates		skurad@vmware.com	Feb 14, 2021	Never expires	\$0.31

7 deployments

SAVE CANCEL

Le informazioni sui costi visualizzate per un progetto e per le singole distribuzioni vengono visualizzate dopo il provisioning di almeno una distribuzione associata al progetto. I costi vengono calcolati e aggiornati giornalmente in modo da poter tenere traccia del costo di una distribuzione nel corso del tempo. I valori iniziali sono basati sui benchmark di settore.

Gli amministratori del cloud possono modificare i valori per riflettere i costi effettivi.

Per ulteriori informazioni, vedere [Come utilizzare le schede dei prezzi in vRealize Automation](#).

Come funzionano i progetti di Cloud Assembly al momento della distribuzione

I progetti controllano l'accesso degli utenti alle zone cloud e alla proprietà degli utenti delle risorse di cui è stato eseguito il provisioning. Gli amministratori del cloud e gli sviluppatori di modelli cloud devono comprendere il funzionamento dei progetti al momento della distribuzione, in modo da poter gestire le distribuzioni e risolvere eventuali problemi.

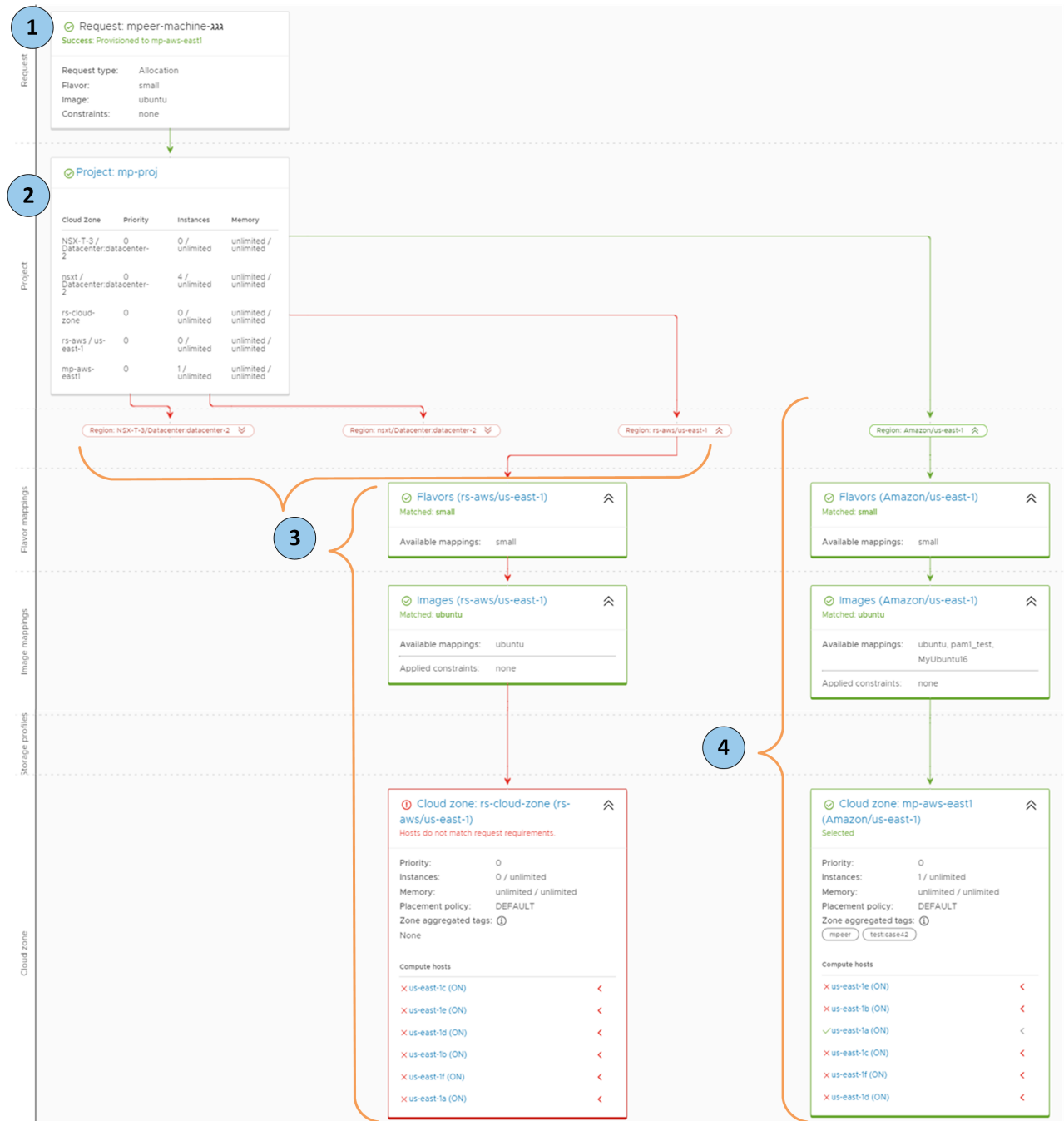
L'amministratore del cloud che configura progetti per vari team deve capire come i progetti determinano il punto in cui vengono distribuiti i componenti del modello cloud. Questa comprensione consente di creare progetti che supportano gli sviluppatori di modelli cloud e di risolvere i problemi relativi alle distribuzioni non riuscite.

Quando si crea un modello cloud, è necessario prima associarlo a un progetto. Al momento della distribuzione, i requisiti del modello cloud vengono valutati in base alle zone cloud del progetto per trovare la migliore posizione di distribuzione.

Il workflow raffigurato di seguito rappresenta il processo.

- 1 Si invia una richiesta di distribuzione del modello cloud.

- 2 Il progetto valuta i requisiti del modello e del progetto, ad esempio le caratteristiche, l'immagine e i tag di vincolo. I requisiti vengono confrontati con le zone cloud del progetto per individuare una zona che supporti i requisiti.
- 3 Queste zone non disponevano delle risorse necessarie per supportare la richiesta.
- 4 Questa zona supporta i requisiti della richiesta e il modello viene distribuito in questa regione dell'account della zona cloud.



Progettazione delle distribuzioni di Cloud Assembly

6

Le distribuzioni iniziano con i modelli cloud, precedentemente denominati blueprint, ovvero le specifiche codificate che definiscono le macchine, le applicazioni e i servizi per la creazione nelle risorse cloud tramite Cloud Assembly.

Funzionamento dei modelli cloud

I modelli possono essere destinati a fornitori cloud specifici o essere indipendenti dal cloud. Le zone cloud assegnate al progetto determinano l'approccio che è possibile adottare. Consultare l'amministratore del cloud per conoscere il tipo di risorse che costituiscono le zone cloud.

La creazione del modello di Cloud Assembly è un processo infrastructure-as-code. Iniziare aggiungendo risorse nella tela di progettazione. Quindi, compilare i dettagli utilizzando l'editor di codice. L'editor di codice consente di digitare direttamente il codice o immettere i valori in un modulo.

Prima di creare un modello cloud

È possibile creare un modello di Cloud Assembly in qualsiasi momento. Per distribuirlo, tuttavia, è necessario prima [Capitolo 4 Creazione dell'infrastruttura delle risorse di Cloud Assembly](#) e [Capitolo 5 Aggiunta e gestione di progetti di Cloud Assembly](#) che includa tale infrastruttura.

Pronti per la progettazione?

Esplorare la navigazione a sinistra o passare direttamente agli argomenti nella tabella seguente.

Inizia	Ulteriori informazioni sulle progettazioni e le funzionalità dei modelli cloud		Altri esempi
Introduzione alle progettazioni di Cloud Assembly	Input dell'utente nelle richieste di vRealize Automation	Contrassegni di risorsa di Cloud Assembly per le richieste	Esempio di modello di Cloud Assembly documentato
Creazione di binding e dipendenze tra le risorse in Cloud Assembly	Denominazione personalizzata per le risorse distribuite in Cloud Assembly	Espressioni di Cloud Assembly	Esempi di risorse di vSphere in Cloud Assembly

Inizia	Ulteriori informazioni sulle progettazioni e le funzionalità dei modelli cloud		Altri esempi
Controllo delle versioni dei modelli di Cloud Assembly	Riutilizzo di un gruppo di proprietà in Cloud Assembly	Proprietà di Cloud Assembly segrete	Ulteriori informazioni sulle risorse di rete nei modelli cloud di vRealize Automation
Altri modi per creare modelli di Cloud Assembly	Accesso remoto a una distribuzione di Cloud Assembly	Inizializzazione della macchina in Cloud Assembly	Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation
Come ottenere supporto per la compilazione del codice in Cloud Assembly	Indirizzi IP statici di vSphere in Cloud Assembly	Configurazioni di Terraform in Cloud Assembly	Ulteriori informazioni sulle risorse di bilanciamento del carico nei modelli cloud di vRealize Automation
	Cluster di macchine e dischi in Cloud Assembly	Posizionamento del disco SCSI con Cloud Assembly	Esempi di modelli cloud di configurazione Puppet di vCenter
	Tipi di risorse personalizzate per i modelli cloud di Cloud Assembly	Estensione e automazione dei cicli di vita delle applicazioni con l'estendibilità	

Questo capitolo include i seguenti argomenti:

- Introduzione alle progettazioni di Cloud Assembly
- Come ottenere supporto per la compilazione del codice in Cloud Assembly
- Creazione di binding e dipendenze tra le risorse in Cloud Assembly
- Controllo delle versioni dei modelli di Cloud Assembly
- Input dell'utente nelle richieste di vRealize Automation
- Riutilizzo di un gruppo di proprietà in Cloud Assembly
- Contrassegni di risorsa di Cloud Assembly per le richieste
- Espressioni di Cloud Assembly
- Proprietà di Cloud Assembly segrete
- Accesso remoto a una distribuzione di Cloud Assembly
- Posizionamento del disco SCSI con Cloud Assembly
- Inizializzazione della macchina in Cloud Assembly
- Cluster di macchine e dischi in Cloud Assembly
- Denominazione personalizzata per le risorse distribuite in Cloud Assembly
- Aggiunta della risorsa SaltStack Config nelle progettazioni di Cloud Assembly
- Configurazioni di Terraform in Cloud Assembly

- Tipi di risorse personalizzate per i modelli cloud di Cloud Assembly
- Progettazioni di Cloud Assembly per prepararsi alle modifiche giorno 2
- Altri esempi di codice di Cloud Assembly
- Schema delle proprietà delle risorse di vRealize Automation
- Altri modi per creare modelli di Cloud Assembly
- Estensione e automazione dei cicli di vita delle applicazioni con l'estendibilità

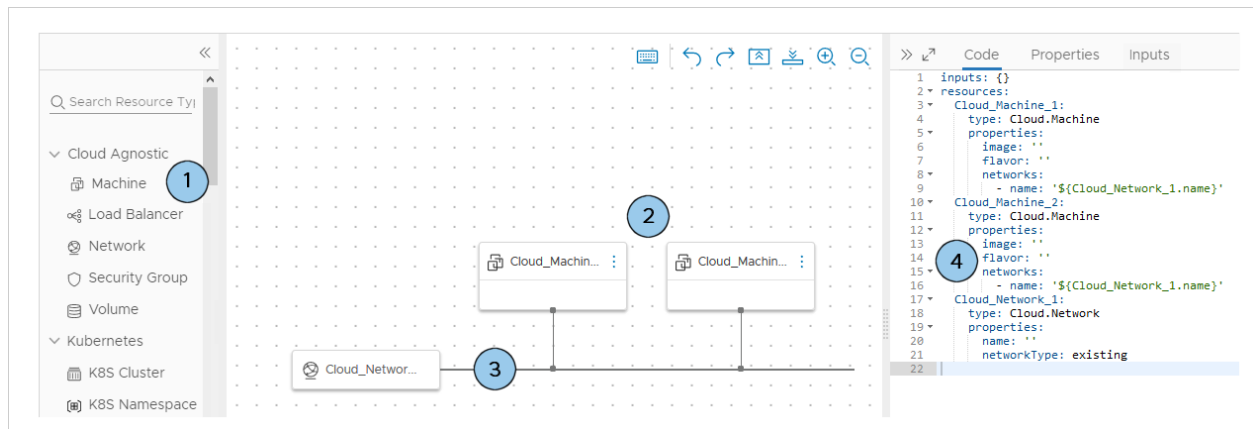
Introduzione alle progettazioni di Cloud Assembly

È possibile utilizzare la pagina Progettazione per creare le specifiche del modello di Cloud Assembly per le macchine e le applicazioni di cui si desidera eseguire il provisioning.

Come utilizzare la pagina Progettazione

Per creare un modello cloud da zero, passare a **Progettazione > Modelli cloud**. Quindi, fare clic su **Nuovo da > Tela vuota**.

- 1 Individuare le risorse.
- 2 Trascinare le risorsa nella tela.
- 3 Connettere le risorse.
- 4 Configurare le risorse modificando il codice del modello cloud.



Selezione e aggiunta di risorse alla tela

Le risorse vengono visualizzate a sinistra della pagina Progettazione per la selezione e il trascinamento.

Risorse indipendenti dal cloud	È possibile distribuire risorse indipendenti dal cloud a qualsiasi fornitore di soluzioni cloud. Al momento del provisioning, la distribuzione utilizza risorse specifiche del cloud corrispondenti. Ad esempio, se si prevede che un modello cloud venga distribuito in zone cloud di AWS e vSphere, utilizzare risorse indipendenti dal cloud.
Risorse del fornitore cloud	Le risorse del fornitore, come quelle specifiche di Amazon Web Services, Microsoft Azure, Google Cloud Platform o VMware vSphere, possono essere distribuite solo nelle zone cloud di AWS, Azure, GCP o vSphere. È possibile aggiungere risorse indipendenti dal cloud a un modello cloud che contiene risorse specifiche del cloud per un determinato fornitore. È necessario tenere in considerazione quali sono i fornitori supportati dalle zone cloud del progetto.
Risorse di gestione della configurazione	Le risorse di gestione della configurazione dipendono dalle applicazioni integrate. Ad esempio, una risorsa Puppet può monitorare e imporre la configurazione delle altre risorse.

Connessione delle risorse

Utilizzare i controlli grafici della tela di progettazione di Cloud Assembly per connettere le risorse.

Le risorse devono essere compatibili per una connessione. Ad esempio:

- Connessione di un bilanciamento del carico a un cluster di macchine.
- Connessione di una macchina a una rete.
- Connessione di uno storage esterno a una macchina.

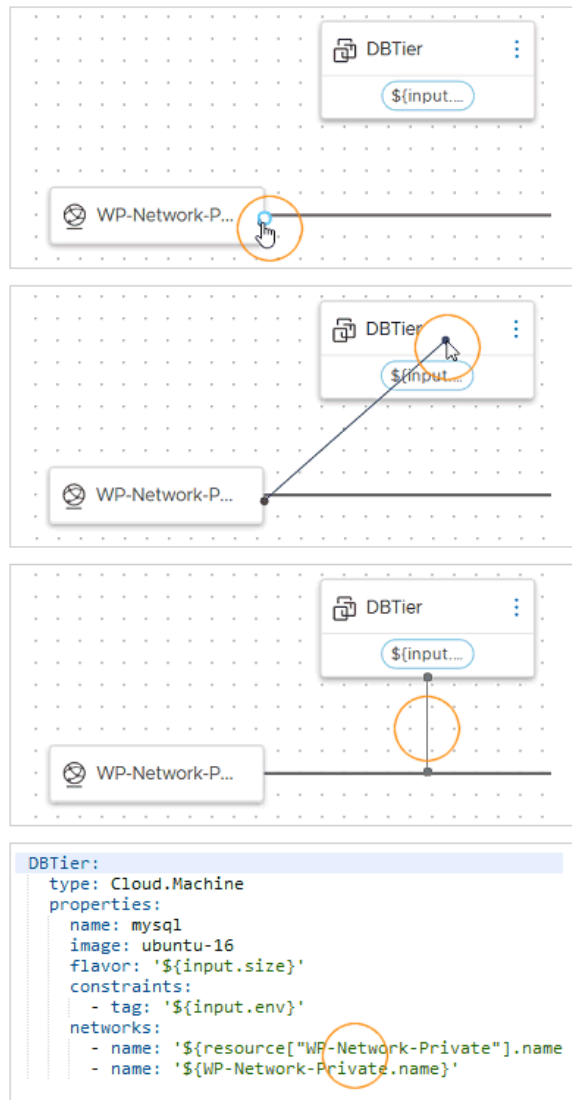
Importante Un connettore a linea continua richiede che le due risorse siano distribuite nella stessa zona cloud. Se si aggiungono vincoli in conflitto alle risorse, la distribuzione potrebbe non riuscire.

Ad esempio, non è possibile distribuire risorse connesse in cui i tag di vincolo forzano il posizionamento di una di queste in una zona in us-west-1 e l'altra in una zona in us-east-1.

Le frecce continue o tratteggiate indicano solo una dipendenza, non una connessione. Per ulteriori informazioni sulle dipendenze, vedere [Creazione di binding e dipendenze tra le risorse in Cloud Assembly](#).

Per eseguire la connessione, passare il puntatore del mouse sopra il bordo di una risorsa per visualizzare la finestra di connessione. Fare quindi clic e trascinare la finestra nella risorsa di destinazione e rilasciarla.

Nell'editor di codice viene visualizzato il codice aggiuntivo della risorsa di origine nel codice della risorsa di destinazione.



Nella figura, la macchina SQL e la rete privata sono connesse, pertanto devono essere distribuite nella stessa zona cloud.

Modifica del codice del modello cloud

L'editor di codice consente di digitare, tagliare, copiare e incollare direttamente il codice. Se non si desidera procedere con la modifica del codice, è possibile fare clic su una risorsa già presente nella tela di progettazione, fare clic sulla scheda **Proprietà** dell'editor di codice e immettere i valori. I valori delle proprietà immessi vengono visualizzati nel codice come se fossero stati digitati direttamente.

The screenshot displays the vRealize Automation Cloud Assembly interface. On the left, a code editor shows the following JSON configuration for a 'WebTier' resource:

```
WebTier:
  type: Cloud.Machine
  properties:
    name: wordpress
    flavor: '${input.size}'
    image: ubuntu
    count: '${input.count}'
    constraints:
      - tag: '${input.env}'
    networks:
      - network: '${resource["WP-Network-Private"].id}'
        assignPublicIpAddress: true
    storage:
      disks:
        - capacityGb: '${input.archiveDiskSize}'
          name: ArchiveDisk
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
  packages:
    - apache2
    - php
    - php-mysql
    - libapache2-mod-php
```

On the right, the 'Properties' tab is active, showing a form for configuring the resource. The form includes the following fields and sections:

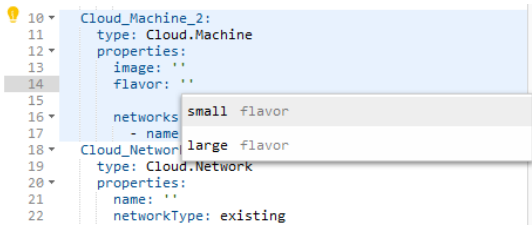
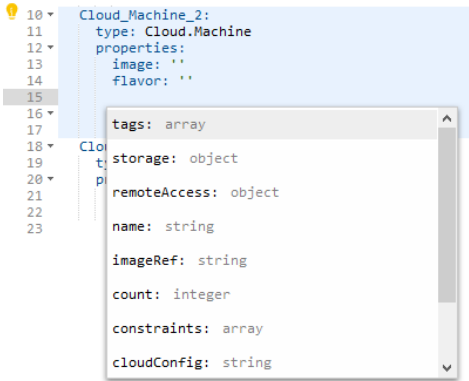
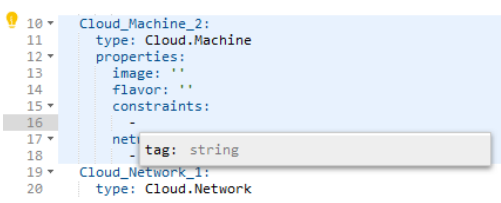
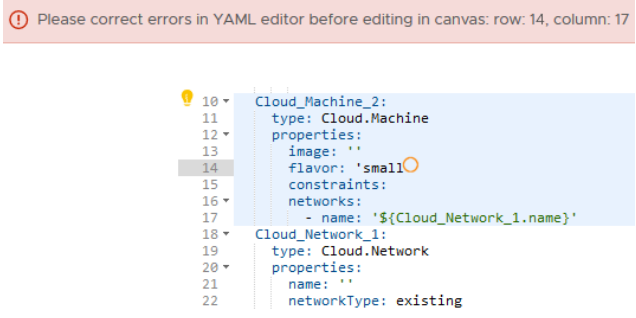
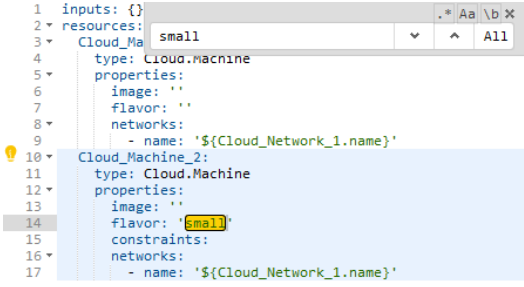
- Count:** A text input field with the value "\${input.count}" and a copy icon.
- Image Type:** A dropdown menu with the value "ubuntu" and a copy icon.
- Flavor *:** A dropdown menu with the value "\${input.size}" and a copy icon.
- Storage:** A section with a plus icon and a dropdown menu.
- Constraints:** A section with a plus icon and a dropdown menu.
- Maximum Capacity of the disk in GB:** A text input field with the value "1" and a copy icon.
- Size of boot disk in GB:** A text input field with the value "1" and a copy icon.
- Networks:** A section with a plus icon and a dropdown menu.

Si noti che è possibile copiare e incollare il codice da un modello cloud all'altro.

Come ottenere supporto per la compilazione del codice in Cloud Assembly

Aggiungendo le risorse di Cloud Assembly e connettendole nella tela viene creato solo un codice di avvio. Per configurarle completamente, modificare il codice.

L'editor di codice consente di digitare direttamente il codice o immettere i valori delle proprietà in un modulo. Per agevolare la creazione diretta del codice, l'editor di Cloud Assembly include funzionalità di completamento della sintassi e controllo degli errori.

Suggerimenti dell'editor	Esempio
Valori disponibili	
Proprietà consentite	
Proprietà figlio	
Errori di sintassi	
Ctrl+F per la ricerca	

Suggerimenti dell'editor **Esempio**

Parametri facoltativi

Guida dello schema Per tutte le proprietà personalizzate, è possibile fare riferimento anche al [Tipo schema di risorse di vRealize Automation in VMware {code}](#).

cloudConfig
 Type: string
 When provisioning an instance, machine cloud-init startup instructions from user data fields. Sample cloud config instructions:

```
#cloud-config
repo_update: true
repo_upgrade: all
packages:
- httpd
- db-server

runcmd:
- [ sh, -c, "amazon-linux-extras insta
- systemctl start httpd
- sudo systemctl enable httpd
```

```
DBTier:
type: Cloud.Machine
properties:
  name: mysql
  image: ubuntu-16
  flavor: '${input.size}'
  constraints:
    - tag: '${input.env}'
  networks:
    - name: '${resource["WP-Network-Private
    - name: '${WP-Network-Private.name}'
  remoteAccess:
    authentication: usernamePassword
    username: '${input.username}'
    password: '${input.userpassword}'
  cloudConfig:
    cloud-config
    repo_update: true
    repo_upgrade: all
    packages:
      - mysql-server
    runcmd:
      - sed -e '/bind-address/ s/^#/#/' -i
      - service mysql restart
      - mysql -e "GRANT ALL PRIVILEGES ON *.
      - mysql -e "FLUSH PRIVILEGES;"
  attachedDisks: []
  bTier:
  type: Cloud.Machine
```

Creazione di binding e dipendenze tra le risorse in Cloud Assembly

Quando si distribuisce un modello di Cloud Assembly, una risorsa potrebbe avere bisogno che un'altra risorsa sia disponibile per prima.

Importante Le frecce indicano solo una dipendenza, non una connessione. Per connettere le risorse in modo da farle comunicare, vedere [Introduzione alle progettazioni di Cloud Assembly](#).

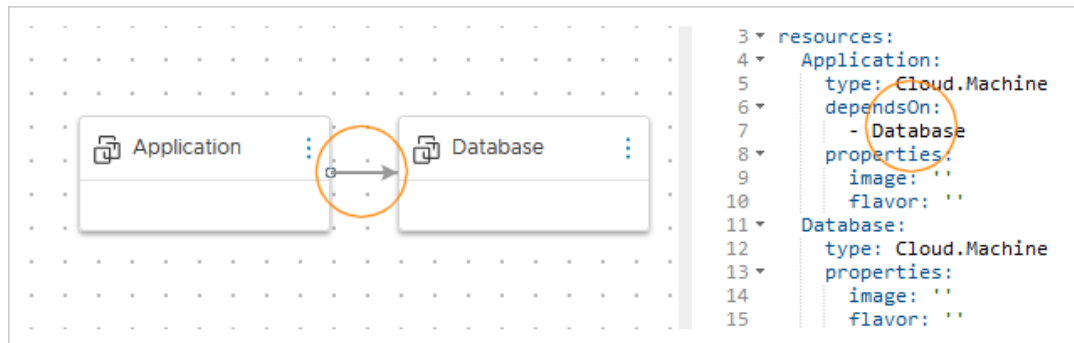
Dipendenze esplicite

A volte una risorsa richiede che un altro componente venga distribuito prima. Ad esempio, potrebbe essere necessario che esista un server di database prima che sia possibile creare e configurare per l'accesso un server applicazioni.

Una dipendenza esplicita imposta l'ordine di creazione al momento della distribuzione o per le azioni di scalabilità verticale o scalabilità orizzontale. È possibile aggiungere una dipendenza esplicita utilizzando la tela di progettazione grafica o l'editor di codice.

- Opzione Tela di progettazione: consente di disegnare una connessione a partire dalla risorsa dipendente fino alla risorsa da distribuire per prima.
- Opzione Editor di codice: consente di aggiungere una proprietà `dependsOn` alla risorsa dipendente e di identificare la risorsa da distribuire per prima.

Una dipendenza esplicita crea una freccia continua nella tela.



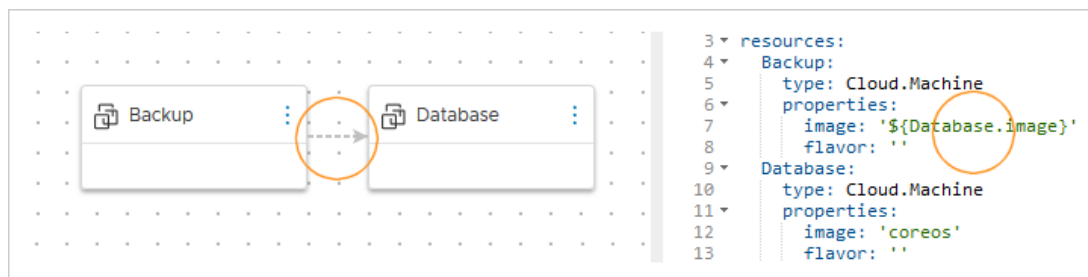
Binding di proprietà

A volte una proprietà di una risorsa richiede un valore presente in una proprietà di un'altra risorsa. Ad esempio, un server di backup potrebbe richiedere l'immagine del sistema operativo del server di database di cui è in corso il backup, per cui il server di database deve esistere per primo.

Denominato anche dipendenza implicita, un binding di proprietà controlla l'ordine di creazione attendendo la disponibilità della proprietà necessaria prima di distribuire la risorsa dipendente. È possibile aggiungere un binding di proprietà utilizzando l'editor di codice.

- Modificare la risorsa dipendente, aggiungendo una proprietà che identifichi la risorsa e la proprietà che devono esistere prima.

Un binding di proprietà crea una freccia tratteggiata nella tela.



Controllo delle versioni dei modelli di Cloud Assembly

Lo sviluppatore di modelli cloud può acquisire in modo sicuro uno snapshot di una progettazione funzionante prima di rischiare ulteriori modifiche.

Al momento della distribuzione, è possibile selezionare una qualsiasi delle versioni da distribuire.

Acquisizione della versione di un modello cloud

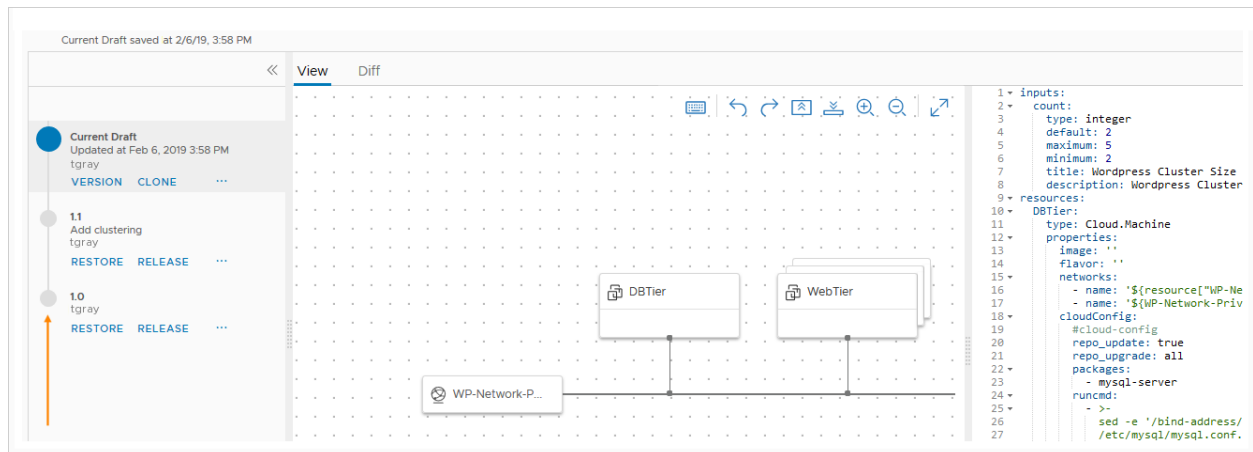
Dalla pagina di progettazione, fare clic su **Versione** e specificare un nome.

Il nome deve essere alfanumerico, senza spazi. Solo punti, trattini e caratteri di sottolineatura sono consentiti come caratteri speciali.

Ripristino di una versione meno recente

Dalla pagina di progettazione, fare clic su **Cronologia versioni**.

A sinistra, selezionare una versione precedente per ispezionarla nella tela e nell'editor di codice. Quando si trova la versione desiderata, fare clic su **Ripristina**. Il ripristino sovrascrive la bozza corrente senza rimuovere le versioni con nome.



Rilascio di una versione in Service Broker

Dalla pagina di progettazione, fare clic su **Cronologia versioni**.

A sinistra, selezionare una versione e rilasciarla.

Non è possibile rilasciare una bozza corrente finché non se ne controlla la versione.

Reimportazione della versione in Service Broker

Per abilitare la nuova versione per gli utenti del catalogo, importarla nuovamente.

In Service Broker, passare a **Contenuti e criteri > Origini contenuto**.

Nell'elenco delle origini, fare clic sull'origine del progetto che contiene il modello cloud con la versione appena rilasciata.

Fare clic **Salva e importa**.

Confronto delle versioni dei modelli cloud

Quando le modifiche e le versioni si accumulano, si consiglia di identificare le differenze tra di esse.

In Cloud Assembly, nella vista Cronologia versioni, selezionare una versione e fare clic su **Diff**. Quindi, dal menu a discesa **Diff rispetto a**, selezionare un'altra versione con cui confrontare.

Si noti che è possibile alternare tra la revisione delle differenze di codice e le differenze di topologia visiva.

Figura 6-1. Differenze di codice

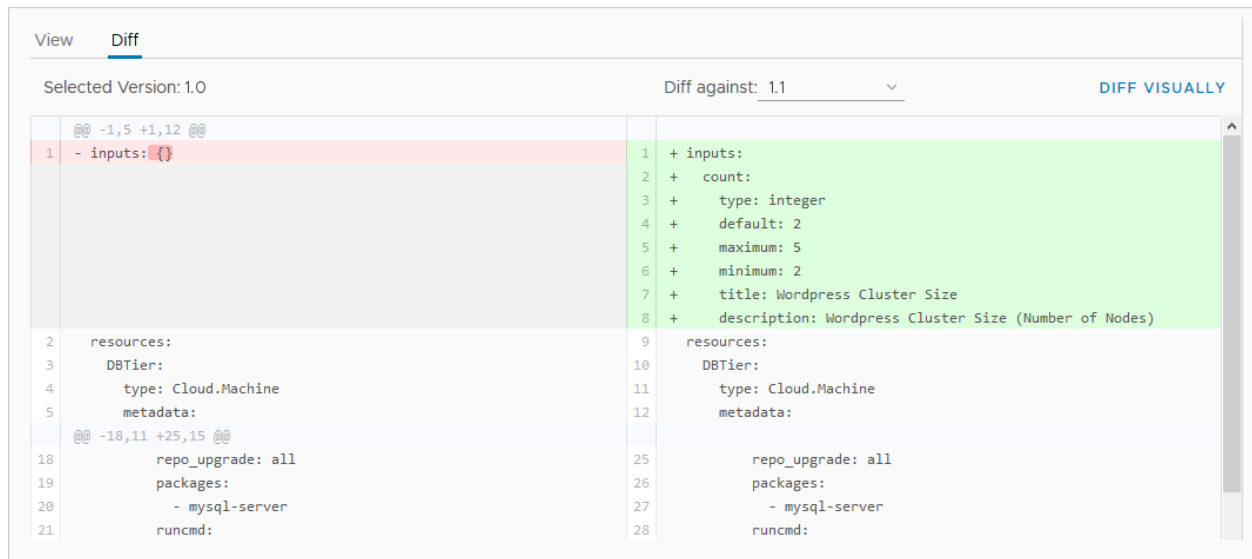
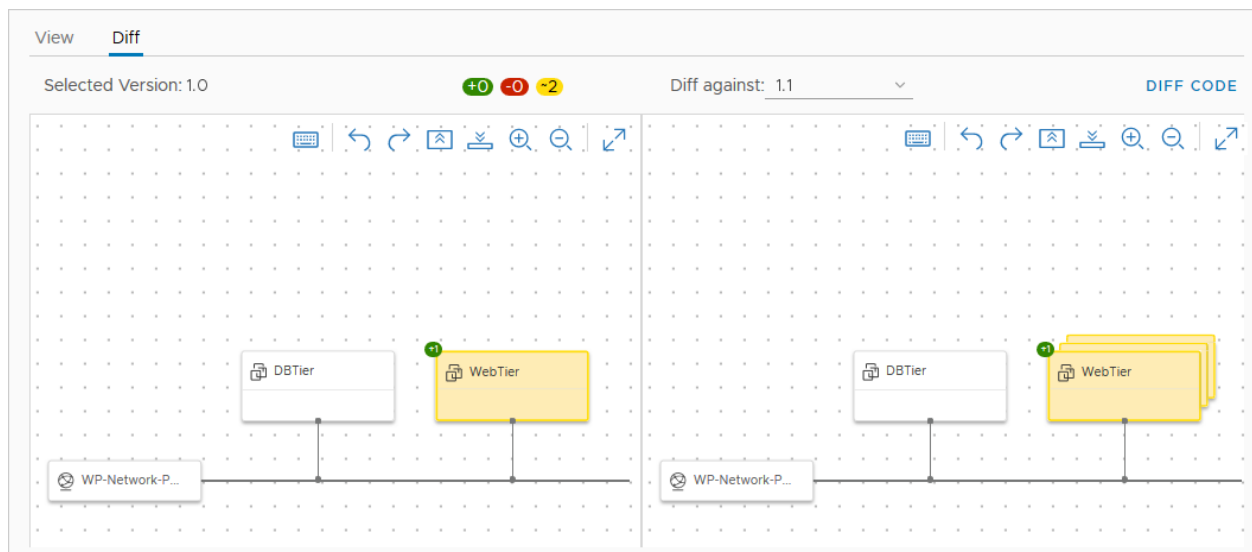


Figura 6-2. Differenze di topologia visiva



Clonazione di un modello cloud

Anche se non è come salvare una versione, dalla pagina di progettazione, **Azioni > Clona** crea una copia del modello corrente per lo sviluppo alternativo.

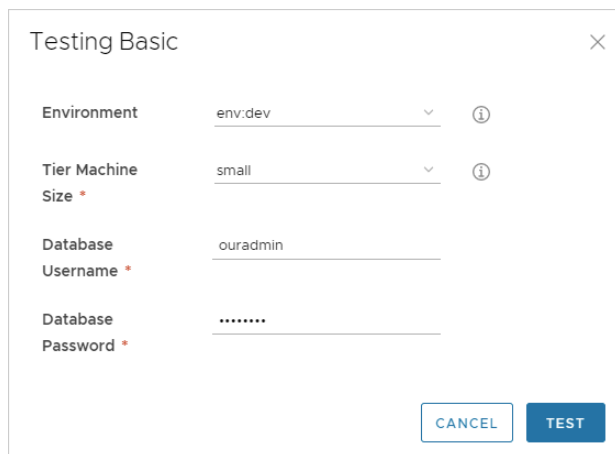
Input dell'utente nelle richieste di vRealize Automation

Il progettista di modelli cloud usa i parametri di input in modo che gli utenti possano effettuare selezioni personalizzate al momento della richiesta.

Funzionamento degli input

Quando gli utenti forniscono input, non è più necessario salvare più copie del modello che sono solo leggermente diverse. Inoltre, gli input possono preparare un modello per le operazioni giorno 2. Vedere [Come utilizzare gli input del modello cloud per gli aggiornamenti giorno 2 di vRealize Automation](#).

I seguenti input illustrano come creare un modello cloud per un server di database MySQL in cui gli utenti possono distribuire tale modello in ambienti di risorse cloud diversi e applicare ogni volta capacità e credenziali diverse.



Aggiunta di parametri di input

Aggiungere una sezione `inputs` al codice del modello in cui impostare valori selezionabili.

Nell'esempio seguente è possibile selezionare le dimensioni della macchina, il sistema operativo e il numero di server in cluster.

```
inputs:
  wp-size:
    type: string
    enum:
      - small
      - medium
    description: Size of Nodes
```



```

    title: Node Size
  wp-image:
    type: string
    enum:
      - coreos
      - ubuntu
    title: Select Image/OS
  wp-count:
    type: integer
    default: 2
    maximum: 5
    minimum: 2
    title: Wordpress Cluster Size
    description: Wordpress Cluster Size (Number of nodes)

```

Se non si è sicuri di come modificare il codice, è possibile fare clic sulla scheda **Input** dell'editor di codice e immettere le impostazioni in tale scheda. L'esempio seguente illustra alcuni input per il database MySQL menzionato in precedenza.

The screenshot shows the 'Inputs' tab of the 'Cloud Template Inputs' editor. A table lists four inputs: 'size', 'username', 'userpassword', and 'databaseDiskSize'. A modal window titled 'Edit Cloud Template Input: size' is open, showing the configuration for the 'size' input.

<input type="checkbox"/>	Name	Title	Type	Default Value
<input type="checkbox"/>	size	Tier Machine Size	string	
<input type="checkbox"/>	username	Database Username	string	
<input type="checkbox"/>	userpassword	Database Password	string	****
<input type="checkbox"/>	databaseDiskSize	MySQL Data Disk Size	number	4

Edit Cloud Template Input: size

Name *

Title

Description

Type

Encrypted ☐

Riferimenti ai parametri di input

Successivamente, nella sezione `resources`, fare riferimento a un parametro di input utilizzando la sintassi `${input.property-name}`.

Se un nome di proprietà include uno spazio, delimitarlo con parentesi quadre e virgolette doppie anziché utilizzare la notazione dei punti: `${input["property name"]}`

Importante Nel codice del modello cloud non è possibile utilizzare la parola `input` se non per indicare un parametro di input.

```
resources:
  WebTier:
    type: Cloud.Machine
    properties:
      name: wordpress
      flavor: '${input.wp-size}'
      image: '${input.wp-image}'
      count: '${input.wp-count}'
```

Input facoltativi

Gli input sono in genere obbligatori e contrassegnati con un asterisco. Per rendere facoltativo un input, impostare un valore predefinito vuoto come mostrato.

```
owner:
  type: string
  minLength: 0
  maxLength: 30
  title: Owner Name
  description: Account Owner
  default: ''
```

Testing Basic

Environment: env.dev

Tier Machine Size: small

Owner Name: ←

Database Username: ouradmin

Database Password:

CANCEL TEST

Elenco delle proprietà di input

Proprietà	Descrizione
const	Utilizzata con oneOf. Valore reale associato al titolo descrittivo.
default	Valore precompilato per l'input. Il valore predefinito deve essere di tipo corretto. Non immettere una parola come valore predefinito per un numero intero.
description	Testo della guida dell'utente per l'input.
encrypted	Indica se crittografare l'input inserito dall'utente. Può essere true o false. Le password sono in genere crittografate. È inoltre possibile creare proprietà crittografate riutilizzabili in più modelli cloud. Vedere Proprietà di Cloud Assembly segrete .
enum	Menu a discesa di valori consentiti. Utilizzare l'esempio seguente come guida per il formato. <pre>enum: - value 1 - value 2</pre>
format	Imposta il formato previsto per l'input. Ad esempio, (25/04/19) supporta data-ora. Consente di utilizzare il selettore della data nei moduli personalizzati di Service Broker.
items	Dichiara gli elementi all'interno di una matrice. Supporta numeri, numeri interi, stringhe, valori booleani o oggetti.
maxItems	Numero massimo di elementi selezionabili in una matrice.
maxLength	Numero massimo di caratteri consentiti per una stringa. Ad esempio, per fare in modo che un campo non contenga più di 25 caratteri, immettere <code>maxLength: 25</code> .
maximum	Valore massimo consentito per un numero o un numero intero.
minItems	Numero minimo di elementi selezionabili in una matrice.
minLength	Numero minimo di caratteri consentiti per una stringa.
minimum	Valore minimo consentito per un numero o un numero intero.
oneOf	Consente al modulo di input dell'utente di visualizzare un nome descrittivo (title) per un valore meno descrittivo (const). Se si imposta un valore predefinito, specificare const, non title. Valida per l'uso con i tipi stringa, numero intero e numero.

Proprietà	Descrizione
pattern	Caratteri consentiti per gli input stringa nella sintassi delle espressioni regolari. Ad esempio '[a-z]+' o '[a-z0-9A-Z@#&]+'.
properties	Dichiara il blocco delle proprietà key:value per gli oggetti.
readOnly	Utilizzata per fornire solo un'etichetta del modulo.
title	Utilizzata con oneOf. Nome descrittivo per un valore const. Il titolo viene visualizzato nel modulo di input dell'utente al momento della distribuzione.
type	Tipo di dati numero, numero intero, stringa, booleano o oggetto. Importante Un tipo booleano aggiunge una casella di controllo vuota al modulo di richiesta. Se si lascia invariata la casella, l'input non viene impostato su False. Per impostare l'input su False, gli utenti devono selezionare e deselezionare la casella.
writeOnly	Sostituisce le pressioni dei tasti con asterischi nel modulo. Non può essere utilizzata con enum. Viene visualizzata come campo della password nei moduli personalizzati di Service Broker.

Altri esempi

Stringa con enumerazione

```
image:
  type: string
  title: Operating System
  description: The operating system version to use.
  enum:
    - ubuntu 16.04
    - ubuntu 18.04
  default: ubuntu 16.04

shell:
  type: string
  title: Default shell
  description: The default shell that will be configured for the created user.
  enum:
    - /bin/bash
    - /bin/sh
```

Numero intero con minimo e massimo

```
count:
  type: integer
  title: Machine Count
  description: The number of machines that you want to deploy.
  maximum: 5
  minimum: 1
  default: 1
```

Matrice di oggetti

```
tags:
  type: array
  title: Tags
  description: Tags that you want applied to the machines.
  items:
    type: object
    properties:
      key:
        type: string
        title: Key
      value:
        type: string
        title: Value
```

Stringa con nomi descrittivi

```
platform:
  type: string
  oneOf:
    - title: AWS
      const: platform:aws
    - title: Azure
      const: platform:azure
    - title: vSphere
      const: platform:vsphere
  default: platform:aws
```

Stringa con convalida del pattern

```
username:
  type: string
  title: Username
  description: The name for the user that will be created when the machine is provisioned.
  pattern: ^[a-zA-Z]+$
```

Stringa come password

```
password:
  type: string
  title: Password
  description: The initial password that will be required to logon to the machine.
  Configured to reset on first login.
  encrypted: true
  writeOnly: true
```

Stringa come area di testo

```
ssh_public_key:
  type: string
  title: SSH public key
  maxLength: 256
```

Booleano

```
public_ip:
  type: boolean
  title: Assign public IP address
  description: Choose whether your machine should be internet facing.
  default: false
```

Selettore calendario data e ora

```
leaseDate:
  type: string
  title: Lease Date
  format: date-time
```

Azioni di vRealize Orchestrator come input

In un modello di Cloud Assembly, è possibile includere le azioni di vRealize Orchestrator come input del modello cloud.

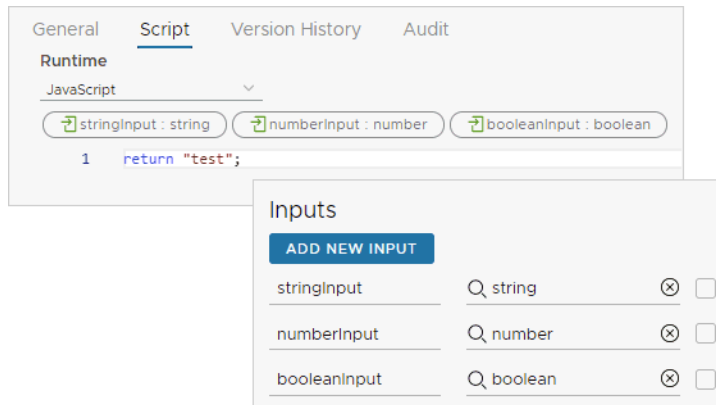
Aggiunta di un'azione di vRealize Orchestrator agli input del modello cloud

Per utilizzare le azioni di vRealize Orchestrator come input del modello cloud, seguire queste linee guida.

- 1 Nell'istanza di vRealize Orchestrator integrata in vRealize Automation, creare un'azione che esegua l'operazione desiderata.

L'azione di vRealize Orchestrator può includere solo tipi stringa, numero intero, numero e valori booleani primitivi. I tipi di vRealize Orchestrator non sono supportati.

In questo semplice esempio, l'azione di vRealize Orchestrator raccoglie tre input e restituisce una stringa hardcoded.



- 2 In Cloud Assembly, creare o modificare un modello cloud.
- 3 Nell'editor di codice, fare clic sulla scheda **Input** e su **Nuovo input modello cloud**.
- 4 Per aggiungere gli input dell'azione di vRealize Orchestrator, fare clic sul tipo, quindi su **Costante**.

Aggiungere separatamente ogni input dell'azione di vRealize Orchestrator come nuovo input del modello cloud.

The screenshot shows the 'New Cloud Template Input' form. It has fields for 'Name *' (filled with 'numberInput'), 'Display Name' (filled with 'Number for VRO'), and 'Description' (empty). Below these is a 'Type' section with a row of buttons: 'STRING', 'INTEGER', 'NUMBER', 'BOOLEAN', 'OBJECT', and 'ARRAY'. The 'NUMBER' button is highlighted with an orange arrow. Below the 'Type' section is a 'Default value source' section with two radio buttons: 'Constant' (selected) and 'External source'. An orange arrow points to the 'Constant' radio button. At the bottom is a 'Default value' field (empty).

- 5 Dopo aver aggiunto gli input dell'azione, creato un nuovo input del modello cloud, fare clic sul tipo, fare clic su **Origine esterna**, quindi fare clic su **Seleziona**.

New Cloud Template Input

Name * vroAction

Display Name VRO Action

Description

Type **STRING** INTEGER NUMBER BOOLEAN OBJECT ARRAY

Default value source ☐ Constant ☒ External source

Action Add an existing action

SELECT

- 6 In **Azione**, cercare e selezionare l'azione di vRealize Orchestrator creata, quindi fare clic su **Salva**.

Add an existing action

Action *

returnSimpleAction
com.form.service.test

CANCEL **SAVE**

Quando si distribuisce il modello cloud, le impostazioni dell'azione di vRealize Orchestrator vengono visualizzate nel modulo di input per l'utente richiedente.

Values for VRO

String for VRO

VRO Action

Number for VRO

On-Off for VRO

test

☐

Valori predefiniti configurabili

Per compilare il modulo di input con valori predefiniti, eseguire una delle operazioni seguenti quando si aggiunge l'azione di vRealize Orchestrator come origine esterna.

- Specificare manualmente il valore della proprietà predefinita.

Deselezionare l'opzione **Associa** e immettere il valore.

Add an existing action

Action *

Action Parameters

Input

Q com.form.service.test/Action

Readme

☐ Bind

- Utilizzare un altro valore di proprietà dagli input già presenti nel modello cloud.

Selezionare l'opzione **Associa** e selezionare una proprietà nell'elenco a discesa.

Add an existing action

Action *

Action Parameters

Input

Q com.form.service.test/Action

Canvas fields

Hard String

Input String

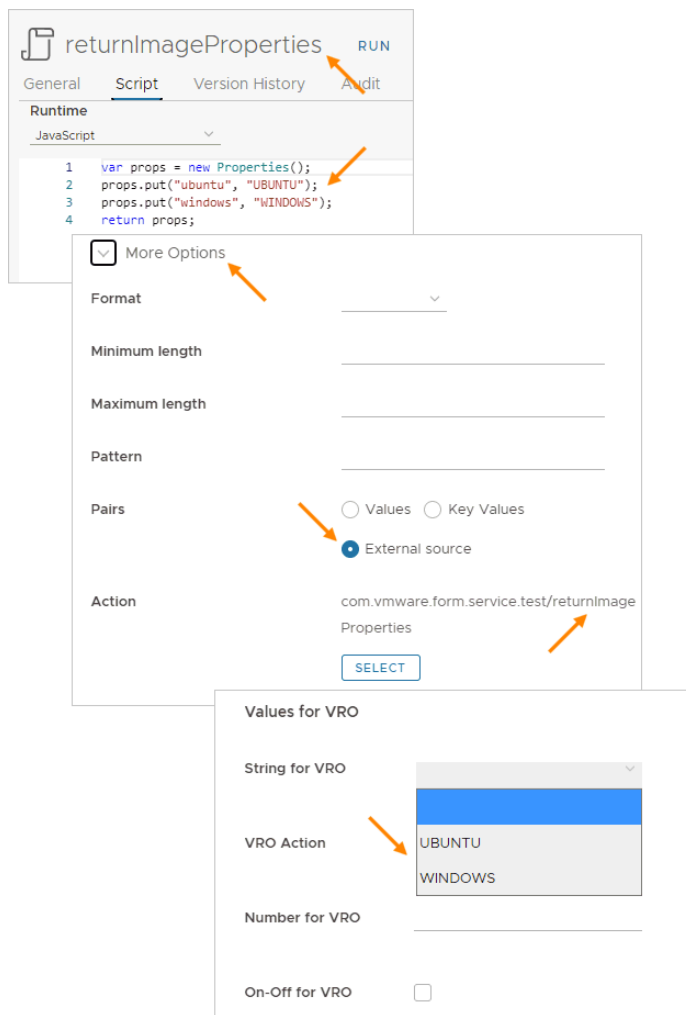
☒ Bind

Aggiunta di selezioni di input enumerate di vRealize Orchestrator

Per creare un elenco di selezione basato su vRealize Orchestrator in un modulo di input, procedere come segue durante l'aggiunta agli input del modello cloud.

- 1 In vRealize Orchestrator, creare un'azione che mappi i valori desiderati per l'elenco.
- 2 In Cloud Assembly, quando si aggiunge l'input del modello cloud, espandere **Altre opzioni**.
- 3 Per **Coppie**, fare clic su **Origine esterna**, fare clic su **Seleziona** e aggiungere l'azione di vRealize Orchestrator creata.

Nota Se si crea anche un valore predefinito quando si aggiunge la proprietà, tale valore predefinito deve corrispondere esattamente a uno dei valori enumerati dall'azione di vRealize Orchestrator.



Riutilizzo di un gruppo di proprietà in Cloud Assembly

Quando sono presenti proprietà di Cloud Assembly che vengono utilizzate sempre insieme, è possibile unirle in un gruppo di proprietà.

Più proprietà possono essere aggiunte in progettazioni di Cloud Assembly diverse molto più rapidamente come gruppo anziché una alla volta. È inoltre possibile gestire o modificare il set di proprietà da un'unica posizione in modo da garantirne l'applicazione coerente.

Solo gli utenti con il ruolo di amministratore di Cloud Assembly possono creare, aggiornare o eliminare un gruppo di proprietà. L'amministratore può condividere un gruppo di proprietà con un'intera organizzazione o limitarne l'uso solo all'interno di un progetto.

Attenzione Un gruppo di proprietà può essere incluso in molti modelli cloud, inclusi quelli già rilasciati nel catalogo. Le modifiche apportate a un gruppo di proprietà possono riguardare altri utenti.

Esistono due tipi di gruppi di proprietà.

- **Gruppi di proprietà di input in Cloud Assembly**

I gruppi di proprietà di input raccolgono e applicano un set di proprietà coerente al momento della richiesta dell'utente. I gruppi di proprietà di input possono includere voci che l'utente può aggiungere o selezionare oppure valori di sola lettura richiesti dalla progettazione.

Le proprietà che l'utente deve modificare o selezionare possono essere leggibili o crittografate. Le proprietà di sola lettura vengono visualizzate nel modulo di richiesta, ma non possono essere modificate. Se si desidera che i valori di sola lettura rimangano completamente nascosti, utilizzare invece un gruppo di proprietà costanti.

- **Gruppi di proprietà costanti in Cloud Assembly**

I gruppi di proprietà costanti applicano proprietà note in modo invisibile all'utente. I gruppi di proprietà costanti sono di fatto metadati invisibili. Forniscono valori alle progettazioni di Cloud Assembly in modo che l'utente richiedente non possa leggerli, né rendersi conto della loro presenza. Alcuni esempi possono essere codici di licenza o credenziali di account di dominio.

I due tipi di gruppi di proprietà vengono gestiti in modo molto diverso da Cloud Assembly. Quando si crea un gruppo di proprietà, è innanzitutto necessario scegliere se creare input o costanti. Non è possibile creare un gruppo di proprietà combinato né convertire un set di proprietà esistente e il relativo gruppo di proprietà da un tipo all'altro.

Gruppi di proprietà di input in Cloud Assembly

I gruppi di proprietà di input di Cloud Assembly in genere includono impostazioni correlate che devono essere immesse o selezionate dall'utente. Possono inoltre includere valori di sola lettura richiesti dalla progettazione del modello cloud.

Creazione del gruppo di proprietà di input

- 1 Passare a **Progettazione > Gruppi di proprietà** e fare clic su **Nuovo gruppo di proprietà**.
- 2 Selezionare **Valori di input**.
- 3 Specificare un nome e inserire una descrizione per il nuovo gruppo di proprietà.

Nome	I nomi dei gruppi di proprietà devono essere univoci all'interno di una determinata organizzazione. Sono consentiti solo lettere, numeri e caratteri di sottolineatura.
Nome visualizzato	Aggiungere un'intestazione per l'intero gruppo di proprietà, che verrà visualizzata nel modulo di richiesta.
Descrizione	Descrivere l'uso a cui è destinato questo set di proprietà.
Scope	<p>Stabilire se un amministratore può condividere il gruppo di proprietà con l'intera organizzazione. In caso contrario, un solo progetto potrà accedere al gruppo di proprietà.</p> <p>Anche se è sempre possibile aggiungere o modificare proprietà nel gruppo, l'ambito è permanente e non può essere modificato in un secondo momento.</p>
Progetto	Quando l'ambito è solo di un progetto, questo progetto può accedere al gruppo di proprietà.

4 Per aggiungere una proprietà al gruppo, fare clic su **Nuova proprietà**.

Il pannello per l'aggiunta di una nuova proprietà è molto simile alla scheda Input dell'editor di codice della pagina di progettazione di Cloud Assembly.

Nome	Nome in formato libero per la singola proprietà. Sono consentiti solo lettere, numeri e caratteri di sottolineatura.
Nome visualizzato	Aggiungere il nome di una singola proprietà da visualizzare nel modulo di richiesta.
Tipo	String, Integer, Number, Boolean (true o false), Object o Array.
Valore predefinito	<p>Voce del valore preimpostato che viene visualizzato nel modulo di richiesta.</p> <p>Per tutti i tipi ad eccezione di Booleano, l'immissione dell'utente è facoltativa per impostazione predefinita. Per assicurarsi che tutti gli input includano voci, eseguire una delle operazioni seguenti:</p> <ul style="list-style-type: none"> ■ Impostare un valore predefinito. ■ Richiedere l'input dell'utente aggiungendo la proprietà del modello cloud seguente al codice completato. <p>populateRequiredOnNonDefaultProperties: true</p>
Crittografato	Quando si seleziona questa opzione, il valore immesso nel modulo di richiesta e nella successiva distribuzione viene nascosto. Le proprietà crittografate non possono avere un valore predefinito.

Sola lettura	Valore non modificabile ma visibile nel modulo di richiesta. Richiede un valore predefinito.
Altre opzioni	Opzioni che variano in base al tipo di proprietà. Espandere il menu a discesa, aggiungere eventuali impostazioni aggiuntive e fare clic su Crea .

Nell'esempio che segue, la proprietà che viene aggiunta rappresenta l'immagine del sistema operativo e l'utente richiedente può scegliere tra due opzioni.

Nota I sistemi operativi mostrati nella figura di esempio devono già far parte dell'infrastruttura di Cloud Assembly configurata.

New Property

Name *

Display Name

Description

Type ☒ STRING ☐ INTEGER ☐ NUMBER ☐ BOOLEAN ☐ OBJECT ☐ ARRAY

Default value

Encrypted ☐

Read-only ☐ ⓘ

More Options

Format

Minimum length

Maximum length

Pattern

Pairs ☒ Values ☐ Key Values

Enum

Value

5 Aggiungere altre proprietà al gruppo e fare clic su **Salva** al termine dell'operazione.

Properties 2 items

Add at least one property in order to create a property group

+ NEW PROPERTY
x DELETE

<input type="checkbox"/>	Name	Display Name	Type	Default Value
<input type="checkbox"/>	image	Machine Image	string	coreos
<input type="checkbox"/>	flavor	Machine Flavor	string	small

Aggiunta del gruppo di proprietà agli input del modello cloud

Anche nel caso di un lungo elenco di input di proprietà, è sufficiente aggiungere solo il gruppo di proprietà per fare in modo che tutte le proprietà vengano inserite nel modulo di richiesta.

- 1 Nella pagina di progettazione del modello cloud, sopra l'area di modifica a destra, fare clic sulla scheda **Input**.
- 2 Fare clic su **Nuovo input modello cloud**.
- 3 Specificare un nome e inserire una descrizione del gruppo di proprietà.

Nome	Immettere un nome simile al nome del gruppo di proprietà creato in precedenza.
Nome visualizzato	Immettere la stessa intestazione creata in precedenza per l'intero gruppo di proprietà, che verrà visualizzata nel modulo di richiesta.
Tipo	Selezionare Oggetto .
Tipo di oggetto	Selezionare Gruppo di proprietà .
Elenco dei gruppi di proprietà	Selezionare il gruppo di proprietà desiderato. Vengono visualizzati solo i gruppi di proprietà creati e disponibili per il progetto. Si noti che i gruppi di proprietà costanti non vengono visualizzati.

New Cloud Template Input

Name *

Display Name

Description

Type

STRING INTEGER NUMBER BOOLEAN **OBJECT** ARRAY

Select Object Type ☐ Properties ☒ Property Groups

Select from the existing property groups

Search

Name	Description
<input checked="" type="radio"/> machine	

4 Fare clic su **Crea**.

Il processo crea per gli input del modello cloud un codice simile a quello illustrato nell'esempio seguente.

```
inputs:
  pgmachine:
    type: object
    title: Machine Properties
    $ref: /ref/property-groups/machine
  pgrequester:
    type: object
    title: Requester Details
    $ref: /ref/property-groups/requesterDetails
```

È inoltre possibile immettere codice direttamente nella pagina di progettazione di Cloud Assembly e sfruttare i suggerimenti automatici mentre si digita `$ref: /ref/p...` nell'editor di codice.

Associazione delle risorse del modello cloud al gruppo di proprietà

Per utilizzare i valori di input del gruppo di proprietà, aggiungere binding sotto la risorsa.

In base al tipo di valori contenuti in un gruppo di proprietà, è possibile che si desideri farvi riferimento singolarmente. È possibile immettere i valori separatamente, in base al nome del gruppo di proprietà e al nome della proprietà.

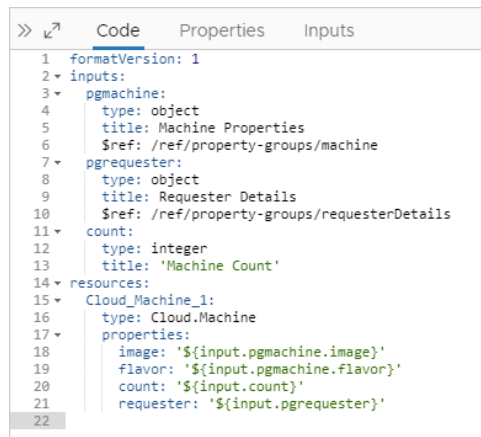
```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: '${input.pgmachine.image}'
      flavor: '${input.pgmachine.flavor}'
```

È inoltre possibile aggiungere rapidamente un intero set di valori a una risorsa facendo riferimento a un intero gruppo di proprietà.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      requester: '${input.pgrequester}'
```

Codice completato

Dopo aver completato l'inserimento di input e le risorse, il codice completato è simile all'esempio seguente.



```
>> Code Properties Inputs
1 formatVersion: 1
2 inputs:
3   pgmachine:
4     type: object
5     title: Machine Properties
6     $ref: /ref/property-groups/machine
7   pgrequester:
8     type: object
9     title: Requester Details
10    $ref: /ref/property-groups/requesterDetails
11  count:
12    type: integer
13    title: 'Machine Count'
14  resources:
15    Cloud_Machine_1:
16      type: Cloud.Machine
17      properties:
18        image: '${input.pgmachine.image}'
19        flavor: '${input.pgmachine.flavor}'
20        count: '${input.count}'
21        requester: '${input.pgrequester}'
22
```

Alla richiesta di distribuzione, i gruppi di proprietà vengono visualizzati affinché l'utente richiedente li completi.

Deployment Inputs

Machine Properties

Machine Image

coreos

▼

Machine Flavor

small

▼

Requester Details

Email

Mobile

Internal account?

☐

PIN

Account Type

User

Machine Count *

Gruppi di proprietà nell'editor moduli personalizzati di Service Broker

I gruppi di proprietà di input vengono visualizzati nell'interfaccia del modulo personalizzato di Service Broker e possono essere personalizzati. Non esistono considerazioni speciali da fare sui gruppi di proprietà quando li si personalizza. Gli utenti di Service Broker possono anche non sapere che l'origine delle immissioni è un gruppo di proprietà anziché proprietà create separatamente.

The screenshot shows the 'General' tab of a vRealize Automation Cloud Assembly form. It features two highlighted groups of input properties:

- Machine Properties:** Includes 'Machine Image' and 'Machine Flavor', both represented as dropdown menus.
- Requester Details:** Includes 'Email', 'Mobile' (text inputs), 'Internal account?' (checkbox), 'PIN' (text input), and 'Account Type' (dropdown menu).

Per ulteriori informazioni, vedere [Personalizzazione di un'icona e del modulo di richiesta di Service Broker](#).

Azioni di vRealize Orchestrator in un gruppo di proprietà di input

In un gruppo di proprietà di input di Cloud Assembly, è possibile aggiungere l'interazione dinamica con vRealize Orchestrator.

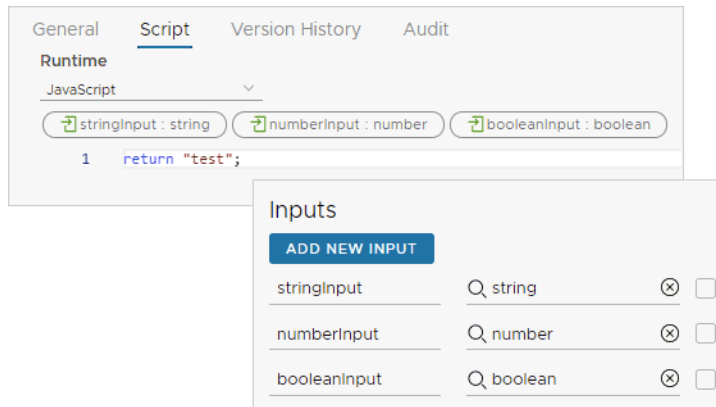
Aggiunta di un'azione di vRealize Orchestrator a un gruppo di proprietà di input

Per aggiungere l'interazione dinamica con vRealize Orchestrator a un gruppo di proprietà di input, attenersi alle linee guida seguenti.

- 1 Nell'istanza di vRealize Orchestrator integrata in vRealize Automation, creare un'azione che esegua l'operazione desiderata.

L'azione di vRealize Orchestrator può includere solo tipi stringa, numero intero, numero e valori booleani primitivi. I tipi di vRealize Orchestrator non sono supportati.

In questo semplice esempio, l'azione di vRealize Orchestrator raccoglie tre input e restituisce una stringa hardcoded.



- 2 In Cloud Assembly, avviare il processo di creazione o modifica di un gruppo di proprietà di input. Vedere [Gruppi di proprietà di input in Cloud Assembly](#) se necessario.
- 3 Per aggiungere gli input di azione di vRealize Orchestrator a un gruppo di proprietà, aggiungere nuove proprietà, fare clic sul tipo, quindi fare clic su **Costante**.
Aggiungere separatamente ogni input di azione di vRealize Orchestrator.

The screenshot shows the 'New Property' form. It has fields for 'Name' (set to 'numberInput'), 'Display Name' (set to 'Number for VRO'), and 'Description'. Below these is a 'Type' section with a row of buttons: 'STRING', 'INTEGER', 'NUMBER', 'BOOLEAN', 'OBJECT', and 'ARRAY'. The 'NUMBER' button is highlighted with an orange arrow. Below the 'Type' section is a 'Default value source' section with two radio buttons: 'Constant' (selected) and 'External source'. An orange arrow points to the 'Constant' radio button. At the bottom is a 'Default value' field.

- 4 Dopo aver aggiunto gli input, aggiungere una nuova proprietà, fare clic sul tipo, fare clic su **Origine esterna**, quindi fare clic su **Seleziona**.

New Property

Name *

Display Name

Description

Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Default value source ☐ Constant ☒ External source

Action

- 5 In **Azione**, cercare e selezionare l'azione di vRealize Orchestrator creata, quindi fare clic su **Salva**.

Add an existing action

Action *

☒ returnSimpleAction
com.form.service.test

- 6 Salvare il gruppo di proprietà e aggiungerlo al modello cloud. Vedere [Gruppi di proprietà di input in Cloud Assembly](#) se necessario.

Quando si distribuisce il modello cloud, il gruppo di proprietà dell'azione di vRealize Orchestrator viene visualizzato nel modulo di input per l'utente richiedente.

Values for VRO

String for VRO

VRO Action

Number for VRO

On-Off for VRO

test

☐

Valori predefiniti configurabili

Per compilare il modulo di input con valori predefiniti, eseguire una delle operazioni seguenti quando si aggiunge l'azione di vRealize Orchestrator come origine esterna.

- Specificare manualmente il valore della proprietà predefinita.

Deselezionare l'opzione **Associa** e immettere il valore.

Add an existing action

Action *

Action Parameters

Input

Q com.form.service.test/Action

Readme

☐ Bind

- Utilizzare un altro valore di proprietà dello stesso gruppo di proprietà.

Selezionare l'opzione **Associa** e selezionare una proprietà nell'elenco a discesa.

Add an existing action

Action *

Action Parameters

Input

Q com.form.service.test/Action

Canvas fields

Hard String

Input String

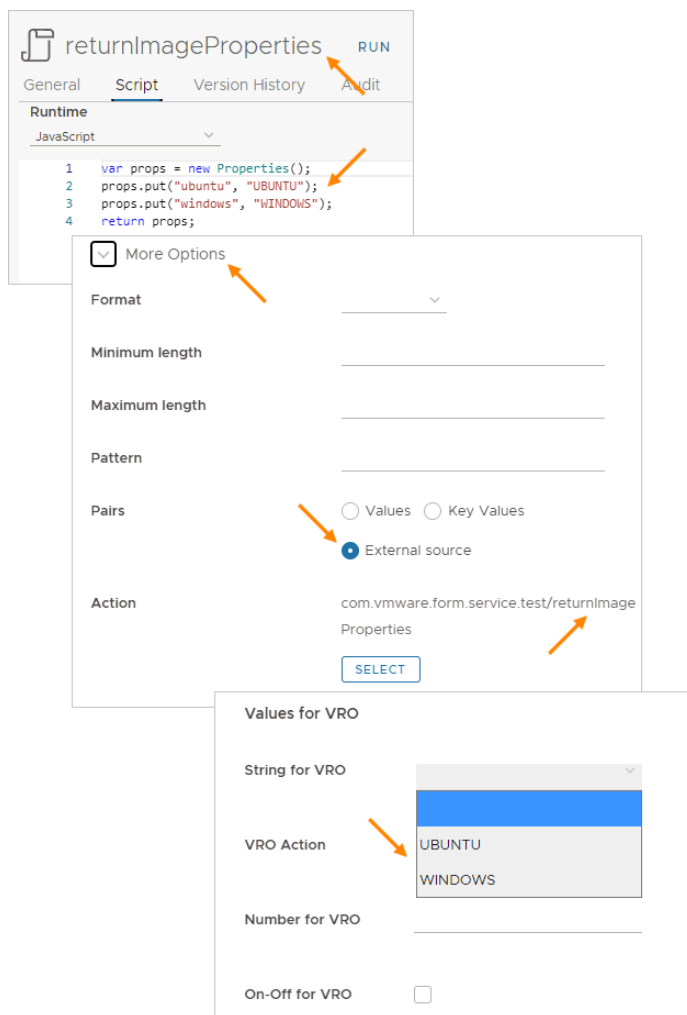
☒ Bind

Aggiunta di selezioni di input enumerate di vRealize Orchestrator

Per creare un elenco di selezione basato su vRealize Orchestrator in un modulo di input, procedere come segue durante l'aggiunta a un gruppo di proprietà.

- 1 In vRealize Orchestrator, creare un'azione che mappi i valori desiderati per l'elenco.
- 2 In Cloud Assembly, quando si aggiunge una proprietà al gruppo, espandere **Altre opzioni**.
- 3 Per **Coppie**, fare clic su **Origine esterna**, fare clic su **Seleziona** e aggiungere l'azione di vRealize Orchestrator creata.

Nota Se si crea anche un valore predefinito quando si aggiunge la proprietà, tale valore predefinito deve corrispondere esattamente a uno dei valori enumerati dall'azione di vRealize Orchestrator.



Gruppi di proprietà costanti in Cloud Assembly

Le costanti di Cloud Assembly consentono di applicare coppie chiave-valore note alle progettazioni in modo invisibile all'utente.

Funzionamento delle costanti

La chiave viene visualizzata nel codice del modello cloud e il valore diventa parte delle distribuzioni basate su tale modello cloud. Le costanti richiedono il binding di `propgroup` sotto la risorsa.

Il binding di `propgroup` viene utilizzato solo con gruppi di proprietà costanti, non con gruppi di proprietà di input.

Proprietà segrete

Se si prevede di aggiungere una proprietà segreta a un gruppo di proprietà, creare la proprietà segreta prima di procedere. Vedere [Proprietà di Cloud Assembly segrete](#).

Creazione del gruppo di proprietà costanti

- 1 Passare a **Progettazione > Gruppi di proprietà** e fare clic su **Nuovo gruppo di proprietà**.
- 2 Selezionare **Valori costanti**.
- 3 Specificare un nome e inserire una descrizione per il nuovo gruppo di proprietà.

Nome	I nomi dei gruppi di proprietà devono essere univoci all'interno di una determinata organizzazione. Sono consentiti solo lettere, numeri e caratteri di sottolineatura.
Nome visualizzato	Lasciare vuoto. Nel modulo di richiesta non viene visualizzata alcuna intestazione.
Descrizione	Descrivere l'uso a cui è destinato questo set di costanti.
Scope	<p>Stabilire se un amministratore può condividere il gruppo di proprietà con l'intera organizzazione. In caso contrario, un solo progetto potrà accedere al gruppo di proprietà.</p> <p>Anche se è sempre possibile aggiungere o modificare proprietà nel gruppo, l'ambito è permanente e non può essere modificato in un secondo momento.</p> <p>Segreti: se si prevede di aggiungere una proprietà segreta al gruppo di proprietà, è necessario utilizzare un singolo ambito del progetto. Le proprietà segrete vengono salvate solo a livello di progetto.</p>
Progetto	Quando l'ambito è solo di un progetto, questo progetto può accedere al gruppo di proprietà.

- 4 Per aggiungere una proprietà costante al gruppo, fare clic su **Nuova proprietà**.
- 5 Immettere un nome che rappresenti la chiave e una descrizione.
- 6 Selezionare un tipo di proprietà.
- 7 Immettere il valore costante desiderato e fare clic su **Crea**.
 - I tipi stringa, numero intero e numero utilizzano l'immissione diretta.

- Per un valore di stringa segreta, selezionare nell'elenco delle proprietà segrete per il progetto.
- Il tipo booleano utilizza una casella di selezione per indicare true.
- Per il tipo di oggetto o array, sostituire `null` con il valore desiderato.

New Property

Name *

Description

Type

STRING INTEGER NUMBER BOOLEAN OBJECT ARRAY

Select Type ☒ Constant value ☐ Secret

Constant value

New Property [X]

Name *

Description

Type

STRING **INTEGER** NUMBER BOOLEAN OBJECT ARRAY

Select Type ☐ Constant value ☒ Secret

Search

	Name	Description
<input checked="" type="radio"/>	AccountNumber	
<input type="radio"/>	password	
<input type="radio"/>	RemoteAccessKey1	

7 secrets

- 8 Aggiungere altre costanti al gruppo e fare clic su **Salva** al termine dell'operazione.

Properties 3 items

Add at least one property in order to create a property group

[+ NEW PROPERTY](#) [X DELETE](#)

<input type="checkbox"/>	Name	Display Name	Type	Constant Value
<input type="checkbox"/>	payerFederal		boolean	true
<input type="checkbox"/>	payerCostCenter		integer	7890
<input type="checkbox"/>	payerAccountNumber		string	123456

Associazione delle risorse del modello cloud al gruppo di proprietà

Per utilizzare i valori costanti in una risorsa in modo invisibile all'utente, aggiungere binding `propgroup` nella risorsa.

È possibile aggiungere rapidamente un intero set di costanti a una risorsa facendo riferimento al gruppo di proprietà stesso.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      payerInfo: '${propgroup.payerDetails}'
```

In alternativa, è possibile aggiungere singole costanti del gruppo di proprietà a parti selezionate della progettazione.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      payerAccount: '${propgroup.payerDetails.payerAccountNumber}'
      payerCost: '${propgroup.payerDetails.payerCostCenter}'
      payerFed: '${propgroup.payerDetails.payerFederal}'
```

Ulteriori informazioni sui gruppi di proprietà di Cloud Assembly

Un gruppo di proprietà di Cloud Assembly può essere incluso in molti modelli cloud e ciò influisce sulla modalità di gestione dei gruppi di proprietà.

Modifica di un gruppo di proprietà

Le modifiche apportate a un gruppo di proprietà Cloud Assembly influiscono su ogni modello cloud che lo utilizza. Inoltre, quando viene rilasciata la versione modificata del modello cloud, tali modifiche influiscono ora sugli utenti del catalogo di Service Broker.

Nell'elenco dei gruppi di proprietà e nelle pagine di modifica dei gruppi di proprietà è indicato il numero di modelli cloud che includono il gruppo di proprietà. Per visualizzare quali modello cloud saranno interessati da una modifica, fare clic sul numero.

The screenshot displays the 'Property Groups' management interface. At the top, there's a header 'Property Groups' with a count of '61 items' and a filter icon. Below this are buttons for '+ NEW PROPERTY GROUP' and 'x DELETE', along with a search bar labeled 'Filter...'. A table lists the property groups:

	Name	Type	Properties	Cloud Templates	Last Updated
<input type="radio"/>	machine	Input	2	2 ←	Apr 29, 2021, 4:26:18 PM
<input type="radio"/>	mh_const	Constant	5	1	Apr 27, 2021, 5:29:33 PM

An orange arrow points from the 'Cloud Templates' column of the 'machine' group to a detailed view of its 'Cloud Templates' and 'Properties'.

The detailed view shows 'Cloud Templates' with a count of '2' and an orange arrow. Below it, the 'Properties' section has a count of '2 items' and a message: 'Add at least one property in order to create a property group'. It includes buttons for '+ NEW PROPERTY' and 'x DELETE'. A table lists the properties:

<input type="checkbox"/>	Name	Display Name	Type	Default Value
<input type="checkbox"/>	image	Machine Image	string	coreos
<input type="checkbox"/>	flavor	Machine Flavor	string	small

Prima di modificare un gruppo di proprietà, assicurarsi che la modifica sia accettabile per tutti coloro che creano o aggiornano distribuzioni in base ai modelli cloud elencati.

Eliminazione di un gruppo di proprietà

L'eliminazione di un gruppo di proprietà causerebbe errori in ogni modello cloud che lo utilizza.

Non è possibile eliminare un gruppo di proprietà finché non lo si rimuove manualmente da tutti i modelli cloud in cui è incluso. Per rimuovere un gruppo di proprietà da un modello cloud, aprire il modello cloud nella tela di progettazione.

- Gruppi di proprietà di input

Nella scheda Input, selezionare e rimuovere il gruppo di proprietà. In alternativa, utilizzare l'editor di codice per eliminare il gruppo di proprietà associato nella sezione `inputs` del codice.

- Gruppi di proprietà costanti

Utilizzare l'editor di codice per eliminare la voce o le voci `propgroup` associate nella sezione `resources` del codice.

Nota Non è possibile eliminare un gruppo di proprietà se è incluso in un modello cloud con versione. I modelli cloud con versione sono in sola lettura.

Contrassegni di risorsa di Cloud Assembly per le richieste

Cloud Assembly include diverse impostazioni dei modelli cloud che regolano le modalità di gestione di una risorsa al momento della richiesta.

Le impostazioni del contrassegno di risorsa non fanno parte dello schema delle proprietà dell'oggetto risorsa. Per una determinata risorsa, aggiungere le impostazioni del contrassegno all'esterno della sezione delle proprietà come mostrato.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    preventDelete: true
    properties:
      image: coreos
      flavor: small
      attachedDisks:
        - source: '${resource.Cloud_Volume_1.id}'
  Cloud_Volume_1:
    type: Cloud.Volume
    properties:
      capacityGb: 1
```

Contrassegno di risorsa	Descrizione
allocatePerInstance	<p>Impostata su true. L'allocazione delle risorse può essere personalizzata per ogni macchina in un cluster. Se si utilizza l'estendibilità, true causa l'esecuzione ripetuta dell'argomento dell'evento di estendibilità <code>compute.allocation.pre</code> quando si distribuisce più di una macchina cloud.</p> <p>L'impostazione predefinita è false, che alloca le risorse in modo uniforme all'interno del cluster, il che determina la stessa configurazione per ogni macchina. Inoltre, le azioni giorno 2 potrebbero non essere possibili separatamente per le singole risorse.</p> <p>L'allocazione per istanza consente a <code>count.index</code> di applicare correttamente la configurazione per le singole macchine. Per gli esempi di codice , vedere Cluster di macchine e dischi in Cloud Assembly .</p>
createBeforeDelete	<p>Alcune azioni di aggiornamento richiedono che la risorsa esistente venga rimossa e ne venga creata una nuova. Per impostazione predefinita, la rimozione è la prima, che può causare condizioni in cui la risorsa precedente è stata eliminata, ma la nuova non è stata creata per qualche motivo.</p> <p>Impostare questo contrassegno su true se è necessario assicurarsi che la nuova risorsa sia stata creata correttamente prima di eliminare quella precedente.</p>

Contrassegno di risorsa	Descrizione
createTimeout	<p>Il timeout predefinito di Cloud Assembly per le richieste di allocazione, creazione e pianificazione delle risorse è di 2 ore (2h). Inoltre, un amministratore di progetto può impostare un timeout predefinito personalizzato per queste richieste, applicabile all'intero progetto.</p> <p>Questo contrassegno consente di sovrascrivere qualsiasi valore predefinito e impostare il timeout individuale per un'operazione di risorsa specifica. Vedere anche <code>updateTimeout</code> e <code>deleteTimeout</code>.</p>
deleteTimeout	<p>Il timeout predefinito di Cloud Assembly per le richieste di eliminazione è di 2 ore (2h). Inoltre, un amministratore di progetto può impostare un timeout predefinito diverso per le richieste di eliminazione, applicabili all'intero progetto.</p> <p>Questo contrassegno consente di sovrascrivere qualsiasi valore predefinito e impostare il timeout individuale per un'operazione di eliminazione di una risorsa specifica. Vedere anche <code>updateTimeout</code> e <code>createTimeout</code>.</p>
dependsOn	<p>Questo contrassegno identifica una dipendenza esplicita tra le risorse, in cui una risorsa deve esistere prima di creare quella successiva. Per ulteriori informazioni, vedere Creazione di binding e dipendenze tra le risorse in Cloud Assembly.</p>
dependsOnPreviousInstances	<p>Se impostata su <code>true</code>, crea le risorse del cluster in sequenza. L'impostazione predefinita è <code>false</code>, che crea simultaneamente tutte le risorse in un cluster.</p> <p>Ad esempio, la creazione sequenziale è utile per i cluster di database in cui è necessario creare nodi primari e secondari, ma la creazione di un nodo secondario richiede impostazioni di configurazione che connettano il nodo a un nodo primario esistente.</p>
forceRecreate	<p>Non tutte le azioni di aggiornamento richiedono che la risorsa esistente venga rimossa e ne venga creata una nuova. Se si desidera che un aggiornamento rimuova la risorsa precedente e ne crei una nuova, indipendentemente dal fatto che l'aggiornamento lo abbia fatto per impostazione predefinita, impostare questo contrassegno su <code>true</code>.</p>
ignoreChanges	<p>Gli utenti di una risorsa potrebbero riconfigurarla, modificando la risorsa dal suo stato distribuito.</p> <p>Se si desidera eseguire un aggiornamento della distribuzione ma non sovrascrivere la risorsa modificata con la configurazione del modello cloud, impostare questo contrassegno su <code>true</code>.</p>

Contrassegno di risorsa	Descrizione
ignorePropertiesOnUpdate	<p>Gli utenti di una risorsa possono personalizzare determinate proprietà e tali proprietà potrebbero essere reimpostate nello stato del modello cloud originale durante un'azione di aggiornamento.</p> <p>Per impedire che le proprietà vengano reimpostate da un'azione di aggiornamento, impostare questo contrassegno su true.</p>
preventDelete	<p>Se è necessario proteggere una risorsa creata dall'eliminazione accidentale durante gli aggiornamenti, impostare questo contrassegno su true. Se un utente elimina la distribuzione, tuttavia, la risorsa viene eliminata.</p>
recreatePropertiesOnUpdate	<p>Gli utenti di una risorsa potrebbero riconfigurare le proprietà modificando la risorsa dal suo stato distribuito. Durante un aggiornamento, una risorsa può essere ricreata o meno. Le risorse che non sono state ricreate potrebbero rimanere con le proprietà in stati modificati.</p> <p>Se si desidera ricercare una risorsa e le sue proprietà, indipendentemente dal fatto che l'aggiornamento lo abbia fatto per impostazione predefinita, impostare questo contrassegno su true.</p>
updateTimeout	<p>Il timeout predefinito di Cloud Assembly per le richieste di aggiornamento è di 2 ore (2h). Inoltre, un amministratore di progetto può impostare un timeout predefinito diverso per le richieste di aggiornamento, applicabili all'intero progetto.</p> <p>Questo contrassegno consente di sovrascrivere qualsiasi valore predefinito e impostare il timeout individuale per un'operazione di aggiornamento di una risorsa specifica. Vedere anche deleteTimeout e createTimeout.</p>

Espressioni di Cloud Assembly

Per una maggiore flessibilità, è possibile aggiungere espressioni al codice del modello cloud di Cloud Assembly.

Funzionamento delle espressioni

Le espressioni di Cloud Assembly utilizzano il costrutto `${expression}`, come illustrato negli esempi seguenti.

Nota Le espressioni Cloud Assembly non sono uguali alle espressioni regolari. Vedere la [Sintassi dell'espressione Cloud Assembly](#) per Cloud Assembly.

I seguenti esempi di codice sono stati tagliati in modo da mostrare solo le righe importanti. L'intero modello cloud non modificato è disponibile alla fine.

Esempi

Al momento della distribuzione, consentire all'utente di incollare la chiave crittografata necessaria per l'accesso remoto:

```
inputs:
  sshKey:
    type: string
    maxLength: 500
resources:
  frontend:
    type: Cloud.Machine
    properties:
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
```

Per la distribuzione di VMware Cloud on AWS, impostare il nome della cartella sul nome richiesto del *Carico di lavoro*:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
```

Al momento della distribuzione, assegnare alla macchina un tag *env* tutto minuscolo che corrisponda all'ambiente selezionato:

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
resources:
  frontend:
```

```

type: Cloud.Machine
properties:
  constraints:
    - tag: '${"env:" + to_lower(input.environment)}'

```

Impostare il numero di macchine nel cluster front-end su uno (piccolo) o due (grande). Si noti che il cluster grande è impostato tramite processo di eliminazione:

```

inputs:
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      count: '${input.envsize == "Small" ? 1 : 2}'

```

Collegare le macchine alla stessa rete *Predefinita* associandole alla proprietà trovata nella risorsa di rete:

```

resources:
  frontend:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
  Cloud_Network_1:
    type: Cloud.Network
    properties:
      name: Default
      networkType: existing

```

Crittografare le credenziali di accesso inviate all'API:

```

resources:
  apitier:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        #cloud-config
        runcmd:
          - export apikey=${base64_encode(input.username:input.password)}
          - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com

```

Individuare l'indirizzo della macchina API:

```
resources:
  frontend:
    type: Cloud.Machine
    properties:
      cloudConfig: |
        runcmd:
          - echo ${resource.apitier.networks[0].address}
  apitier:
    type: Cloud.Machine
    properties:
      networks:
        - network: '${resource.Cloud_Network_1.name}'
```

Modello cloud completo

```
inputs:
  environment:
    type: string
    enum:
      - AWS
      - vSphere
      - Azure
      - VMC
      - GCP
    default: vSphere
  sshKey:
    type: string
    maxLength: 500
  envsize:
    type: string
    enum:
      - Small
      - Large
resources:
  frontend:
    type: Cloud.Machine
    properties:
      folderName: '${input.environment == "VMC" ? "Workload" : ""}'
      image: ubuntu
      flavor: medium
      count: '${input.envsize == "Small" ? 1 : 2}'
      remoteAccess:
        authentication: publicPrivateKey
        sshKey: '${input.sshKey}'
      cloudConfig: |
        packages:
          - nginx
        runcmd:
          - echo ${resource.apitier.networks[0].address}
      constraints:
        - tag: '{"env:" + to_lower(input.environment)}'
    networks:
```



```

    - network: '${resource.Cloud_Network_1.name}'
apitier:
  type: Cloud.Machine
  properties:
    folderName: '${input.environment == "VMC" ? "Workload" : ""}'
    image: ubuntu
    flavor: small
    cloudConfig: |
      #cloud-config
      runcmd:
        - export apikey=${base64_encode(input.username:input.password)}
        - curl -i -H 'Accept:application/json' -H 'Authorization:Basic :$apikey' http://
example.com
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: '${input.sshKey}'
  constraints:
    - tag: '${"env:" + to_lower(input.environment)}'
  networks:
    - network: '${resource.Cloud_Network_1.name}'
Cloud_Network_1:
  type: Cloud.Network
  properties:
    name: Default
    networkType: existing
  constraints:
    - tag: '${"env:" + to_lower(input.environment)}'

```

Sintassi dell'espressione Cloud Assembly

La sintassi dell'espressione espone tutte le funzionalità disponibili delle espressioni nei modelli Cloud Assembly.

Nota Le espressioni Cloud Assembly non sono uguali alle espressioni regolari.

La seguente sintassi è rappresentata solo in parte negli esempi illustrati in [Espressioni di Cloud Assembly](#).

Valori letterali

Sono supportati i valori letterali seguenti:

- Booleano (true o false)
- Intero
- Virgola mobile
- Stringa

La barra rovesciata esegue l'escape delle virgolette doppie, delle virgolette singole e della barra rovesciata stessa:

" con escape diventa \"

' con escape diventa \'

\ con escape diventa \\

Le virgolette devono essere sottoposte a escape solo all'interno di una stringa racchiusa dallo stesso tipo di virgolette, come illustrato nel seguente esempio.

```
"I am a \"double quoted\" string inside \"double quotes\"."
```

- Null

Variabili di ambiente

Nomi di ambiente:

- orgId
- projectId
- projectName
- deploymentId
- deploymentName
- blueprintId
- blueprintVersion
- blueprintName
- requestedBy (utente)
- requestedAt (ora)

Sintassi:

```
env.ENV_NAME
```

Esempio:

```
${env.blueprintId}
```

Variabili di risorsa

Le variabili di risorsa consentono di eseguire il binding alle proprietà delle risorse da altre risorse.

Sintassi:

```
resource.RESOURCE_NAME.PROPERTY_NAME
```

I nomi delle risorse non possono contenere trattini né punti. I caratteri di sottolineatura sono consentiti.

Esempi:

- \${resource.db.id}

- `${resource.db.networks[0].address}`
- `${resource.app.id}` (restituisce la stringa per le risorse non in cluster, dove il conteggio non è specificato. Restituisce la matrice per le risorse in cluster.)
- `${resource.app[0].id}` (restituisce la prima voce per le risorse in cluster.)

Variabili autonome delle risorse

Le variabili autonome delle risorse sono consentite solo per le risorse che supportano la fase di allocazione. Le variabili autonome delle risorse sono disponibili (o hanno un valore impostato) solo dopo il completamento della fase di allocazione.

Sintassi:

```
self.property_name
```

Esempio:

```
${self.address} (restituisce l'indirizzo assegnato durante la fase di allocazione.)
```

Si noti che per una risorsa denominata `resource_x`, `self.property_name` e `resource.resource_x.property_name` sono uguali e sono entrambi considerati come autoriferimenti.

Condizioni

Sintassi:

- Gli operatori di uguaglianza sono `==` e `!=`.
- Gli operatori relazionali sono `<` `>` `<=` e `>=`.
- Gli operatori logici sono `&&` `||` e `!`.
- Le istruzioni condizionali utilizzano il modello:
condition-expression ? true-expression : false-expression

Esempi:

```
${input.count < 5 && input.size == 'small'}
```

```
${input.count < 2 ? "small":"large"}
```

Indice di conteggio cluster

Sintassi:

```
count.index
```

Esempi:

- Restituisce il tipo di nodo per le risorse in cluster:
`${count.index == 0 ? "primary":"secondary"}`

- Impostare la dimensione di ciascun disco durante l'allocazione:

```
inputs:
  disks:
    type: array
    minItems: 0
    maxItems: 12
    items:
      type: object
      properties:
        size:
          type: integer
          title: Size (GB)
          minSize: 1
          maxSize: 2048
resources:
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    allocatePerInstance: true
    properties:
      capacityGb: '${input.disks[count.index].size}'
      count: '${length(input.disks)}'
```

- Per ulteriori esempi, vedere [Cluster di macchine e dischi in Cloud Assembly](#).

Operatori aritmetici

Sintassi:

Gli operatori sono + - / * e %.

Esempio:

```
${(input.count + 5) * 2}
```

Concatenazione di stringhe

Sintassi:

```
${'ABC' + 'DEF'} restituisce ABCDEF.
```

Operatori [] e .

L'espressione segue ECMAScript nell'unificazione del trattamento degli operatori [] e .

Quindi, `expr.identifier` è equivalente a `expr["identifier"]`. L'identificatore viene utilizzato per costruire un valore letterale il cui valore è l'identificatore. L'operatore [] viene quindi utilizzato con tale valore.

Esempio:

```
${resource.app.networks[0].address}
```

Inoltre, quando una proprietà include uno spazio, delimitarlo con parentesi quadre e virgolette doppie anziché utilizzare la notazione dei punti.

Non corretto:

```
input.operating system
```

Corretto:

```
input["operating system"]
```

Costruzione della mappa

Sintassi:

```
${{'key1':'value1', 'key2':input.key2}}
```

Costruzione della matrice

Sintassi:

```
${['key1','key2']}
```

Esempio:

```
${[1,2,3]}
```

Funzioni

Sintassi:

```
${function(arguments...)}
```

Esempio:

```
${to_lower(resource.app.name)}
```

Tabella 6-1. Funzioni

Funzione	Descrizione
abs(number)	Valore numerico assoluto
avg(array)	Restituisce la media di tutti i valori della matrice di numeri
base64_decode(string)	Restituisce il valore base64 decodificato
base64_encode(string)	Restituisce il valore base64 codificato
ceil(number)	Restituisce il valore più piccolo (più vicino a infinito negativo) maggiore o uguale all'argomento e uguale a un numero intero matematico
contains(array, value)	Controlla se la matrice contiene un valore
contains(string, value)	Controlla se la stringa contiene un valore
digest(value, type)	Restituisce il digest del valore utilizzando il tipo supportato (md5, sha1, sha256, sha384, sha512)
ends_with(subject, suffix)	Controlla se la stringa dell'oggetto finisce con la stringa di un prefisso

Tabella 6-1. Funzioni (continua)

Funzione	Descrizione
<code>filter_by(array, filter)</code>	Restituisce solo le voci di array che superano l'operazione di filtro <code>filter_by([1,2,3,4], x => x >= 2 && x <= 3)</code> restituisce <code>[2, 3]</code> <code>filter_by({'key1':1, 'key2':2}, (k,v) => v != 1)</code> restituisce <code>[{"key2": 2}]</code>
<code>floor(number)</code>	Restituisce il valore più grande (più vicino a infinito positivo) minore o uguale all'argomento e uguale a un numero intero matematico
<code>format(format, values...)</code>	Restituisce una stringa formattata utilizzando il formato e i valori di Class Formatter di Java.
<code>from_json(string)</code>	Analizza la stringa JSON
<code>join(array, delim)</code>	Unisce la matrice di stringhe con un delimitatore e restituisce una stringa
<code>json_path(value, path)</code>	Valuta il percorso rispetto al valore utilizzando XPath for JSON .
<code>keys(map)</code>	Restituisce le chiavi della mappa
<code>length(array)</code>	Restituisce la lunghezza della matrice
<code>length(string)</code>	Restituisce la lunghezza della stringa
<code>map_by(array, operation)</code>	Restituisce ogni voce di array con un'operazione applicata <code>map_by([1,2], x => x * 10)</code> restituisce <code>[10, 20]</code> <code>map_by([1,2], x => to_string(x))</code> restituisce <code>["1", "2"]</code> <code>map_by({'key1':1, 'key2':2}, (k,v) => {k:v*10})</code> restituisce <code>[{"key1":10}, {"key2":20}]</code>
<code>map_to_object(array, keyname)</code>	Restituisce un array di coppie key:value del nome della chiave specificato associato ai valori di un altro array <code>map_to_object(resource.Disk[*].id, "source")</code> restituisce un array di coppie key:value con un campo di chiave denominato source associato a stringhe di ID disco Si noti che <code>map_by(resource.Disk[*].id, id => {'source':id})</code> restituisce lo stesso risultato
<code>matches(string, regex)</code>	Verifica se la stringa corrisponde a un'espressione regex
<code>max(array)</code>	Restituisce il valore massimo della matrice di numeri
<code>merge(map, map)</code>	Restituisce una mappa unita
<code>min(array)</code>	Restituisce il valore minimo della matrice di numeri
<code>not_null(array)</code>	Restituisce la prima voce che non è null
<code>now()</code>	Restituisce l'ora corrente in formato ISO-8601

Tabella 6-1. Funzioni (continua)

Funzione	Descrizione
range(start, stop)	Restituisce una serie di numeri in incrementi di 1 che inizia con il numero iniziale e termina subito prima del numero finale
replace(string, target, replacement)	Sostituisce la stringa contenente la stringa di destinazione con la stringa di destinazione
reverse(array)	Inverte le voci della matrice
slice(array, begin, end)	Restituisce una sezione della matrice dall'indice iniziale all'indice finale
split(string, delim)	Divide la stringa con un delimitatore e restituisce una matrice di stringhe
starts_with(subject, prefix)	Controlla se la stringa dell'oggetto inizia con la stringa di un prefisso
substring(string, begin, end)	Restituisce la sottostringa della stringa dall'indice iniziale all'indice finale
sum(array)	Restituisce la somma di tutti i valori della matrice di numeri
to_json(value)	Serializza il valore come stringa JSON
to_lower(str)	Converte la stringa in lettere minuscole
to_number(string)	Analizza la stringa come numero
to_string(value)	Restituisce la rappresentazione stringa del valore
to_upper(str)	Converte la stringa in lettere maiuscole
trim(string)	Rimuove gli spazi iniziali e finali
url_encode(string)	Codifica la stringa utilizzando la specifica di codifica URL
uuid()	Restituisce l'UUID generato in modo casuale
values(map)	Restituisce i valori della mappa

Risoluzione dei problemi

Il linguaggio YAML utilizza i due punti e lo spazio (": ") come separatore tra chiave e valore nelle coppie chiave-valore. La sintassi dell'espressione dipende dal codice YAML. A volte, uno spazio dopo i due punti può causare un errore nell'espressione.

Ad esempio, lo spazio tra "win" : e "lin" nell'espressione seguente causa un errore.

```
${contains(input.image,"(Windows)" == true ? "win" : "lin")}
```

L'espressione in funzione omette lo spazio.

```
${contains(input.image,"(Windows)" == true ? "win" : "lin")}
```

Se un'espressione continua a non riuscire, provare a racchiudere l'intera espressione in un segno di graduazione come mostrato.

```
ezOS: '${contains(input.image,"(Windows)" == true ? "win" : "lin")}'
```

Proprietà di Cloud Assembly segrete

Una proprietà di Cloud Assembly segreta è un valore riutilizzabile e crittografato che gli utenti dei progetti possono aggiungere alle loro progettazioni di modelli cloud.

Le credenziali e le chiavi di accesso sicure sono tipici esempi di proprietà segrete. Una volta creato e salvato, il valore di una proprietà segreta non potrà mai più essere decrittografato o letto.

Creazione di una proprietà segreta

- 1 Accedere a Cloud Assembly con privilegi del ruolo di amministratore del progetto.
- 2 Passare a **Infrastruttura > Amministrazione > Segreti** e fare clic su **Nuovo segreto**.
- 3 Selezionare il progetto.
- 4 Immettere un nome di proprietà univoco per il segreto, senza spazi né caratteri speciali.
Il nome è l'identificatore visibile per il segreto.

- 5 Immettere il valore del segreto.

Quando si digita, il valore viene oscurato per impostazione predefinita, proteggendolo nel caso in cui lo schermo sia condiviso.

Se necessario, è possibile fare clic sul simbolo dell'occhio per rivelare e controllare un valore. Dopo che è stato salvato, tuttavia, un valore segreto viene crittografato nel database e non potrà mai più essere esposto.

- 6 Facoltativamente è possibile immettere una descrizione più lunga della proprietà segreta.
- 7 Fare clic su **Crea**.

Aggiunta di una proprietà segreta a un modello cloud

Gli utenti del progetto possono aggiungere una proprietà segreta come binding nel codice del modello cloud.

Si noti che iniziando a digitare i caratteri `'${secret.` viene rivelato l'elenco di selezione dei segreti creati per il progetto.

```
type: Cloud.Machine
properties:
  name: ourvm
  image: mint20
  flavor: small
  remoteAccess:
    authentication: publicPrivateKey
    sshKey: '${secret.ourPublicKey}'
    username: root
```

Per aggiungere una proprietà segreta a una configurazione Terraform, vedere [Utilizzo di una proprietà di Cloud Assembly segreta in una configurazione Terraform](#).

Accesso remoto a una distribuzione di Cloud Assembly

Per accedere in remoto a una macchina distribuita da Cloud Assembly, prima della distribuzione aggiungere le proprietà al modello cloud di tale macchina.

Per l'accesso remoto è possibile configurare una delle seguenti opzioni di autenticazione.

Nota Nei casi in cui è necessario copiare le chiavi, è anche possibile creare una sezione `cloudConfig` nel modello cloud per copiare automaticamente le chiavi al momento del provisioning. Le specifiche non sono documentate qui, ma [Inizializzazione della macchina in Cloud Assembly](#) fornisce informazioni generali su `cloudConfig`.

Generazione di una coppia di chiavi al momento del provisioning

Se non si dispone di una coppia di chiavi pubblica-privata per l'autenticazione dell'accesso remoto, Cloud Assembly è in grado di generarla.

Utilizzare il codice seguente come linea guida.

- 1 In Cloud Assembly, prima del provisioning, aggiungere proprietà `remoteAccess` al modello cloud come mostrato nell'esempio.

Il nome utente è facoltativo. Se viene omissso, il sistema genera un ID casuale come nome utente.

Esempio:

```
type: Cloud.Machine
properties:
  name: our-vm2
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: generatedPublicPrivateKey
    username: testuser
```

- 2 In Cloud Assembly, eseguire il provisioning della macchina dal relativo modello cloud e portarlo a uno stato di avvio.

Il processo di provisioning genera le chiavi.

- 3 Individuare il nome della chiave nelle proprietà **Risorse > Distribuzioni > Topologia**.
- 4 Utilizzare l'interfaccia del provider cloud, ad esempio il client di vSphere, per accedere alla riga di comando della macchina sottoposta a provisioning.
- 5 Concedere l'autorizzazione di lettura alla chiave privata.

```
chmod 600 key-name
```

- 6 Passare alla distribuzione di Cloud Assembly, selezionare la macchina e fare clic su **Azioni > Ottieni chiave privata**.

- 7 Copiare il file della chiave privata nella macchina locale.

Un percorso di file locale tipico è `/home/username/.ssh/key-name`.

- 8 Aprire una sessione SSH remota e connettersi alla macchina di cui è stato eseguito il provisioning.

```
ssh -i key-name user-name@machine-ip
```

Come fornire la propria coppia di chiavi pubblica-privata

Molte aziende creano e distribuiscono le proprie coppie di chiavi pubbliche-private per l'autenticazione.

Utilizzare il codice seguente come linea guida.

- 1 Nell'ambiente locale, ottenere o generare la coppia di chiavi pubblica-privata.

Per ora, è sufficiente generare e salvare le chiavi localmente.

- 2 In Cloud Assembly, prima del provisioning, aggiungere proprietà `remoteAccess` al modello cloud come mostrato nell'esempio.

La chiave `sshKey` include il codice alfanumerico lungo trovato all'interno del file della chiave pubblica `key-name.pub`.

Il nome utente è facoltativo e viene creato automaticamente per l'accesso. Se viene omesso, il sistema genera un ID casuale come nome utente.

Esempio:

```
type: Cloud.Machine
properties:
  name: our-vm1
  image: Linux18
  flavor: small
  remoteAccess:
```

```

authentication: publicPrivateKey
sshKey: ssh-rsa Iq+5aQgBP3ZNT4o1baP5Ii+dstIcowRRkyobbfpA1mj9tslf
qGxvU66PX9IeZax5hZvNWFgjw6ag+Z1zndOLhVdVoW49f274/mIRild7Uuw...
username: testuser

```

- 3 In Cloud Assembly, eseguire il provisioning della macchina dal relativo modello cloud e portarlo a uno stato di avvio.
- 4 Utilizzando il client del fornitore di soluzioni cloud, accedere alla macchina di cui è stato eseguito il provisioning.
- 5 Aggiungere il file della chiave pubblica alla cartella principale della macchina. Utilizzare la chiave specificata in `remoteAccess.sshKey`.
- 6 Verificare che il file della chiave privata di controparte sia presente nella macchina locale.
La chiave è in genere `/home/username/.ssh/key-name` senza estensione `.pub`.
- 7 Aprire una sessione SSH remota e connettersi alla macchina di cui è stato eseguito il provisioning.

```
ssh -i key-name user-name@machine-ip
```

Come fornire una coppia di chiavi AWS

Aggiungendo il nome di una coppia di chiavi AWS al modello cloud, è possibile accedere in remoto a una macchina che Cloud Assembly distribuisce in AWS.

Tenere presente che le coppie di chiavi AWS sono specifiche della regione. Se si effettua il provisioning dei carichi di lavoro in `us-east-1`, la coppia di chiavi deve esistere in `us-east-1`.

Utilizzare il codice seguente come linea guida. Questa opzione funziona solo per le zone cloud AWS.

```

type: Cloud.Machine
properties:
  image: Ubuntu
  flavor: small
  remoteAccess:
    authentication: keyPairName
    keyPair: cas-test
constraints:
  - tag: 'cloud:aws'

```

Fornire un nome utente e una password

Aggiungendo il nome utente e la password al modello cloud, è possibile ottenere un accesso remoto semplice a una macchina distribuita da Cloud Assembly.

Sebbene sia meno sicuro, l'accesso remoto con un nome utente e una password potrebbe essere tutto ciò che la situazione richiede. Si tenga presente che alcuni fornitori di cloud o talune configurazioni potrebbero non supportare questa opzione meno sicura.

- 1 In Cloud Assembly, prima del provisioning, aggiungere proprietà `remoteAccess` al modello cloud come mostrato nell'esempio.

Impostare il nome utente e la password per l'account con cui si prevede di accedere.

Esempio:

```
type: Cloud.Machine
properties:
  name: our-vm3
  image: Linux18
  flavor: small
  remoteAccess:
    authentication: usernamePassword
    username: testuser
    password: admin123
```

- 2 In Cloud Assembly, eseguire il provisioning della macchina dal relativo modello cloud e portarlo a uno stato di avvio.
- 3 Passare all'interfaccia del fornitore di soluzioni cloud e accedere alla macchina di cui è stato eseguito il provisioning.
- 4 Nella macchina di cui è stato eseguito il provisioning, creare o attivare l'account.
- 5 Dalla macchina locale, aprire una sessione remota con l'indirizzo IP o l'FQDN della macchina di cui è stato eseguito il provisioning e accedere con il nome utente e la password come di consueto.

Posizionamento del disco SCSI con Cloud Assembly

Per gestire un disco SCSI, è necessario specificarne e conoscerne il controller SCSI e il numero di unità logica (LUN). Per un oggetto disco di vSphere, è possibile utilizzare Cloud Assembly per assegnare entrambi i valori nel modello cloud.

La possibilità di utilizzare controller SCSI diversi è importante per le prestazioni ed è necessaria per alcuni tipi di distribuzione, come i cluster RAC (Real Application Cluster) di Oracle.

Proprietà del controller SCSI e del disco LUN

Per assegnare un controller SCSI e un LUN, aggiungere le seguenti proprietà del modello cloud:

```
SCSIController
```

```
unitNumber
```

È inoltre possibile omettere le proprietà. In questo caso l'assegnazione segue un'impostazione predefinita prevedibile. Cloud Assembly non distribuisce più i dischi SCSI in ordine casuale, rendendone difficoltosa la gestione.

I dischi e i controller SCSI vengono numerati in ordine iniziando da zero. Ogni controller SCSI può supportare dischi SCSI di numeri di unità da 0 a 15.

Opzione 1: impostazione del controller SCSI e del numero di unità

È possibile specificare entrambe le proprietà, come illustrato nell'esempio seguente. In tal caso, l'assegnazione del controller SCSI e del numero di unità corrispondono ai valori immessi.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
        - source: '${resource.Cloud_vSphere_Disk_2.id}'
        - source: '${resource.Cloud_vSphere_Disk_3.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_2
      unitNumber: 0
  Cloud_vSphere_Disk_2:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_2
      unitNumber: 1
  Cloud_vSphere_Disk_3:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
      SCSIController: SCSI_Controller_3
      unitNumber: 4
```

Opzione 2: impostazione del solo controller SCSI

È possibile specificare il controller SCSI e omettere il numero di unità. In questo caso, l'assegnazione del controller SCSI corrisponde al valore immesso. Il numero di unità viene impostato sul primo numero di unità disponibile in tale controller.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
```

```

- source: '${resource.Cloud_vSphere_Disk_2.id}'
- source: '${resource.Cloud_vSphere_Disk_3.id}'
Cloud_vSphere_Disk_1:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
    SCSIController: SCSI_Controller_0
Cloud_vSphere_Disk_2:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
    SCSIController: SCSI_Controller_0
Cloud_vSphere_Disk_3:
  type: Cloud.vSphere.Disk
  properties:
    capacityGb: 1
    SCSIController: SCSI_Controller_1

```

Opzione 3: omissione di entrambe le proprietà

È possibile omettere il controller SCSI e il numero di unità. In questo caso, l'assegnazione viene impostata sul primo controller SCSI disponibile e sul primo numero di unità disponibile in tale controller.

```

resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: centos
      cpuCount: 1
      totalMemoryMB: 1024
      attachedDisks:
        - source: '${resource.Cloud_vSphere_Disk_1.id}'
        - source: '${resource.Cloud_vSphere_Disk_2.id}'
        - source: '${resource.Cloud_vSphere_Disk_3.id}'
  Cloud_vSphere_Disk_1:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Disk_2:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1
  Cloud_vSphere_Disk_3:
    type: Cloud.vSphere.Disk
    properties:
      capacityGb: 1

```

Opzione non applicabile: solo LUN

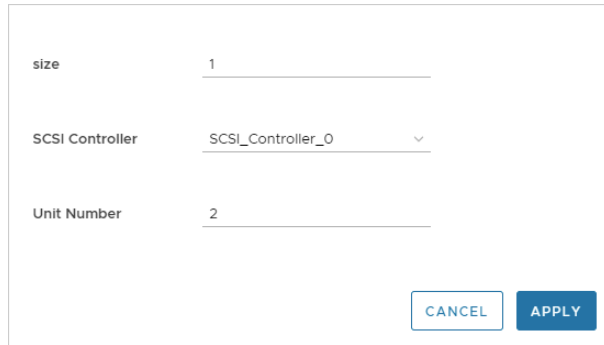
Non è possibile omettere il controller SCSI e specificare solo un numero di unità. Questa operazione potrebbe causare una distribuzione in cui più controller SCSI dispongono di un disco con tale numero ma, a scopo di gestione, non si sa di quale disco si tratti.

Utilizzo degli input per impostare il controller SCSI e il LUN

Per rendere la progettazione più dinamica, utilizzare gli input in modo che l'utente possa specificare il controller SCSI e il numero di unità al momento della richiesta o dell'aggiornamento.

```
inputs:
  diskProperties:
    type: array
    minItems: 1
    maxItems: 10
    items:
      type: object
      properties:
        size:
          type: integer
        SCSIController:
          type: string
          title: SCSI Controller
          enum:
            - SCSI_Controller_0
            - SCSI_Controller_1
            - SCSI_Controller_2
            - SCSI_Controller_3
        unitNumber:
          type: integer
          title: Unit Number

resources:
  app:
    type: Cloud.vSphere.Machine
    allocatePerInstance: true
    properties:
      flavor: small
      image: centos
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 0, 4), 'source')}'
  disk:
    type: Cloud.vSphere.Disk
    allocatePerInstance: true
    properties:
      capacityGb: '${input.diskProperties[count.index].size}'
      SCSIController: '${input.diskProperties[count.index].SCSIController}'
      unitNumber: '${input.diskProperties[count.index].unitNumber}'
      count: ${length(input.diskProperties)}
```



size	1
SCSI Controller	SCSI_Controller_0
Unit Number	2

CANCEL APPLY

Inizializzazione della macchina in Cloud Assembly

È possibile applicare l'inizializzazione della macchina in Cloud Assembly eseguendo comandi direttamente o, se la distribuzione avviene in zone cloud basate su vSphere, tramite le specifiche di personalizzazione.

Funzionamento dei comandi e delle specifiche di personalizzazione

- Comandi

Una sezione cloudConfig nel codice del modello cloud contiene i comandi che si desidera eseguire.

- Specifiche di personalizzazione

Una proprietà nel codice del modello cloud fa riferimento a una specifica di personalizzazione di vSphere in base al nome.

Comandi e specifiche di personalizzazione potrebbero non essere combinati

Quando si distribuisce in vSphere, procedere con cautela se si tenta di combinare l'inizializzazione di cloudConfig e delle specifiche di personalizzazione. Formalmente non sono compatibili e potrebbero produrre risultati incoerenti o indesiderati quando vengono utilizzate insieme.

Per un esempio di interazione tra i comandi e le specifiche di personalizzazione, vedere [Indirizzi IP statici di vSphere in Cloud Assembly](#).

Specifiche di personalizzazione di vSphere nei modelli di Cloud Assembly

Quando si distribuisce nelle zone cloud basate su vSphere in Cloud Assembly, le specifiche di personalizzazione possono applicare le impostazioni del sistema operativo guest al momento della distribuzione.

Abilitazione della specifica di personalizzazione

Le specifiche di personalizzazione devono essere presenti in vSphere, nella destinazione della distribuzione.

Modificare direttamente il codice del modello cloud. L'esempio seguente fa riferimento a una specifica di personalizzazione `cloud-assembly-linux` per un host WordPress in vSphere.

```
resources:
  WebTier:
    type: Cloud.vSphere.Machine
    properties:
      name: wordpress
      cpuCount: 2
      totalMemoryMB: 1024
      imageRef: 'Template: ubuntu-18.04'
      customizationSpec: 'cloud-assembly-linux'
      folderName: '/Datacenters/Datacenter/vm/deployments'
```

Indica se utilizzare le specifiche di personalizzazione o i comandi cloudConfig

Se si desidera che l'esperienza di provisioning corrisponda alle operazioni attualmente eseguite in vSphere, l'approccio migliore può essere continuare a utilizzare le specifiche di personalizzazione. Tuttavia, per eseguire l'espansione a un provisioning del cloud ibrido o multiplo, un approccio più neutro è rappresentato dai comandi di inizializzazione di cloudConfig.

Per ulteriori informazioni sulle sezioni cloudConfig nei modelli cloud, vedere [Comandi di configurazione nei modelli di Cloud Assembly](#).

Comandi e specifiche di personalizzazione potrebbero non essere combinati

Quando si distribuisce in vSphere, procedere con cautela se si tenta di combinare l'inizializzazione del comando cloudConfig incorporato e delle specifiche di personalizzazione. Formalmente non sono compatibili e potrebbero produrre risultati incoerenti o indesiderati quando vengono utilizzate insieme.

Per un esempio di interazione tra i comandi e le specifiche di personalizzazione, vedere [Indirizzi IP statici di vSphere in Cloud Assembly](#).

Comandi di configurazione nei modelli di Cloud Assembly

È possibile aggiungere una sezione cloudConfig al codice del modello di Cloud Assembly, in cui aggiungere comandi di inizializzazione della macchina eseguiti al momento della distribuzione.

Formati dei comandi cloudConfig

- Linux: i comandi di inizializzazione seguono lo standard [cloud-init](#) aperto.
- Windows: i comandi di inizializzazione utilizzano [Cloudbase-init](#).

Linux [cloud-init](#) e Windows [Cloudbase-init](#) non condividono la stessa sintassi. Una sezione cloudConfig per un sistema operativo non funzionerà nell'immagine di una macchina dell'altro sistema operativo.

Cosa possono eseguire i comandi cloudConfig

È possibile utilizzare i comandi di inizializzazione per automatizzare l'applicazione di dati o impostazioni al momento della creazione dell'istanza. In questo modo è possibile personalizzare gli utenti, le autorizzazioni, le installazioni e tutte le altre operazioni basate sui comandi. Gli esempi includono:

- Impostazione di un nome host
- Generazione e configurazione di chiavi private SSH
- Installazione dei pacchetti

Posizione in cui è possibile aggiungere i comandi cloudConfig

È possibile aggiungere una sezione cloudConfig al codice del modello cloud, ma è anche possibile aggiungerne una in anticipo a un'immagine della macchina durante la configurazione dell'infrastruttura. Quindi, tutti i modelli cloud che fanno riferimento all'immagine di origine ottengono la stessa inizializzazione.

È possibile disporre di una mappa immagine e di un modello cloud in cui entrambi contengono comandi di inizializzazione. Al momento della distribuzione, i comandi vengono uniti e Cloud Assembly esegue i comandi consolidati.

Quando lo stesso comando viene visualizzato in entrambe le posizioni ma include parametri differenti, viene eseguito solo il comando di mappatura dell'immagine.

Per ulteriori dettagli, vedere [Ulteriori informazioni sulle mappature dell'immagine in vRealize Automation](#).

Comandi cloudConfig di esempio

Nell'esempio seguente la sezione cloudConfig è tratta dal codice del modello cloud del [Creazione un modello cloud di base](#) per il server MySQL basato su Linux.

Nota Per garantire la corretta interpretazione dei comandi, includere sempre il carattere pipe cloudConfig: | come mostrato.

```
cloudConfig: |
  #cloud-config
  repo_update: true
  repo_upgrade: all
  packages:
    - apache2
    - php
    - php-mysql
    - libapache2-mod-php
```

```

- php-mcrypt
- mysql-client
runcmd:
- mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
- i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
- mysql -u root -pmysqlpassword -h ${DBTier.networks[0].address} -e "create database
wordpress_blog;"
- mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
mywordpresssite/wp-config.php
- sed -i -e s/"define( 'DB_NAME', 'database_name_here' );"/"define( 'DB_NAME',
'wordpress_blog' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_USER', 'username_here' );"/"define( 'DB_USER',
'root' );"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define( 'DB_PASSWORD', 'password_here' );"/"define( 'DB_PASSWORD',
'mysqlpassword' );"/ /var/www/html/mywordpresssite/wp-config.php && sed
-i -e s/"define( 'DB_HOST', 'localhost' );"/"define( 'DB_HOST', '$
{DBTier.networks[0].address}' );"/ /var/www/html/mywordpresssite/wp-config.php
- service apache2 reload

```

Se uno script cloud-init si comporta in modo imprevisto, controllare l'output della console acquisita in `/var/log/cloud-init-output.log` durante la risoluzione dei problemi. Per ulteriori informazioni su cloud-init, [vedere la documentazione di cloud-init](#).

Comandi e specifiche di personalizzazione potrebbero non essere combinati

Quando si distribuisce in vSphere, procedere con cautela se si tenta di combinare l'inizializzazione del comando cloudConfig incorporato e delle specifiche di personalizzazione. Formalmente non sono compatibili e potrebbero produrre risultati incoerenti o indesiderati quando vengono utilizzate insieme.

Per un esempio di interazione tra i comandi e le specifiche di personalizzazione, vedere [Indirizzi IP statici di vSphere in Cloud Assembly](#).

Modelli di vSphere per l'inizializzazione in Cloud Assembly


Quando il modello di Cloud Assembly distribuisce un'immagine basata su un modello di vSphere, il modello di vSphere deve essere configurato in anticipo affinché supporti cloud-init.

Per configurare un modello di vSphere per il supporto di cloud-init, eseguire i passaggi seguenti.

- 1 Nella macchina virtuale che diventerà il modello, installare cloud-init.

Ad esempio, utilizzare `yum` per installare cloud-init su CentOS o `apt-get` per installare su Ubuntu.

- 2 Impostare il CD-ROM della macchina virtuale sulla modalità passthrough.

CD/DVD drive 1 *	Client Device
Status	<input type="checkbox"/> Connect At Power On
CD/DVD Media	To connect, power on the VM and select the media from the VM Hardware panel on Summary tab
Device Mode	 Passthrough CD-ROM

- 3 Dalla riga di comando del sistema operativo guest, eseguire `cloud-init clean`.

Nota Al termine di `cloud-init clean`, non modificare ulteriormente la macchina virtuale.

- 4 Arrestare la macchina virtuale e convertirla in un modello.

Indirizzi IP statici di vSphere in Cloud Assembly

Quando si esegue la distribuzione in vSphere in Cloud Assembly, è possibile assegnare un indirizzo IP statico, ma è necessario evitare conflitti tra i comandi di inizializzazione di `cloudConfig` e le specifiche della personalizzazione.

Progettazioni di esempio

Le seguenti progettazioni applicano un indirizzo IP statico senza creare alcun conflitto tra i comandi di inizializzazione del modello cloud e le specifiche della personalizzazione. Tutti contengono l'impostazione di rete `assignment: static`.

Progettazione	Codice del modello cloud di esempio
<p>Assegnazione di un indirizzo IP statico a una macchina Linux che non dispone di codice cloud-init</p>	<pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: linux-template networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre>
<p>Assegnare un indirizzo IP statico a una macchina Linux con un codice cloud-init che non contiene comandi di assegnazione di rete. NOTA: la specifica di personalizzazione di vSphere viene applicata se si imposta la proprietà customizeGuestOs su true o se si omette la proprietà customizeGuestOs.</p>	<p>Esempio di Ubuntu</p> <pre>resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: true cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: root:Pa\$\$w0rd expire: false write_files: - path: /tmpFile.txt content: \${resource.wpnet.dns} runcmd: - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}'</pre> <p>Esempio di CentOS</p> <pre>resources: wpnet: type: Cloud.Network properties:</pre>

Progettazione**Codice del modello cloud di esempio**

```
name: wpnet
networkType: public
constraints:
  - tag: sqa
DBTier:
type: Cloud.vSphere.Machine
properties:
  flavor: small
  image: centos-template
  customizeGuestOs: true
  cloudConfig: |
    #cloud-config
    write_files:
      - path: /test.txt
        content: |
          deploying in power off.
          then rebooting.
networks:
  - name: '${wpnet.name}'
    assignment: static
    network: '${resource.wpnet.id}'
```

Progettazione	Codice del modello cloud di esempio
<p>Assegnare un indirizzo IP statico a una macchina Linux con codice cloud-init che contiene comandi di assegnazione di rete.</p> <p>La proprietà <code>customizeGuestOs</code> deve essere <code>false</code>.</p>	<p>Esempio di Ubuntu</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu-template customizeGuestOs: false cloudConfig: #cloud-config write_files: - path: /etc/netplan/99-installer- config.yaml content: network: version: 2 renderer: networkd ethernet: ens160: addresses: - \${resource.DBTier.networks[0].address}/\${ {resource.wpnet.prefixLength} gateway4: \$ {resource.wpnet.gateway} nameservers: search: \$ {resource.wpnet.dnsSearchDomains} addresses: \${resource.wpnet.dns} runcmd: - netplan apply - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}' </pre> <p>Esempio di CentOS</p> <pre> resources: wpnet: type: Cloud.Network properties: name: wpnet networkType: public constraints: - tag: sqa DBTier: type: Cloud.vSphere.Machine properties: flavor: small image: centos-template </pre>

Progettazione**Codice del modello cloud di esempio**

```

customizeGuestOs: false
cloudConfig: |
  #cloud-config
  ssh_pwauth: yes
  chpasswd:
    list: |
      root:VMware1!
    expire: false
  runcmd:
    - nmcli con add type
  ethernet con-name 'custom ens192'
  ifname ens192 ip4 ${self.networks[0].address}/
    ${resource.wpnet.prefixLength} gw4 $
    {resource.wpnet.gateway}
    - nmcli con mod 'custom ens192' ipv4.dns "$
    {join(resource.wpnet.dns, ' ')}"
    - nmcli con mod 'custom ens192' ipv4.dns-
    search "${join(resource.wpnet.dnsSearchDomains, ',')}"
    - nmcli con down 'System ens192' ; nmcli
  con up 'custom ens192'
    - nmcli con del 'System ens192'
    - hostnamectl set-hostname --static `dig -x
    ${self.networks[0].address} +short | cut -d "." -f 1`
    - hostnamectl set-hostname --pretty $
    {self.resourceName}
    - touch /etc/cloud/cloud-init.disabled
  networks:
    - name: '${wpnet.name}'
      assignment: static
      network: '${resource.wpnet.id}'

```

Quando la distribuzione è basata su un'immagine di riferimento, assegnare un indirizzo IP statico a una macchina Linux con il codice cloud-init che contiene i comandi di assegnazione di rete. La proprietà `customizeGuestOs` deve essere `false`. Il modello cloud non deve inoltre includere la proprietà `ovfProperties`, che blocca la personalizzazione.

```

resources:
  wpnet:
    type: Cloud.Network
    properties:
      name: wpnet
      networkType: public
      constraints:
        - tag: sqa
  DBTier:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small

imageRef: 'https://cloud-images.ubuntu.com/releases/focal/release/ubuntu-20.04-server-cloudimg-amd64.ova'
customizeGuestOs: false
cloudConfig: |
  #cloud-config
  ssh_pwauth: yes
  chpasswd:
    list: |
      root:Pa$$w0rd
      ubuntu:Pa$$w0rd
    expire: false
  write_files:
    - path: /etc/netplan/99-netcfg-vrac.yaml
      content: |
        network:
          version: 2
          renderer: networkd

```


Progettazione	Codice del modello cloud di esempio
	<pre> ethernets: ens192: dhcp4: no dhcp6: no addresses: - \${resource.DBTier.networks[0].address}/\${ {resource.wpnet.prefixLength} gateway4: \$ {resource.wpnet.gateway} nameservers: search: \$ {resource.wpnet.dnsSearchDomains} addresses: \${resource.wpnet.dns} runcmd: - netplan apply - hostnamectl set-hostname --pretty \$ {self.resourceName} - touch /etc/cloud/cloud-init.disabled networks: - name: '\${wpnet.name}' assignment: static network: '\${resource.wpnet.id}' </pre>

Progettazioni che non funzionano o possono generare risultati indesiderati

- Il codice cloud-init non contiene comandi di assegnazione di rete e la proprietà `customizeGuestOs` è `false`.
Non sono presenti né comandi di inizializzazione né specifiche di personalizzazione per configurare le impostazioni di rete.
- Il codice cloud-init non contiene comandi di assegnazione di rete e la proprietà `ovfProperties` è impostata.
I comandi di inizializzazione non sono presenti, ma `ovfProperties` ha bloccato la specifica di personalizzazione.
- Il codice cloud-init contiene i comandi di assegnazione di rete e la proprietà `customizeGuestOs` non è presente o è impostata su `true`.
L'applicazione della specifica di personalizzazione è in conflitto con i comandi di inizializzazione.

Altre soluzioni per cloud-init e specifiche di personalizzazione

Quando si esegue la distribuzione in vSphere, è inoltre possibile personalizzare un'immagine per risolvere i conflitti delle specifiche di personalizzazione e di cloud-init. Per ulteriori informazioni, vedere il repository esterno seguente.

- [Script di preparazione dell'immagine di vSphere](#)

Distribuzione ritardata in Cloud Assembly

Potrebbe essere necessario inizializzare completamente una macchina virtuale prima di procedere con la distribuzione di Cloud Assembly.

Ad esempio, la distribuzione di una macchina che sta ancora installando pacchetti e l'avvio di un server Web potrebbero causare condizioni in cui un utente veloce tenta di raggiungere l'applicazione prima che sia disponibile.

Quando si utilizza questa funzionalità, tenere presenti le considerazioni seguenti.

- La funzionalità utilizza il modulo [cloud-init](#) `phone_home` ed è disponibile durante la distribuzione delle macchine Linux.
- Phone Home non è disponibile per Windows a causa delle limitazioni di [Cloudbase-init](#).
- Phone Home può influire sull'ordine di distribuzione come una dipendenza esplicita, ma ha una maggiore flessibilità nelle opzioni di temporizzazione ed elaborazione.

Vedere [Creazione di binding e dipendenze tra le risorse in Cloud Assembly](#).

- Phone Home richiede una sezione `cloudConfig` nel modello cloud.
- La creatività rappresenta un fattore. I comandi di inizializzazione possono includere il tempo di attesa integrato tra le operazioni, che possono essere utilizzate insieme a Phone Home.
- Phone Home basato su modello cloud non funziona se il modello di macchina contiene già le impostazioni del modulo `phone_home`.
- La macchina deve avere accesso alla comunicazione in uscita in Cloud Assembly.

Per introdurre un ritardo di distribuzione in Cloud Assembly, aggiungere una sezione `cloudConfigSettings` al modello cloud:

```
cloudConfigSettings:
  phoneHomeShouldWait: true
  phoneHomeTimeoutSeconds: 600
  phoneHomeFailOnTimeout: true
```

Proprietà	Descrizione
<code>phoneHomeShouldWait</code>	Indica se attendere l'inizializzazione, può essere <code>true</code> o <code>false</code> .
<code>phoneHomeTimeoutSeconds</code>	Intervallo di tempo in cui decidere se procedere con la distribuzione anche se l'inizializzazione è ancora in esecuzione. Il valore predefinito è 10 minuti.
<code>phoneHomeFailOnTimeout</code>	Indica se procedere con la distribuzione dopo il timeout, può essere <code>true</code> o <code>false</code> . Tenere presente che anche quando si procede, la distribuzione potrebbe comunque non riuscire per motivi differenti.

Personalizzazione guest di Windows in Cloud Assembly

Affinché Cloud Assembly possa inizializzare automaticamente una macchina Windows al momento della distribuzione, preparare un'immagine che supporti Cloudbase-Init, quindi un modello cloud che contenga i comandi appropriati.

Il processo di creazione dell'immagine varia a seconda del fornitore cloud. L'esempio mostrato qui è per vSphere.

Immagine Cloud Assembly di Windows per vSphere

Affinché Cloud Assembly possa inizializzare una macchina Windows distribuita in vSphere, l'immagine deve essere basata su un modello di vSphere con Cloudbase-Init installato e configurato.

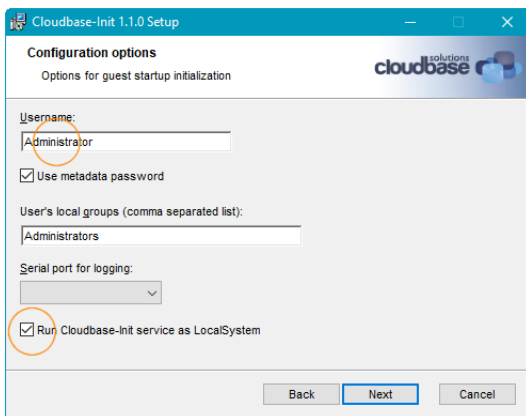
Creazione dell'immagine

- 1 Utilizzare vSphere per creare e accendere una macchina virtuale Windows.
- 2 Nella macchina virtuale, accedere a Windows.
- 3 Scaricare Cloudbase-Init.

<https://cloudbase.it/cloudbase-init/#download>

- 4 Avviare il file di installazione .msi di Cloudbase-Init.

Durante l'installazione, immettere **Administrator** come nome utente e selezionare l'opzione da eseguire come LocalSystem.



Altre selezioni di installazione possono rimanere come valori predefiniti.

- 5 Consentire l'esecuzione dell'installazione, ma non chiudere la pagina finale di completamento dell'installazione guidata.

Importante Non chiudere la pagina finale dell'installazione guidata.

- 6 Con la pagina di completamento dell'installazione guidata ancora aperta, utilizzare Windows per passare al percorso di installazione di Cloudbase-Init e aprire il file seguente in un editor di testo.

```
conf\cloudbase-init-unattend.conf
```

- 7 Impostare `metadata_services` su `OvfService` come mostrato. Aggiungere l'impostazione se non esiste già.

```
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
```

- 8 Salvare e chiudere `cloudbase-init-unattend.conf`.
- 9 Nella stessa cartella, aprire il file seguente in un editor di testo.

```
conf\cloudbase-init.conf
```

- 10 Impostare `first_logon_behaviour`, `metadata_services` e `plugins` come mostrato. Aggiungere le impostazioni se non esistono già.

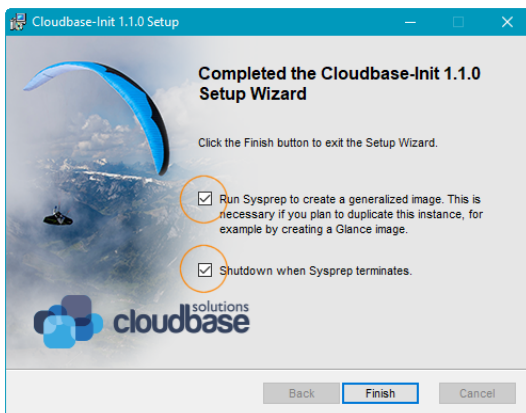
```
first_logon_behaviour=always
. . .
metadata_services=cloudbaseinit.metadata.services.ovfservice.OvfService
. . .
plugins=cloudbaseinit.plugins.windows.createuser.CreateUserPlugin,cloudbaseinit.plugins.win
dows.setuserpassword.SetUserPasswordPlugin,cloudbaseinit.plugins.common.sshpublickeys.SetUs
erSSHPublicKeysPlugin,cloudbaseinit.plugins.common.userdata.UserDataPlugin
. . .
```

- 11 Salvare e chiudere `cloudbase-init.conf`.
- 12 Nella pagina di completamento dell'installazione guidata, selezionare le opzioni per eseguire Sysprep e arrestare dopo Sysprep, quindi fare clic su **Fine**.

Nota VMware ha riscontrato casi in cui l'esecuzione di Sysprep impedisce il funzionamento delle distribuzioni dell'immagine.

Durante la distribuzione, Cloud Assembly applica una specifica di personalizzazione generata dinamicamente, che disconnette l'interfaccia di rete. Lo stato di Sysprep in sospeso nell'immagine potrebbe causare un errore della specifica di personalizzazione e lasciare disconnessa la distribuzione.

Se si sospetta che ciò si verifichi nell'ambiente in uso, provare a lasciare le opzioni Sysprep disattivate durante la creazione dell'immagine.



13 Dopo l'arresto della macchina virtuale, utilizzare vSphere per trasformarla in un modello.

Dettagli aggiuntivi

La seguente tabella si espande in base alle voci di configurazione effettuate durante l'installazione.

Impostazione di configurazione	Scopo
Username, CreateUserPlugin e SetUserPasswordPlugin	Dopo Sysprep, il primo avvio utilizza CreateUserPlugin per creare l'account Administrator del nome utente con una password vuota. SetUserPasswordPlugin consente a Cloudbase-Init di cambiare la password vuota con la password di accesso remota che verrà inclusa nel modello cloud.
First Logon Behavior	Questa impostazione richiede all'utente di modificare la password al primo accesso.
Metadata services	Elencando solo OvfService, Cloudbase-Init non cercherà di trovare altri servizi di metadati che non sono supportati in vCenter. In questo modo si ottengono file di registro più puliti, in quanto in caso contrario i registri compilerebbero le voci relative alla mancata individuazione di tali servizi.
Plugins	Elencando solo i plug-in con le funzionalità supportate da OvfService, anche in questo caso i registri sono più puliti. Cloudbase-Init esegue i plug-in nell'ordine specificato.
Run as LocalSystem	Questa impostazione supporta tutti i comandi di inizializzazione avanzati che potrebbero richiedere l'avvio di Cloudbase-Init con un account amministratore dedicato.

Comandi Cloudbase-Init per Windows in Cloud Assembly

Per eseguire l'inizializzazione della macchina Windows al momento della distribuzione, aggiungere i comandi Cloudbase-Init al codice del modello di Cloud Assembly.

L'esempio mostrato qui è basato su vSphere, ma altri fornitori cloud devono essere simili.

Prerequisiti

- Creare l'infrastruttura. In Cloud Assembly, aggiungere l'account cloud di vSphere e una zona cloud associata.
- Aggiungere le mappature delle immagini e aggiungere profili di rete e storage.

Nell'infrastruttura, una mappatura dell'immagine deve fare riferimento a un modello Windows creato per supportare Cloudbase-Init. Vedere [Immagine Cloud Assembly di Windows per vSphere](#).

Se il modello non è elencato, passare ad Account cloud e sincronizzare le immagini. In caso contrario, la sincronizzazione automatica viene eseguita ogni 24 ore.

- Aggiungere un progetto, aggiungere utenti e assicurarsi che gli utenti possano eseguire il provisioning nella propria zona cloud.

Per ulteriori informazioni sulla creazione di infrastrutture e progetti, vedere gli esempi nel [Tutorial: configurazione e verifica dell'infrastruttura e delle distribuzioni multi-cloud in Cloud Assembly](#).

Procedura

- 1 In Cloud Assembly, passare alla scheda **Progettazione** e creare un modello cloud.

- 2 Aggiungere una sezione `cloudConfig` con i comandi Cloudbase-Init desiderati.

I seguenti esempi di comandi creano un nuovo file nell'unità `C:` di Windows e impostano il nome host.

```
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    properties:
      image: cloudbase-init-win-2016
      flavor: small
      remoteAccess:
        authentication: usernamePassword
        username: Administrator
        password: Password1234@$
      cloudConfig: |
        #cloud-config
        write_files:
          content: Cloudbase-Init test
          path: C:\test.txt
          set_hostname: testname
```

Per ulteriori informazioni, vedere la [documentazione di Cloudbase-Init](#).

- 3 Aggiungere le proprietà `remoteAccess` in modo da configurare la macchina per l'accesso iniziale a Windows.

Come accennato durante la creazione del modello, il servizio metadati raccoglie le credenziali di accesso e le espone a `CreateUserPlugin` e `SetUserPasswordPlugin`. Si tenga presente che la password deve soddisfare i requisiti delle password di Windows.

- 4 Da Cloud Assembly, testare e distribuire il modello cloud.
- 5 Dopo la distribuzione, utilizzare Windows RDP e le credenziali nel modello per accedere alla nuova macchina Windows e verificare la personalizzazione.

Nell'esempio precedente, si cerca il file `C:\test.txt` e si controllano le proprietà di sistema per il nome host.

Cluster di macchine e dischi in Cloud Assembly

Le progettazioni di modelli di Cloud Assembly possono distribuire un cluster di macchine e collegare un cluster di dischi.

Per distribuire cluster di macchine e dischi, utilizzare il `allocatePerInstance` [Contrassegni di risorsa di Cloud Assembly per le richieste](#) e la [Sintassi dell'espressione Cloud Assembly](#) `count.index` e `map_to_object` nei modelli cloud.

I seguenti esempi di codici di modelli cloud possono essere utilizzati come linee guida per progettazioni che distribuiscono cluster.

Due macchine che condividono un cluster di dischi

```
resources:
  app0:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 0,2), "source")}'
  appl:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 2,4), "source")}'
  disk:
    type: Cloud.Volume
    allocatePerInstance: true
    properties:
      count: 4
      capacityGb: 5
```

Numero variabile di macchine con un disco ciascuna

```
inputs:
  count:
    type: integer
    default: 2
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      count: '${input.count}'
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, count.index, count.index +
1), "source")}'
  disk:
    type: Cloud.Volume
```

```

allocatePerInstance: true
properties:
  count: '${input.count}'
  capacityGb: 5

```

Numero variabile di macchine con due dischi ciascuna

```

inputs:
  count:
    type: integer
    default: 2
resources:
  Cloud_Machine_1:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      image: ubuntu
      flavor: small
      count: ${input.count}
      attachedDisks: '${map_to_object(slice(resource.disk[*].id, 2*count.index,
2*(count.index + 1)), "source")}'
    disk:
      type: Cloud.Volume
      allocatePerInstance: true
      properties:
        count: ${2*input.count}
        capacityGb: 5

```

Impostazione delle dimensioni del disco al momento della richiesta

```

inputs:
  disksize:
    type: array
    minItems: 2
    maxItems: 2
    items:
      type: object
      properties:
        size:
          type: integer
resources:
  app:
    type: Cloud.Machine
    allocatePerInstance: true
    properties:
      flavor: small
      image: ubuntu
      attachedDisks: ${map_to_object(slice(resource.disk[*].id, 0, 2), 'source')}
    disk:
      type: Cloud.Volume

```



```
allocatePerInstance: true
properties:
  count: 2
  capacityGb: ${input.disksize[count.index].size}
```

Denominazione personalizzata per le risorse distribuite in Cloud Assembly

In qualità di amministratore del progetto o del cloud, si dispone di una convenzione di denominazione prestabilita per le risorse del proprio ambiente e si desidera che la risorsa distribuita segua tale convenzione senza che sia necessaria l'interazione dell'utente. È possibile creare un modello di denominazione per tutte le distribuzioni di un progetto di Cloud Assembly.

Ad esempio, la convenzione di denominazione dell'host consiste nell'aggiungere a una risorsa il prefisso *projectname-sitecode-costcenter-whereDeployed-identifier*. È possibile configurare il modello di denominazione personalizzato per le macchine per ogni progetto. Alcune variabili di modello vengono estratte dal sistema durante la distribuzione, mentre altre sono basate sulle proprietà personalizzate del progetto. Il modello di denominazione personalizzato per il prefisso riportato sopra ha un aspetto simile all'esempio seguente.

```
${project.name}-${resource.siteCode}-${resource.costCenter}-${endpoint.name}-${#####}
```

L'identificatore, fornito nel modello come `${#####}`, mostra un identificatore di sei cifre.

L'identificatore è un contatore che garantisce l'univocità. Il contatore è globale per l'organizzazione e viene incrementato in tutti i progetti, non solo in quello corrente. Quando si dispone di più progetti, non aspettarsi una sequenza da 000123 a 000124 per le distribuzioni nel progetto corrente. È possibile prevedere un incremento da 000123 a 000127.

Tutti i nomi delle risorse devono essere univoci. Per garantire l'univocità, utilizzare la proprietà del numero incrementale. I numeri aumentano per tutte le distribuzioni, incluse le distribuzioni denominate da Cloud Assembly. Man mano che il sistema diventa più robusto e poiché il sistema applica nomi personalizzati a molti tipi di risorse, la numerazione può apparire casuale, ma i valori garantiscono comunque l'univocità. I numeri aumentano anche quando si esegue una distribuzione di test.

L'elenco seguente è un esempio di dove vengono applicati i nomi personalizzati. L'elenco non è da intendersi come definitivo.

Tabella 6-2. Elenco di esempio delle risorse a cui vengono applicati nomi personalizzati

Gruppo di risorse	Tipi di risorse
Macchine virtuali	<ul style="list-style-type: none"> ■ Cloud.Machine ■ Cloud.vSphere.Machine ■ Cloud.AWS.EC2.Instance ■ Cloud.GCP.Machine ■ Cloud.Azure.Machine
Bilanciamenti del carico	<ul style="list-style-type: none"> ■ Cloud.LoadBalancer ■ Cloud.NSX.LoadBalancer
Reti	<ul style="list-style-type: none"> ■ Cloud.Network ■ Cloud.vSphere.Network ■ Cloud.NSX.Network
Gruppi di sicurezza	<ul style="list-style-type: none"> ■ Cloud.SecurityGroup
Dischi	<ul style="list-style-type: none"> ■ Cloud.Volume ■ Cloud.vSphere.Disk ■ Cloud.AWS.Volume ■ Cloud.GCP.Disk ■ Cloud.Azure.Disk
NSX	<ul style="list-style-type: none"> ■ Cloud.NSX.Gateway ■ Cloud.NSX.NAT
Microsoft Azure	<ul style="list-style-type: none"> ■ Cloud.Azure.ResourceGroup

Oltre agli esempi forniti qui, è possibile aggiungere anche il nome utente, l'immagine utilizzata, altre opzioni integrate e stringhe semplici. Durante la creazione del modello, vengono forniti suggerimenti relativi alle opzioni possibili.

Si tenga presente che alcuni valori visualizzati sono solo esempi di casi d'uso. Non sarà possibile utilizzarli alla lettera nel proprio ambiente. Valutare dove apportare le proprie sostituzioni o utilizzare i valori di esempio per adattarli alle proprie esigenze di gestione della distribuzione e dell'infrastruttura cloud.

Prerequisiti

- Assicurarsi di conoscere la convenzione di denominazione che si desidera utilizzare per le distribuzioni di un progetto.
- Questa procedura presuppone che sia presente o che sia possibile creare un modello cloud semplice da utilizzare per testare la denominazione dei prefissi degli host personalizzati.

Procedura

- 1 Selezionare **Infrastruttura > Progetti**.
- 2 Selezionare un progetto esistente o crearne uno nuovo.

- 3 Nella scheda **Provisioning**, individuare la sezione Proprietà personalizzate e creare le proprietà per il codice del sito e i valori del centro di costo.

Qui è possibile sostituire i valori visualizzati dell'esempio con quelli pertinenti per il proprio ambiente.

Custom Properties

Specify the custom properties that should be added to all requests in this project. ⓘ

Define custom properties	Name	Value
	siteCode	BGL
	costCenter	IT-research

Custom Naming

Specify the naming template to be used for machines provisioned in this project.

Template `$(project.name)-$(resource.siteCode)-$(resource.costCenter)-$(endpoint.name)-${#####}` ⓘ

- Creare una proprietà personalizzata con il nome **siteCode** e il valore **BGL**.
 - Aggiungere un'altra proprietà personalizzata con il nome **costCenter** e il valore **IT-research**.
- 4 Individuare la sezione Denominazione personalizzata e aggiungere il modello seguente.

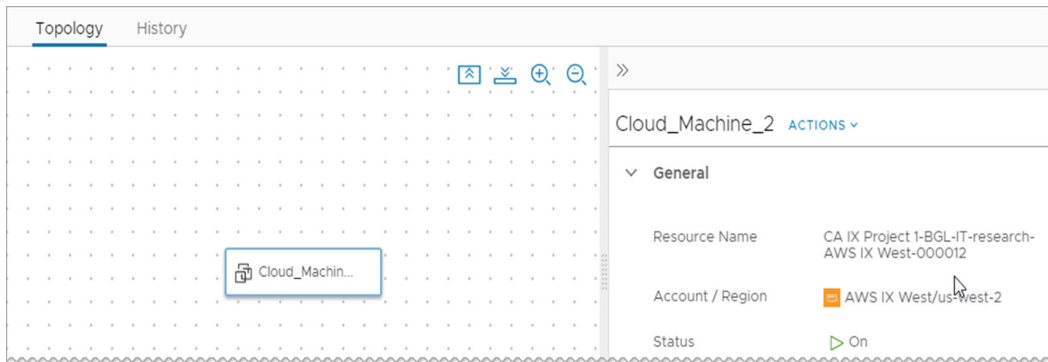
```
$(project.name)-$(resource.siteCode)-$(resource.costCenter)-$(endpoint.name)-${#####}
```

È possibile copiare nella stringa, ma se questo è il primo modello di denominazione, è consigliabile utilizzare il testo del suggerimento e la selezione rapida durante la creazione del modello.

- 5 Distribuire un modello cloud associato al progetto per verificare che il nome personalizzato venga applicato alla risorsa.
- Fare clic sulla scheda **Progettazione**, quindi fare clic su un modello cloud associato al progetto.
 - Distribuire il modello cloud.

Si apre la pagina **Distribuzioni**, che mostra la distribuzione in corso.

- c Una volta completata la distribuzione, fare clic sul nome della distribuzione.
- d Nella scheda **Topologia**, si noti che il nome personalizzato è il nome della risorsa nel riquadro a destra.



- 6 Se è stato distribuito un modello cloud di test per verificare la convenzione di denominazione, è possibile eliminare la distribuzione.

Operazioni successive

Creare modelli di denominazione personalizzati per gli altri progetti.

Aggiunta della risorsa SaltStack Config nelle progettazioni di Cloud Assembly

Se si integra SaltStack Config con vRealize Automation, è possibile applicare la risorsa SaltStack Config per installare i minion nelle macchine virtuali nelle distribuzioni. Dopo aver distribuito il minion, è possibile utilizzare la potente gestione della configurazione di SaltStack Config, la correzione della deviazione e le funzionalità di gestione dello stato per gestire le risorse.

I minion sono agenti che eseguono il servizio salt-minion. Il servizio sottoscrive i processi pubblicati da un Salt Master, che è un server che esegue il servizio Salt-Master. Quando un processo specifico si applica a un minion, il minion esegue il processo.

È possibile utilizzare la risorsa SaltStack Config per distribuire minion e applicare i file di stato quando si distribuiscono le macchine Linux e Windows. Per aggiungere o aggiornare minion e file di stato nelle distribuzioni esistenti, è possibile eseguire l'azione giorno 2 **Applica configurazione Salt**. Questa azione utilizza la proprietà `saltConfiguration`. Per ulteriori informazioni sulla creazione dell'azione giorno 2, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Se è stata utilizzata la proprietà `saltConfiguration` per distribuire i minion e i file di stato come azione giorno 0, è consigliabile aggiornare i modelli cloud per utilizzare la risorsa SaltStack Config. La proprietà `saltConfiguration` verrà deprecata in una versione futura e verrà sostituita con la risorsa SaltStack Config, insieme a un'azione giorno 2 alternativa.

Nota La proprietà `saltConfiguration` e la risorsa SaltStack Config sono supportate nello stesso modello cloud ma non per la stessa risorsa.

Ad esempio, è possibile creare un modello cloud con due macchine. La prima macchina viene collegata a una risorsa SaltStack Config. La seconda macchina non è collegata a una risorsa SaltStack Config e non è inoltre applicata una configurazione Salt. Dopo aver distribuito il modello cloud, è possibile eseguire solo un'operazione giorno 2 sulla seconda macchina per applicare una configurazione Salt. L'azione giorno 2 sulla macchina con la risorsa SaltStack Config verrà disabilitata

Prima di iniziare

- 1 Verificare di aver installato SaltStack Config e configurato l'integrazione. Vedere [Creazione di un'integrazione di SaltStack Config in vRealize Automation](#).
- 2 In SaltStack Config, verificare che la risoluzione dei nomi di dominio completi da minion a master funzioni.
 - a Per verificare il nome di dominio completo nel Salt Master in SaltStack Config, selezionare **Minion > Tutti i minion**.
 - b Filtrare la colonna **ID minion** per il valore **saltmaster**.
 - c Fare clic su **saltmaster** per visualizzare i dettagli.
 - d Verificare che il valore del nome completo di dominio sia corretto.
- 3 Se si distribuiscono minion in una macchina Linux, verificare che le funzionalità SSH siano abilitate per le immagini in vSphere che si intende distribuire con un minion Salt. SSH viene utilizzato per accedere in remoto alla macchina e distribuire il minion.
- 4 Se si distribuiscono minion in una macchina Windows, vedere [Come distribuire i minion utilizzando l'API in un ambiente Windows](#).
- 5 Verificare che sia possibile assegnare indirizzi IP alle macchine distribuite.

SaltStack Config richiede che le macchine dispongano di indirizzi IP. Usare gli indirizzi IP per l'intervallo CIDR dell'IP pubblico per l'SDDC (data center definito da software) in cui si trova il Salt Master.
- 6 Verificare che il modello cloud a cui si sta aggiungendo il minion sia distribuibile prima di aggiungere le proprietà della risorsa SaltStack Config.
- 7 Verificare di disporre dei ruoli di servizio seguenti:
 - a Amministratore di Cloud Assembly
 - b Utente di Cloud Assembly

c Amministratore di Service Broker

Questi ruoli di servizio sono necessari per utilizzare la risorsa SaltStack Config.

Aggiunta della risorsa SaltStack Config al modello cloud

Lo sviluppatore di modelli cloud può aggiungere al codice YAML proprietà che installano il minion SaltStack Config quando si distribuisce il modello.

Le proprietà principali aggiunte al modello includono l'accesso remoto per la macchina che si desidera distribuire e le proprietà di configurazione per la risorsa SaltStack Config. La procedura include solo le proprietà selezionate. Il codice YAML include altre proprietà della risorsa SaltStack Config che non vengono utilizzate in questo esempio. Per ulteriori informazioni, rivedere lo schema.

Sebbene questo esempio mostri come aggiungere il nome utente e la password per le proprietà di accesso remoto, è possibile configurare una proprietà segreta e aggiungerla al modello. Per un esempio, vedere [Proprietà di Cloud Assembly segrete](#).

Procedura

- 1 In Cloud Assembly, selezionare **Progettazione > Modelli cloud**.
- 2 Aprire un modello esistente.
- 3 Individuare la risorsa **SaltStack Config** e trascinarla nella tela.
- 4 Collegare la risorsa **SaltStack Config** alla macchina in cui verrà installato il minion.
- 5 Nel riquadro del codice, aggiungere proprietà alla risorsa `Cloud_SaltStack_1`.

Non è necessario includere tutte le proprietà possibili. I valori utilizzati in questo esempio sono spiegati nella tabella.

```
Cloud_SaltStack_1:
  type: Cloud.SaltStack
  properties:
    masterId: saltstack_enterprise_installer
    hosts:
      - ${resource.Cloud_vSphere_Machine_1.id}
    saltEnvironment: sse
    stateFiles:
      - /doe.sls
    variables:
      user: joe
```

Descrizione delle proprietà `Cloud_SaltStack_1` utilizzate in questo esempio.

Proprietà	Descrizione
masterId	Nello schema di esempio, il valore <code>masterId</code> è <code>saltstack_enterprise_installer</code> . È possibile che in SaltStack Config siano definiti ID master in Amministrazione > Chiavi master .
host	Il valore <code>hosts</code> è l'ID della macchina o del cluster di macchine in cui si desidera installare il minion. Per impostazione predefinita, il nome della macchina viene passato come ID minion in SaltStack Config. È consigliabile scegliere nomi di macchina inferiori a 15 caratteri, specialmente se si distribuiscono minion in Windows. Windows non consente nomi host che superano i 15 caratteri. Se si desidera definire una convenzione di denominazione personalizzata per le macchine da distribuire, vedere Denominazione personalizzata per le risorse distribuite in Cloud Assembly .
saltEnvironment	In questo esempio, <code>sse</code> è un percorso del file per i file di stato. È possibile che i file di stato siano in altre posizioni del file server in SaltStack Config in Configurazione > File server .
stateFiles	In questo esempio, <code>doe.sls</code> è un file di stato fornito nella directory del file server specificato come <code>saltEnvironment</code> .
variables	Le variabili sono i valori utilizzati dal file di stato. In questo esempio, <code>doe.sls</code> accetta un valore <code>user</code> .

6 Aggiungere proprietà `remoteAccess` alla macchina che ospita il minion Salt.

Il valore della chiave `authentication` deve essere `usernamePassword` o `generatedPublicPrivateKey`. `publicPrivateKey` non è supportato.

```
remoteAccess:
  authentication: usernamePassword
  username: adminUser
  password: adminPassword
```

7 Verificare che il codice YAML includa proprietà simili a quelle dell'esempio seguente.

```
resources:
  Cloud_vSphere_Machine_1:
    type: Cloud.vSphere.Machine
    properties:
      image: ubuntu
      flavor: small
      remoteAccess:
        authentication: usernamePassword
        username: adminUser
        password: adminPassword
  Cloud_SaltStack_1:
```

```

type: Cloud.SaltStack
properties:
  masterId: saltstack_enterprise_installer
  hosts:
    - ${resource.Cloud_vSphere_Machine_1.id}
  saltEnvironment: sse
  stateFiles:
    - /doe.sls
  variables:
    user: joe

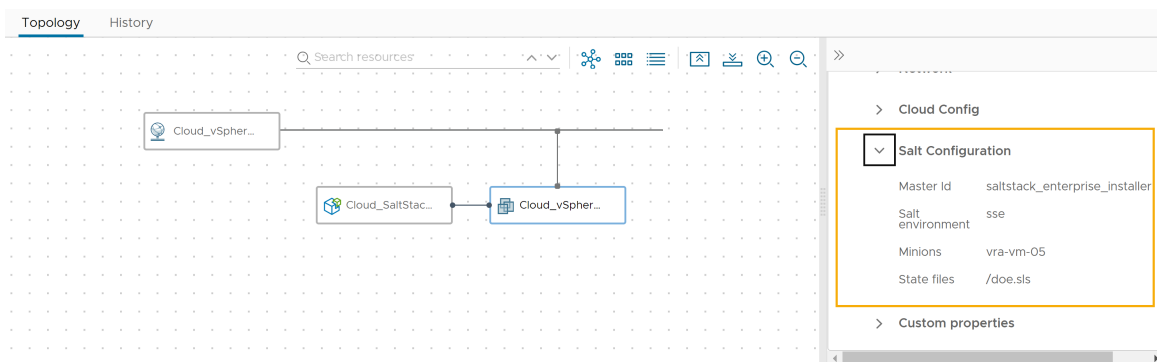
```

8 Testare e distribuire il modello cloud.

Se la distribuzione del minion non riesce, vedere [Risoluzione dei problemi relativi ai minion](#).

9 Verificare le proprietà della configurazione di Salt per la macchina distribuita.

- Selezionare **Distribuzioni > Distribuzioni** e aprire i dettagli della distribuzione.
- Nella scheda **Topologia**, fare clic sulla macchina ed espandere le proprietà nel riquadro destro.



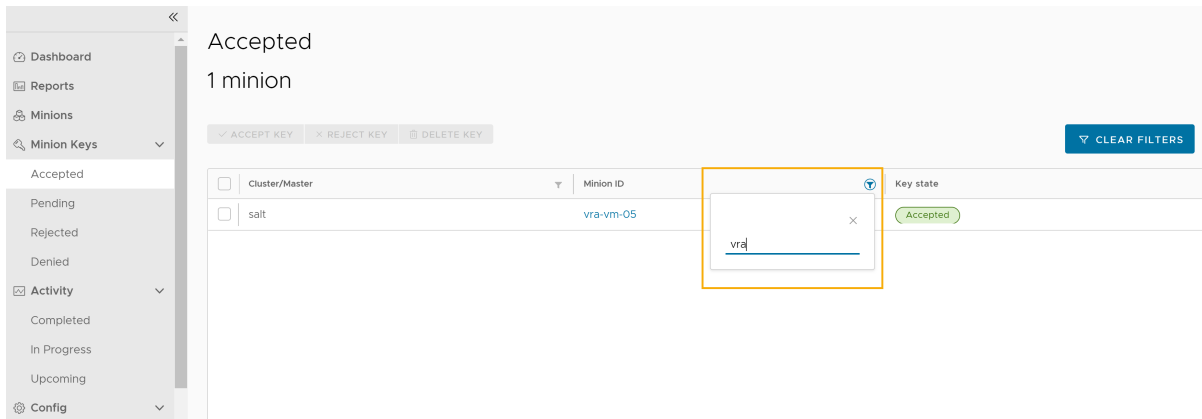
Verifica del minion in SaltStack Config

Dopo aver installato il minion nella macchina virtuale, individuare il minion ed eseguire tutti i processi o i comandi nella risorsa.

Procedura

- Per aprire SaltStack Config, fare clic sul menu Applicazioni nell'angolo superiore - destro e fare clic su **Console Cloud Services**.
- Fare clic sul riquadro del servizio **SaltStack Config**.
- In SaltStack Config, espandere **Chiavi minion** e fare clic su **Accettate**.
- Nella colonna **ID minion**, fare clic sull'icona del filtro e immettere il nome del minion.

Il nome del minion ha come impostazione predefinita il nome host della macchina virtuale. In questo esempio, l'ID minion è vra-vm-05.



- 5 Per visualizzare i dettagli, fare clic sul nome del minion.

È possibile eseguire processi o comandi sul minion. Ad esempio, Utilizzo del disco di esempio. Questo processo restituisce le statistiche sull'utilizzo del disco per un minion.

vra-vm-05

Presence: Present

Key state: Accepted

Master: salt

Targets: [All Minions](#) , [Linux](#) , [Ubuntu](#)

IPv4: 10.196.194.192, 127.0.0.1

OS: Ubuntu16.04

Salt Version: 3002.7

[RUN JOB](#) [RUN COMMAND](#)

Grains Activity

biosreleasedate	12/12/2018
biosversion	6.00
> cpu_flags	--
cpu_model	Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
cpuarch	x86_64
cwd	/
> disks	--

Risoluzione dei problemi relativi ai minion

Informazioni su alcuni errori comuni che gli utenti sperimentano durante la distribuzione dei minion Salt utilizzando la risorsa SaltStack Config o la proprietà `saltConfiguration`.

Avvio dell'host ritardato

Se i servizi Windows o Linux nell'host non sono pronti dopo la distribuzione del modello cloud, è possibile visualizzare un errore "Distribuzione minion e/o esecuzione del file di stato non riuscita" in Cloud Assembly.

Per risolvere questo errore, aggiornare il plug-in Master alla versione stabile più recente. Dopo aver completato l'aggiornamento, è possibile abilitare un'impostazione di configurazione in `/etc/salt/master.d/raas.conf` che consente di attivare il tempo necessario per i servizi Windows e Linux prima di distribuire il minion Salt.

Dopo aver eseguito l'aggiornamento alla versione più recente del plug-in Master, completare i passaggi seguenti per ritardare l'avvio dell'host:

- 1 Selezionare la scheda **Cronologia** nella pagina dei dettagli della distribuzione.
- 2 Se il messaggio di errore indica che l'esecuzione del file di stato e/o della distribuzione del minion non è riuscita, copiare l'ID processo (JID) e aprire SaltStack Config.
- 3 In SaltStack Config, selezionare **Attività > Completata** per aprire i processi completati.
- 4 Nella colonna **JID**, fare clic sull'icona del filtro e digitare il JID.
- 5 Fare clic su JID per rivedere la pagina dei risultati del processo.
- 6 Fare clic sulla scheda **Non elaborato** per visualizzare l'output non elaborato per il processo.

Windows

Se l'ultima riga nell'output non elaborato per il processo contiene il messaggio "Impossibile connettersi all'host: timeout", è necessario aggiungere questa impostazione di configurazione a `/etc/salt/master.d/raas.conf` per ritardare l'avvio di 180 secondi:

```
sseapi_win_minion_deploy_delay: 180
```

Linux

Se l'ultima riga nell'output non elaborato per il processo contiene il messaggio "L'host remoto non è accessibile utilizzando le credenziali fornite", è necessario aggiungere questa impostazione di configurazione a `/etc/salt/master.d/raas.conf` per ritardare l'avvio di 90 secondi:

```
sseapi_linux_minion_deploy_delay: 90
```

- 7 Riavviare il servizio Salt Master

```
systemctl restart salt-master
```

- 8 Ridistribuire il modello cloud.

Se la distribuzione non riesce, è possibile aumentare il parametro di ritardo e ridistribuire il modello.

Passaggi successivi

Per utilizzare le funzionalità di SaltStack Config per gestire le risorse, vedere la documentazione di [SaltStack Config](#).

Configurazioni di Terraform in Cloud Assembly

È possibile incorporare le configurazioni di Terraform come risorsa nei modelli cloud di Cloud Assembly.

Preparazione di un ambiente di runtime di Terraform di Cloud Assembly

I progetti che includono configurazioni Terraform richiedono l'accesso a un ambiente di runtime di Terraform che viene integrato con il prodotto Cloud Assembly in locale.

Come aggiungere un runtime Terraform

L'ambiente di runtime è costituito da un cluster Kubernetes che esegue i comandi della CLI di Terraform per eseguire le operazioni richieste. Inoltre, il runtime raccoglie i registri e restituisce i risultati dai comandi della CLI di Terraform.


Il prodotto vRealize Automation in locale richiede agli utenti di configurare il proprio cluster Kubernetes di runtime di Terraform. È supportato un solo runtime di Terraform per organizzazione. Tutte le distribuzioni di Terraform per tale organizzazione utilizzano lo stesso runtime.

- 1 Verificare di disporre di un cluster Kubernetes in cui eseguire la CLI Terraform.
 - Tutti gli utenti possono fornire un file kubeconfig per eseguire la CLI di Terraform in un cluster Kubernetes non gestito.
 - Gli utenti delle licenze aziendali possono scegliere se eseguire la CLI Terraform in un cluster Kubernetes gestito da vRealize Automation.

In Cloud Assembly, passare a **Infrastruttura > Risorse > Kubernetes** e verificare di disporre di un cluster Kubernetes. Vedere [Come si utilizza Kubernetes in Cloud Assembly](#) se è necessario aggiungerne uno.
- 2 Se il cluster Kubernetes è stato aggiunto o modificato di recente, attendere il completamento della raccolta dati.

La raccolta dati recupera l'elenco degli spazi dei nomi e altre informazioni e potrebbe richiedere fino a 5 minuti in base al provider.
- 3 Una volta completata la raccolta dati, passare a **Infrastruttura > Connessioni > Integrazioni > Aggiungi integrazione** e selezionare la scheda **Runtime di Terraform**.
- 4 Immettere le impostazioni.

Figura 6-3. Esempio di integrazione di runtime Terraform



New Integration

Name *

Description

Terraform Runtime Integration

Runtime type *

☒ Managed kubernetes cluster
☐ External kubeconfig

Kubernetes cluster * ⓘ

Kubernetes namespace * ⓘ

Runtime Container Settings

Image ⓘ

CPU request (Millicores)

CPU limit (Millicores)

Memory request (MB)

Memory limit (MB)

Impostazione	Descrizione
Nome	Assegnare un nome univoco all'integrazione del runtime.
Descrizione	Fornire una spiegazione dello scopo dell'integrazione.
Integrazione runtime Terraform:	
Tipo di runtime (solo aziendale)	Gli utenti delle licenze aziendali possono scegliere se eseguire la CLI Terraform in un cluster Kubernetes gestito da vRealize Automation o uno non gestito.
Kubeconfig Kubernetes (tutti gli utenti)	<p>Per un cluster Kubernetes non gestito, incollare l'intero contenuto del file kubeconfig per il cluster esterno.</p> <p>Per utilizzare un runtime Kubernetes esterno con un server proxy, vedere Come aggiungere supporto proxy.</p> <p>Questa opzione è disponibile per tutti gli utenti.</p>

Impostazione	Descrizione
Cluster Kubernetes (solo aziendale)	<p>Per Kubernetes gestito da vRealize Automation, selezionare il cluster in cui eseguire la CLI Terraform.</p> <p>Il cluster e il file kubeconfig devono essere raggiungibili.</p> <p>È possibile convalidare l'accesso a kubeconfig con un comando GET su <code>/cmx/api/resources/k8s/clusters/{clusterId}/kube-config</code>.</p> <p>Questa opzione è disponibile solo per le licenze aziendali.</p>
Spazio dei nomi Kubernetes	Selezionare lo spazio dei nomi da utilizzare all'interno del cluster per la creazione di pod che eseguono la CLI di Terraform.
Impostazioni contenitore runtime:	
Immagine	<p>Immettere il percorso dell'immagine del contenitore della versione Terraform che si desidera eseguire.</p> <p>Nota Il pulsante CONVALIDA non verifica l'immagine del contenitore.</p>
Richiesta CPU	Immettere la quantità di CPU per i contenitori in esecuzione. Il valore predefinito è 250 millicore.
Limite CPU	Immettere la CPU massima consentita per i contenitori in esecuzione. Il valore predefinito è 250 millicore.
Richiesta memoria	Immettere la quantità di memoria per i contenitori in esecuzione. Il valore predefinito è 512 MB.
Limite di memoria	Immettere la memoria massima consentita per i contenitori in esecuzione. Il valore predefinito è 512 MB.

5 Fare clic su **CONVALIDA** e modificare le impostazioni secondo necessità.

6 Fare clic su **AGGIUNGI**.

Le impostazioni vengono memorizzate nella cache. Dopo aver aggiunto l'integrazione, è possibile modificare le impostazioni, ad esempio il cluster o lo spazio dei nomi, ma potrebbero essere necessari fino a 5 minuti perché venga rilevata una modifica e affinché la CLI di Terraform venga eseguita con le nuove impostazioni.

Risoluzione dei problemi relativi al runtime di Terraform

Alcuni problemi di distribuzione della configurazione Terraform potrebbero essere correlati all'integrazione del runtime.

Problema	Causa	Risoluzione
La convalida non riesce e viene visualizzato un errore in cui si segnala che lo spazio dei nomi non è valido.	È stato modificato il cluster, ma è stato lasciato lo spazio dei nomi precedente nell'interfaccia utente.	Riselezionare sempre uno spazio dei nomi dopo aver modificato la selezione del cluster.
Il menu a discesa dello spazio dei nomi è vuoto o non elenca gli spazi dei nomi appena aggiunti.	La raccolta dati per il cluster non è stata completata. La raccolta dati richiede fino a 5 minuti dopo l'immissione o la modifica del cluster e fino a 10 minuti durante l'immissione o la modifica dello spazio dei nomi.	Per un nuovo cluster con spazi dei nomi esistenti, attendere fino a 5 minuti per il completamento della raccolta dati. Per un nuovo spazio dei nomi in un cluster esistente, attendere fino a 10 minuti per il completamento della raccolta dati. Se il problema persiste, rimuovere il cluster e aggiungerlo di nuovo in Infrastruttura > Risorse > Kubernetes .
I contenitori della CLI di Terraform vengono creati in un cluster precedente, in uno spazio dei nomi precedente o con le impostazioni di runtime precedenti, anche dopo l'aggiornamento dell'account di integrazione.	Il client dell'API Kubernetes utilizzato da vRealize Automation viene memorizzato nella cache per 5 minuti.	L'applicazione delle modifiche potrebbe richiedere fino a 5 minuti.
La convalida o un'operazione di distribuzione di Terraform non riesce e viene visualizzato un messaggio di errore che indica che kubeconfig non è disponibile.	In alcuni casi questi errori si verificano perché il cluster non è raggiungibile da vRealize Automation. In altri casi, le credenziali dell'utente, i token o i certificati non sono validi.	L'errore kubeconfig può verificarsi per una serie di motivi e potrebbe richiedere il coinvolgimento del supporto tecnico per la risoluzione dei problemi.

Come aggiungere supporto proxy

Per fare in modo che il cluster di runtime Kubernetes esterno si connetta tramite un server proxy, eseguire i passaggi seguenti.

- 1 Accedere al server cluster Kubernetes esterno.
- 2 Creare una cartella vuota.
- 3 Nella nuova cartella, aggiungere le seguenti righe a un nuovo file denominato Dockerfile.

```
FROM projects.registry.vmware.com/vra/terraform:latest as final
ENV https_proxy=protocol://username:password@proxy_host:proxy_port
ENV http_proxy=protocol://username:password@proxy_host:proxy_port
ENV no_proxy=.local,.localdomain,localhost
```

- 4 Modificare i valori dei segnaposto in modo che le variabili di ambiente `https_proxy` e `http_proxy` includano le impostazioni del server proxy utilizzate per accedere a Internet.

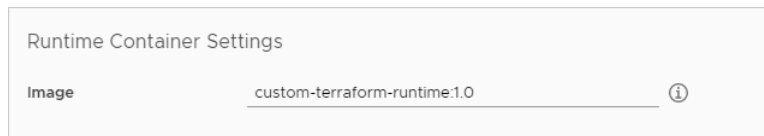
protocol sarà http o https in base al protocollo utilizzato dal server proxy, che potrebbe non corrispondere al nome della variabile di ambiente `https_proxy` o `http_proxy`.

- 5 Salvare e chiudere il file Dockerfile.
- 6 Dalla cartella vuota, eseguire il comando seguente. In base ai privilegi dell'account, potrebbe essere necessario eseguire il comando in modalità sudo.

```
docker build --file Dockerfile --tag custom-terraform-runtime:1.0 .
```

Il comando crea un'immagine Docker custom-terraform-runtime:1.0 locale.

- 7 In Cloud Assembly, sotto **Infrastruttura > Connessioni > Integrazioni**, passare all'integrazione del runtime Terraform.
- 8 Creare o modificare le impostazioni del contenitore di runtime per utilizzare l'immagine custom-terraform-runtime:1.0:



Runtime Terraform di Cloud Assembly senza accesso a Internet

Gli utenti di Cloud Assembly che devono progettare ed eseguire integrazioni di Terraform mentre sono disconnessi da Internet possono configurare il proprio ambiente di runtime seguendo questo esempio.

Nota Per ottenere un'origine per la creazione dell'immagine, la configurazione richiede una breve connessione a Internet. Se non è possibile connettersi temporaneamente a Internet, potrebbe essere necessario eseguire questi passaggi al di fuori del sito disconnesso.

Questo processo presuppone che l'utente [disponga del proprio registro Docker](#) e possa accedere ai repository senza connessione Internet.

Creazione dell'immagine del contenitore personalizzata

- 1 Creare un'immagine del contenitore personalizzata che includa i file binari dei plug-in del provider Terraform.

Il Dockerfile seguente illustra un esempio di creazione di un'immagine personalizzata con il provider GCP di Terraform.

Il download dell'immagine di base `projects.registry.vmware.com/vra/terraform:latest` nel Dockerfile richiede l'accesso a Internet per poter raggiungere il registro VMware Harbor in `projects.registry.vmware.com`.

Le impostazioni del firewall o le impostazioni del proxy possono causare errori nella creazione dell'immagine. Potrebbe essere necessario abilitare l'accesso a releases.hashicorp.com per scaricare i file binari dei plug-in del provider Terraform. Tuttavia, è possibile utilizzare il proprio registro privato per fornire i file binari dei plug-in come opzione.

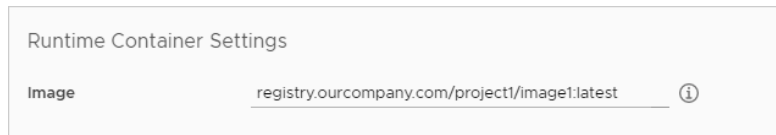
```
FROM projects.registry.vmware.com/vra/terraform:latest as final

# Create provider plug-in directory
ARG plugins=/tmp/terraform.d/plugin-cache/linux_amd64
RUN mkdir -m 777 -p $plugins

# Download and unzip all required provider plug-ins from hashicorp to provider directory
RUN cd $plugins \
    && wget -q https://releases.hashicorp.com/terraform-provider-google/3.58.0/terraform-provider-google_3.58.0_linux_amd64.zip \
    && unzip *.zip \
    && rm *.zip

# For "terraform init" configure terraform CLI to use provider plug-in directory and not
download from internet
ENV TF_CLI_ARGS_init="-plugin-dir=$plugins -get-plugins=false"
```

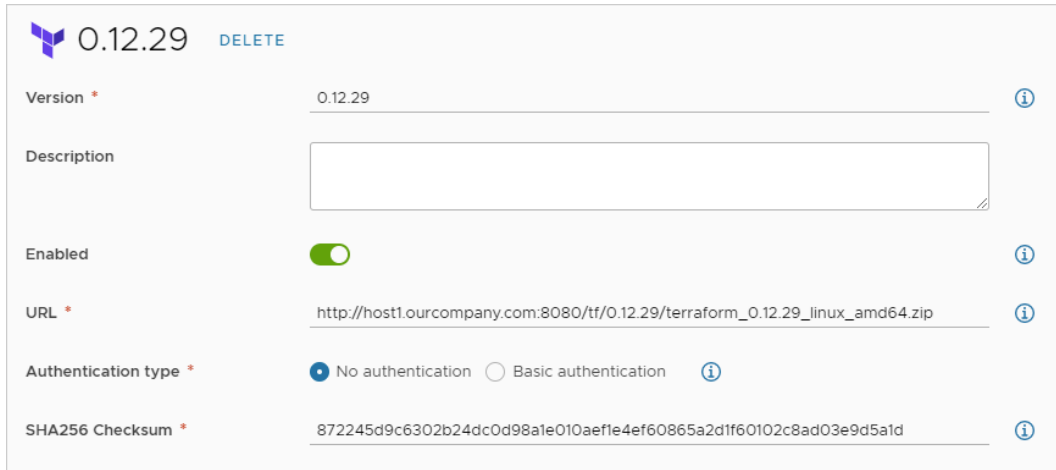
- 2 Creare, contrassegnare ed eseguire il push dell'immagine del contenitore personalizzata nel repository Docker nel sito disconnesso.
- 3 In Cloud Assembly, nel sito disconnesso, in **Infrastruttura > Connessioni > Integrazioni**, passare all'integrazione del runtime Terraform.
- 4 Creare o modificare le impostazioni del contenitore di runtime per aggiungere il repository per l'immagine del contenitore personalizzata. Il nome dell'immagine del contenitore personalizzata di esempio è `registry.ourcompany.com/project1/image1:latest`.



Hosting locale della CLI di Terraform

- 1 Scaricare i file binari della CLI di Terraform.
- 2 Caricare i file binari della CLI di Terraform nel server FTP o Web locale.
- 3 In Cloud Assembly, passare a **Infrastruttura > Configura > Versioni Terraform**.
- 4 Creare o modificare la versione di Terraform in modo che includa l'URL dei file binari della CLI di Terraform ospitati nel server locale.
- 5 Se il server FTP o Web locale richiede l'autenticazione di accesso, selezionare **Autenticazione di base** e immettere il nome utente e la password che possono accedere al server.

Per modificare il tipo di autenticazione, è necessario disporre del ruolo di amministratore del cloud in Cloud Assembly.



0.12.29 [DELETE](#)

Version * 0.12.29 ⓘ

Description

Enabled ☒ ⓘ

URL * http://host1.ourcompany.com:8080/tf/0.12.29/terraform_0.12.29_linux_amd64.zip ⓘ

Authentication type * ☒ No authentication ☐ Basic authentication ⓘ

SHA256 Checksum * 872245d9c6302b24dc0d98a1e010aef1e4ef60865a2df60102c8ad03e9d5a1d ⓘ

Progettazione e distribuzione delle configurazioni di Terraform

Con il runtime in esecuzione, è possibile aggiungere file di configurazione di Terraform a git, progettare modelli cloud per tali file ed eseguire la distribuzione.

Per iniziare, vedere [Preparazione delle configurazioni Terraform in Cloud Assembly](#).

Risoluzione dei problemi

Durante la distribuzione, aprire la distribuzione in Cloud Assembly. Nella scheda Cronologia, cercare gli eventi di Terraform e fare clic su **Mostra registri** a destra. Quando il provider Terraform locale funziona, nel registro vengono visualizzati i seguenti messaggi.

```
Initializing provider plugins
```

```
Terraform has been successfully initialized
```

Per un registro più affidabile, è possibile modificare manualmente il codice del modello cloud per aggiungere `TF_LOG: DEBUG` come illustrato nell'esempio seguente.

```
resources:
  terraform:
    type: Cloud.Terraform.Configuration
    properties:
      providers:
        - name: google
          # List of available cloud zones: gcp/us-west1
          cloudZone: gcp/us-west1
      environment:
        # Configure terraform CLI debug log settings
        TF_LOG: DEBUG
      terraformVersion: 0.12.29
      configurationSource:
        repositoryId: fc569ef7-f013-4489-9673-6909a2791071
        commitId: 3e00279a843a6711f7857929144164ef399c7421
        sourceDirectory: gcp-simple
```

Creazione della propria immagine di base

Nonostante VMware aggiorni l'immagine di base in `projects.registry.vmware.com/vra/terraform:latest`, tale immagine potrebbe essere obsoleta e contenere vulnerabilità.

Per creare la propria immagine di base, utilizzare invece il Dockerfile seguente.

```
FROM alpine:latest as final
RUN apk add --no-cache git wget curl openssh
```

Preparazione delle configurazioni Terraform in Cloud Assembly

Prima di aggiungere una configurazione Terraform a un modello di Cloud Assembly, configurare e integrare il repository di controllo versioni.

- 1 [Prerequisiti](#)
- 2 [Archiviare i file di configurazione di Terraform in un repository di controllo versioni](#)
- 3 [Abilitazione della mappatura della zona cloud](#)
- 4 [Integrare il repository con Cloud Assembly](#)

Prerequisiti

Affinché il prodotto vRealize Automation in locale esegua le operazioni di Terraform, è necessaria l'integrazione di runtime di Terraform. Vedere [Preparazione di un ambiente di runtime di Terraform di Cloud Assembly](#).

Archiviare i file di configurazione di Terraform in un repository di controllo versioni

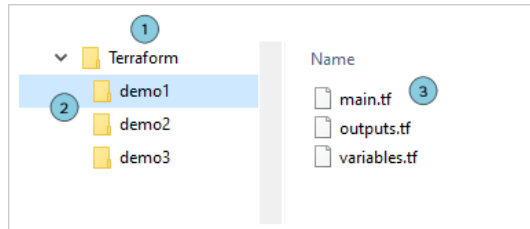
Cloud Assembly supporta i seguenti repository di controllo versioni per le configurazioni Terraform.

- Cloud GitHub, GitHub Enterprise locale
- Cloud GitLab, GitLab Enterprise locale
- Bitbucket locale

Nel repository di controllo delle versioni, creare una directory predefinita con un livello di sottodirectory, ognuna delle quali contenente i file di configurazione di Terraform. Creare una sottodirectory per ogni configurazione di Terraform.

- 1 Directory predefinita
- 2 Singolo livello di sottodirectory
- 3 File di configurazione di Terraform pronti per la distribuzione

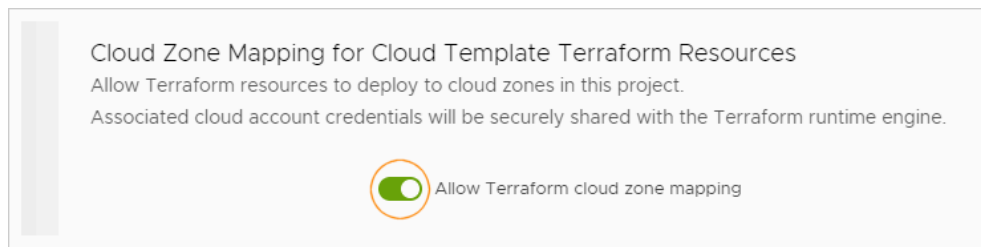
Non includere un file di stato di Terraform con i file di configurazione. Se è presente `terraform.tfstate`, si verificano errori durante la distribuzione.



Abilitazione della mappatura della zona cloud

Se si prevede di distribuire verso un account cloud, il motore di runtime di Terraform richiede le credenziali della zona cloud.

Nella scheda **Provisioning** del progetto, abilitare **Consenti mappatura zone cloud di Terraform**.



Anche se le credenziali sono trasmesse in modo sicuro, per una maggiore sicurezza è opportuno lasciare l'opzione disattivata se gli utenti del progetto non devono distribuire verso un account cloud.

Integrare il repository con Cloud Assembly

In Cloud Assembly, passare a **Infrastruttura > Connessioni > Integrazioni**.

Aggiungere un'integrazione al repository che offre il tipo in cui sono state memorizzate le configurazioni di Terraform: GitHub o Bitbucket.

Quando si aggiunge il progetto all'integrazione, selezionare il tipo **Configurazioni Terraform** e identificare il repository e il ramo.

Cartella è la directory predefinita della struttura precedente.

Add Repository: testProject

Configure a repository to be used for this project.

Type *

Terraform Configurations

ⓘ

Repository *

parnassusdemo/repository1

ⓘ

Branch *

master

Folder

/Terraform

Progettazione di configurazioni di Terraform in Cloud Assembly

Con il repository e i file di configurazione di Terraform, è possibile progettare un modello di Cloud Assembly per questi.

- 1 [Prerequisiti](#)
- 2 [Abilitare le versioni di runtime di Terraform](#)
- 3 [Aggiungere le risorse Terraform alla progettazione](#)
- 4 [Distribuzione del modello cloud](#)

Prerequisiti

Configurare e integrare il repository di controllo delle versioni. Vedere [Preparazione delle configurazioni Terraform in Cloud Assembly](#).

Abilitare le versioni di runtime di Terraform

È possibile definire le versioni di runtime di Terraform disponibili agli utenti durante la distribuzione delle configurazioni di Terraform. Si noti che le configurazioni di Terraform potrebbero includere anche vincoli di versione codificati internamente.

Per creare l'elenco delle versioni consentite, passare a **Infrastruttura > Configura > Versioni Terraform**.

Aggiungere le risorse Terraform alla progettazione

Creare il modello cloud che include le configurazioni di Terraform.

- 1 In Cloud Assembly, passare a **Progettazione > Modelli cloud** e fare clic su **Nuovo da > Terraform**.

Viene visualizzata la configurazione guidata Terraform.

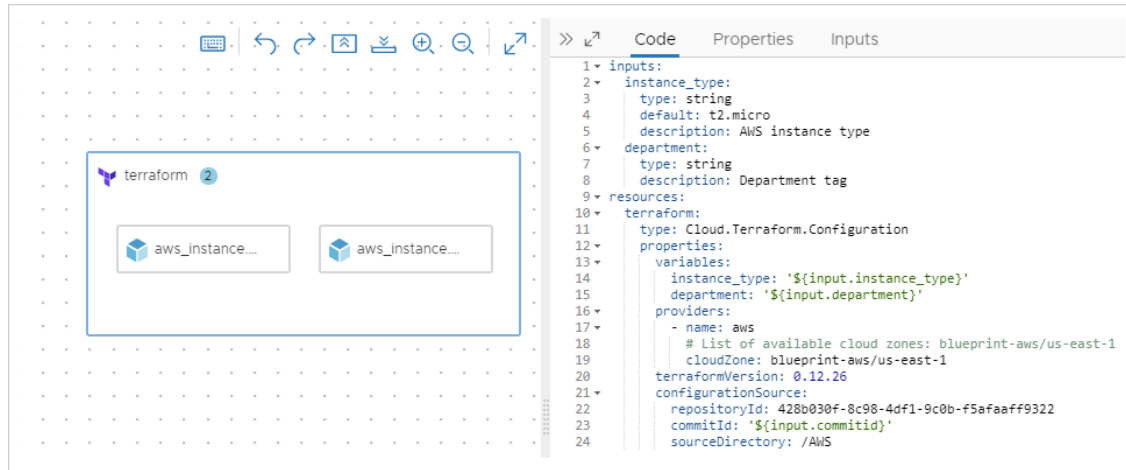
- 2 Seguire le istruzioni visualizzate.

Pagina della procedura guidata	Impostazione	Valore
Nuovo modello cloud	Nome	Assegnare un nome identificativo alla progettazione.
	Descrizione	Fornire una spiegazione dello scopo della progettazione.
	Progetto	Selezionare il progetto che include l'integrazione del repository in cui è memorizzata la configurazione di Terraform.
Origine configurazione	Repository	Selezionare il repository integrato in cui è memorizzata la configurazione di Terraform.

Pagina della procedura guidata	Impostazione	Valore
	Commit	Selezionare un commit del repository oppure lasciare vuota la voce per utilizzare la configurazione di Terraform dal valore head del repository. Limitazione Bitbucket: il numero di commit selezionabili potrebbe essere troncato a causa della configurazione del server del repository di Bitbucket.
	Directory di origine	Selezionare una sottodirectory dalla struttura del repository creata. Le sottodirectory di esempio mostrate nella configurazione precedente erano demo1, demo2 e demo3.
Finalizza configurazione	Repository	Verificare la corretta selezione del repository.
	Directory di origine	Verificare la corretta selezione della directory.
	Versione Terraform	Selezionare la versione di runtime di Terraform da eseguire quando si distribuisce la configurazione di Terraform.
	Provider	Se la configurazione di Terraform includeva un blocco del provider, verificare il provider e la zona cloud in cui questo modello cloud verrà distribuito. L'assenza di provider non costituisce un problema. Dopo aver completato la procedura guidata, è sufficiente modificare il provider e la zona cloud nelle proprietà del modello per aggiungere o modificare la destinazione della distribuzione.
	Variabili	Selezionare i valori riservati per la crittografia, ad esempio le password.
	Output	Verificare gli output della configurazione di Terraform, che vengono convertiti in espressioni a cui il codice della progettazione può fare ulteriore riferimento.

3 Fare clic su **Crea**.

La risorsa Terraform viene visualizzata nella tela del modello cloud, con il codice di Cloud Assembly che riflette la configurazione di Terraform da distribuire.



Se lo si desidera, è possibile aggiungere altre risorse di Cloud Assembly al modello cloud, per combinare il codice Terraform e non Terraform in una progettazione ibrida.

Nota L'aggiornamento delle configurazioni di Terraform nel repository non sincronizza le modifiche nel modello cloud. La sincronizzazione automatica può introdurre rischi per la sicurezza, come le variabili sensibili appena aggiunte.

Per acquisire le modifiche della configurazione di Terraform, eseguire nuovamente la procedura guidata, scegliere il nuovo commit e identificare tutte le eventuali nuove variabili sensibili.

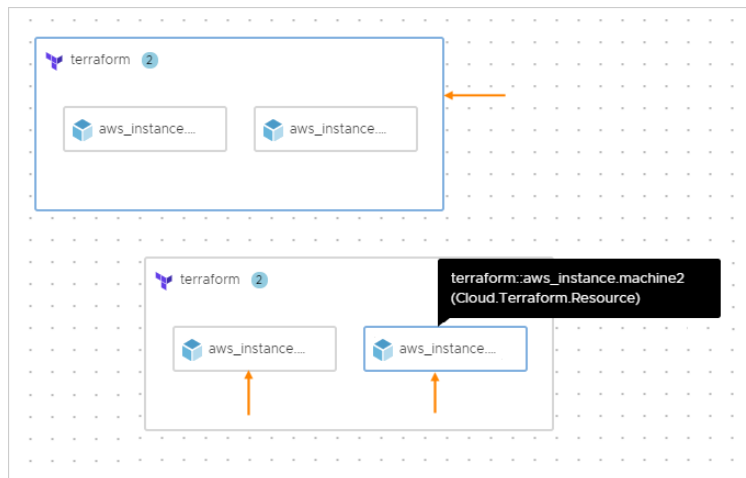
Distribuzione del modello cloud

Quando si distribuisce il modello cloud, la scheda **Cronologia** della distribuzione consente di espandere un evento, ad esempio una fase di allocazione o creazione, per analizzare un registro di messaggi dalla CLI di Terraform.

Approvazioni: oltre alle fasi di Terraform previste, ad esempio PLAN, ALLOCATE o CREATE, Cloud Assembly include la governance mediante una fase di approvazione. Per ulteriori informazioni sulle approvazioni delle richieste, vedere [Come configurare i criteri di approvazione di Service Broker](#).

Timestamp	Status	Resource type	Resource name	Details
Aug 3, 202...	PLAN_FINISHED	Cloud.Terraform.Configurati...	terraform	Creating 2 Terraform resources, updating 0 Terraform resources, deleting 0 Terraform resources
Aug 3, 202...	PLAN_IN_PROGRESS	Cloud.Terraform.Configurati...	terraform	Hide Logs
<pre> 2:24:23 PM * provider.random: version = "~> 2.3" 2:24:23 PM 2:24:23 PM Terraform has been successfully initialized! 2:24:28 PM Refreshing Terraform state in-memory prior to plan... 2:24:28 PM The refreshed state will be used to calculate this plan, but will not be 2:24:28 PM persisted to local or remote state storage. </pre>				
Aug 3, 202...	INITIALIZATION_FINISH...			
Aug 3, 202...	INITIALIZATION_IN_PRO...			

Dopo la distribuzione, viene visualizzata una risorsa esterna che rappresenta il componente Terraform complessivo, con risorse figlio interne per i componenti separati creati da Terraform. La risorsa Terraform principale controlla il ciclo di vita delle risorse figlio.



Utilizzo di una proprietà di Cloud Assembly segreta in una configurazione Terraform

È possibile applicare valori segreti crittografati alle configurazioni Terraform aggiunte alle progettazioni di modelli cloud di Cloud Assembly.

- 1 Nel repository Git, aggiungere un file di origine configurazione Terraform che faccia riferimento alle proprietà segrete come variabili.

In questo esempio di origine configurazione Terraform, le API e le chiavi dell'applicazione sono le variabili segrete.

```

variable "datadog_api_key" {
  description = "Datadog API Key"
}

```

```

variable "datadog_app_key" {
  description = "Datadog App Key"
}
provider "datadog" {
  api_key = "${var.datadog_api_key}"
  app_key = "${var.datadog_app_key}"
}

# Create a new monitor
resource "datadog_monitor" "default" {
  # ...
}

# Create a new timeboard
resource "datadog_timeboard" "default" {
  # ...
}

```

- 2 In Cloud Assembly, passare a **Infrastruttura > Amministrazione > Segreti** e immettere i valori delle proprietà segrete.

Aggiungere i nomi segreti e i valori corrispondenti. Per i nomi, è più facile immettere semplicemente lo stesso nome della variabile dell'origine Terraform.

Se necessario, vedere [Proprietà di Cloud Assembly segrete](#) per ulteriori dettagli.

Secrets			
+ NEW SECRET			
	Name	Project	Value
⋮	datadog_api_key	Terraform	*****
⋮	datadog_app_key	Terraform	*****

- 3 In Cloud Assembly, importare la configurazione di Terraform da utilizzare in un modello cloud.

Passare a **Progettazione > Modelli cloud** e fare clic su **Nuovo da > Terraform**.

Nota Anche se le variabili vengono visualizzate per la selezione nell'ultima pagina della procedura guidata, non è necessario impostare le variabili segrete come sensibili. Le variabili di Cloud Assembly saranno già crittografate e non sarà necessaria la crittografia applicata dalla procedura guidata.

Se necessario, vedere [Progettazione di configurazioni di Terraform in Cloud Assembly](#) per ulteriori dettagli.

Il modello cloud di esempio potrebbe assomigliare al codice seguente:

```

inputs:
  datadog_api_key:
    type: string
    description: Datadog API Key
  datadog_app_key:

```



```

type: string
description: Datadog App Key
resources:
  terraform:
    type: Cloud.Terraform.Configuration
    properties:
      variables:
        datadog_api_key: '${input.datadog_api_key}'
        datadog_app_key: '${input.datadog_app_key}'
      providers: []
      terraformVersion: 0.12.29
      configurationSource:
        repositoryId: 0fbf8f5e-54e1-4da3-9508-2b701gf25f51
        commitId: ed12424b249aa50439kr1c268942a4616bd751b6
        sourceDirectory: datadog

```

- 4 Nell'editor del codice, per i valori segreti, modificare manualmente `input` in `secret` come mostrato.

```

terraform:
  type: Cloud.Terraform.Configuration
  properties:
    variables:
      datadog_api_key: '${secret.datadog_api_key}'
      datadog_app_key: '${secret.datadog_app_key}'

```

- 5 Nella sezione `inputs`: del codice, rimuovere le voci di input che sono state sostituite dalle associazioni con le proprietà segrete.

Ulteriori informazioni sulle configurazioni Terraform in vRealize Automation

È necessario tenere presenti alcune limitazioni e risolvere i problemi quando si integrano le configurazioni Terraform come risorse in vRealize Automation.

Limitazioni per le configurazioni Terraform

- Quando si convalida un progetto con le configurazioni Terraform, il pulsante TEST verifica la sintassi di Cloud Assembly ma non la sintassi del codice Terraform nativo.

Inoltre, il pulsante TEST non convalida gli ID commit associati alle configurazioni Terraform.

- Per un modello cloud che include configurazioni Terraform, la clonazione del modello in un progetto diverso richiede la seguente soluzione alternativa.
 - a Nel nuovo progetto, nella scheda **Integrazioni**, copiare il valore `repositoryId` per l'integrazione.
 - b Aprire il modello del clone. Nell'editor di codice, sostituire il valore `repositoryId` con quello copiato.
- Nel repository di controllo versioni, non includere un file di stato Terraform con i file di configurazione. Se è presente `terraform.tfstate`, si verificano errori durante la distribuzione.

Azioni giorno 2 supportate per la risorsa Terraform principale

Per la risorsa Terraform principale, è possibile visualizzare o aggiornare il file di stato di Terraform. Per ulteriori informazioni sulle azioni del file di stato, vedere l'elenco completo delle azioni in [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Azioni giorno 2 supportate per le risorse secondarie

Dopo aver distribuito le configurazioni di Terraform, potrebbero essere necessari fino a 20 minuti affinché l'azione giorno 2 diventi disponibile nelle risorse secondarie.

Per le risorse secondarie in una configurazione Terraform, sono supportate solo le seguenti azioni giorno 2. Per informazioni dettagliate sulle azioni, consultare l'elenco completo delle azioni in [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Provider	Tipo di risorsa Terraform	Azioni giorno 2 supportate
AWS	aws_instance	Accendi
		Spegni
		Riavvia
		Reimposta
Azure	azurerm_virtual_machine	Accendi
		Spegni
		Riavvia
		Sospendi
vSphere	vsphere_virtual_machine	Accendi
		Spegni
		Riavvia
		Reimposta
		Shutdown
		Sospendi
		Crea snapshot
		Elimina snapshot
		Ripristina snapshot
GCP	google_compute_instance	Accendi
		Spegni

Provider	Tipo di risorsa Terraform	Azioni giorno 2 supportate
		Crea snapshot
		Elimina snapshot

Risoluzione dei problemi della disponibilità delle azioni giorno 2

Le azioni giorno 2 pronte all'uso mancanti o disattivate potrebbero richiedere la risoluzione dei problemi.

Problema	Causa	Risoluzione
Una risorsa Terraform non ha un'azione giorno 2 pronta all'uso prevista nel menu Azioni.	L'azione potrebbe non essere supportata per il provider e il tipo di risorsa menzionati nell'elenco precedente. In alternativa, la visualizzazione dell'azione potrebbe richiedere fino a 20 minuti a causa della tempistica di individuazione delle risorse e della memorizzazione nella cache delle risorse.	Controllare il provider e il tipo di risorsa nella progettazione. Attendere fino a 20 minuti per il completamento della raccolta dati.
Una risorsa Terraform non dispone di un'azione giorno 2 prevista anche dopo i 20 minuti necessari per la raccolta dati.	Un problema di individuazione delle risorse impedisce la visualizzazione dell'azione. Ciò può verificarsi, ad esempio, quando la risorsa viene accidentalmente creata in una zona cloud esterna al progetto. Ad esempio, il progetto include solo un account cloud e una zona cloud della regione us-east-1, ma la configurazione Terraform include un blocco del provider per us-west-1 e non è stato modificato in fase di progettazione. Un'altra possibilità è che la raccolta dati non funzioni.	Controllare le zone cloud del progetto rispetto alle zone cloud nella progettazione. Passare a Infrastruttura > Connessioni > Account cloud e controllare lo stato di raccolta dati e l'ultima ora di raccolta riuscita per l'account cloud.
Anche se non sono presenti problemi evidenti con lo stato e la raccolta dati della risorsa, l'azione giorno 2 è disattivata (grigia).	In alcuni casi, è noto che si verifichino problemi di tempistiche ed errori di raccolta dati intermittenti.	Il problema dovrebbe risolversi entro 20 minuti.
L'azione giorno 2 errata è disattivata, nonostante debba essere attivata in base allo stato della risorsa. Ad esempio, lo spegnimento è abilitato e l'accensione è disattivata, anche se la risorsa è stata spenta utilizzando l'interfaccia del provider.	La tempistica della raccolta dati può causare una mancata corrispondenza temporanea. Se si modifica lo stato di accensione al di fuori di vRealize Automation, è necessario del tempo per applicare correttamente la modifica.	Attendere fino a 20 minuti.

Utilizzo di provider Terraform personalizzati in vRealize Automation

Se si desidera utilizzare un provider Terraform personalizzato, eseguire i passaggi seguenti.

Nel repository di controllo della versione Git, nella directory Terraform che contiene main.tf, aggiungere la seguente struttura di sottodirectory e il file ZIP del provider Terraform.

```
terraform.d/plugins/<HOSTNAME>/<NAMESPACE>/<TYPE>/terraform-provider-
<TYPE_VERSION_TARGET>.zip
```

Ad esempio, se è stata scaricata la versione [azurerm 3.12.0](#), è possibile creare la struttura seguente.

```
terraform.d/plugins/registry.terraform.io/hashicorp/azurerm/terraform-provider-
azurerm_3.12.0_linux_amd64.zip
```

Tipi di risorse personalizzate per i modelli cloud di Cloud Assembly

Quando si crea un modello cloud in Cloud Assembly, la tavolozza dei tipi di risorse include tipi di risorse per l'account cloud e gli endpoint di integrazione supportati. In alcuni casi potrebbe essere necessario creare modelli cloud in base a un elenco esteso di tipi di risorse. È possibile creare tipi di risorse personalizzate, aggiungerle alla tela di progettazione e creare modelli cloud che supportino le esigenze di progettazione e distribuzione.

Nome della risorsa personalizzata e tipo di risorsa

Il nome della risorsa personalizzata identifica la risorsa personalizzata all'interno della tavolozza dei tipi di risorse del modello cloud.

Il tipo di risorsa di una risorsa personalizzata deve iniziare con **Custom.** e ogni tipo di risorsa deve essere univoco. Ad esempio, è possibile impostare `Custom.ADUser` come tipo di risorsa per una risorsa personalizzata che aggiunge gli utenti di Active Directory. Sebbene l'inclusione di **Custom.** non sia convalidata nella casella di testo, la stringa viene aggiunta automaticamente se viene rimossa.

Risorse personalizzate dell'azione di estendibilità

Con i tipi di risorse personalizzate, è possibile utilizzare le azioni di estendibilità nei modelli cloud per creare applicazioni complesse. Ad esempio, è possibile utilizzare l'integrazione nativa delle azioni di estendibilità con Amazon Web Services e Microsoft Azure per l'integrazione semplificata con i rispettivi servizi. È possibile creare risorse personalizzate dell'azione di estendibilità facendo clic sull'opzione **Basato su** nell'editor di risorse personalizzate e selezionando **Schema definito dall'utente ABX**.

Azioni del ciclo di vita per le risorse personalizzate dell'azione di estendibilità

Quando si utilizza un'azione di estendibilità per la risorsa personalizzata, è possibile definire le seguenti azioni del ciclo di vita:

- **Crea:** questa azione di estendibilità viene richiamata quando si avvia una distribuzione.

- **Leggi:** questa azione di estendibilità viene utilizzata per recuperare lo stato più recente della risorsa distribuita.
- **Aggiorna:** questa azione di estendibilità viene richiamata quando si aggiorna una proprietà del modello cloud. Questa azione viene attivata solo quando una proprietà non è contrassegnata con `recreateOnUpdate`.
- **Elimina:** questa azione di estendibilità viene richiamata quando si elimina una distribuzione.

Queste azioni del ciclo di vita possono essere selezionate manualmente dalle azioni di estendibilità esistenti o generate automaticamente selezionando **Genera azioni**. Quando si seleziona **Genera azioni**, è necessario specificare il progetto in cui verrà generata la nuova azione di estendibilità.

Nota È possibile modificare le azioni di estendibilità associate alle azioni del ciclo di vita facendo clic sull'opzione **Apri** accanto all'azione specifica.

Risorse personalizzate di vRealize Orchestrator

Ogni risorsa personalizzata di vRealize Orchestrator è basata su un tipo di inventario dell'SDK e viene creata da un workflow di vRealize Orchestrator con un output che è un'istanza del tipo di SDK desiderato. I tipi primitivi, ad esempio `Properties`, `Date`, `string` e `number` non sono supportati per la creazione di tipi di risorse personalizzate.

Nota I tipi di oggetti SDK possono essere differenziati da altri tipi di proprietà con i due punti (":"), utilizzati per separare il nome del plug-in e il nome del tipo. Ad esempio, `AD:UserGroup` è un tipo di oggetto SDK utilizzato per gestire i gruppi di utenti di Active Directory.

È possibile utilizzare i workflow integrati in vRealize Orchestrator oppure creare workflow personalizzati. L'utilizzo di vRealize Orchestrator per creare workflow Anything-as-a-Service (XaaS) significa che è possibile creare un modello cloud che aggiunge un utente di Active Directory alle macchine al momento della distribuzione o aggiungere un bilanciamento del carico F5 personalizzato a una distribuzione. È possibile creare risorse personalizzate di vRealize Orchestrator facendo clic sull'opzione **Basato su** nell'editor di risorse personalizzate e selezionando **Inventario di vRO**.

Tipo esterno di risorsa personalizzata di vRealize Orchestrator

La proprietà del tipo esterno definisce il tipo di risorsa personalizzata di vRealize Orchestrator. Quando si seleziona un workflow di creazione nel tipo di risorsa personalizzata in Cloud Assembly, il menu a discesa Tipo esterno viene visualizzato sotto tale workflow. Il menu a discesa include le proprietà dei tipi esterni, che vengono selezionate dai parametri di output del workflow di vRealize Orchestrator. Le proprietà di output del workflow selezionate incluse nel menu a discesa devono essere tipi di oggetti SDK non array, ad esempio `VC:VirtualMachine` o `AD:UserGroup`.

Nota Quando si creano workflow personalizzati che utilizzano il plug-in di tipo dinamico, verificare che le variabili vengano create utilizzando il metodo `DynamicTypesManager.getObject()`.

Quando si definiscono i tipi di risorse personalizzate, si definisce anche l'ambito della disponibilità del tipo esterno selezionato. Il tipo esterno selezionato può essere:

- Condiviso tra i progetti.
- Disponibile solo per il progetto selezionato.

È possibile disporre di un solo tipo di risorsa personalizzata con un valore di tipo esterno specifico per ambito definito. Ad esempio, se si crea una risorsa personalizzata nel progetto che utilizza `VC:VirtualMachine` come tipo esterno, non è possibile creare un'altra risorsa personalizzata per lo stesso progetto che utilizza lo stesso tipo di esterno. Non è inoltre possibile creare due risorse personalizzate condivise che utilizzano lo stesso tipo esterno.

Convalida dell'azione del ciclo di vita di vRealize Orchestrator

Quando si aggiungono i workflow di creazione, eliminazione e aggiornamento come azioni del ciclo di vita per la risorsa personalizzata, Cloud Assembly verifica che i workflow selezionati dispongano delle definizioni delle proprietà di input e output corrette.

- Il workflow di creazione deve disporre di un parametro di output che sia un tipo di oggetto SDK, ad esempio `SSH:Host` o `SQL:Database`. Se il workflow selezionato non supera la convalida, non è possibile aggiungere i workflow di aggiornamento o eliminazione oppure salvare le modifiche apportate alla risorsa personalizzata.
- Il workflow di eliminazione deve disporre di un parametro di input che sia un tipo di oggetto SDK che corrisponda al tipo esterno della risorsa personalizzata.
- Il workflow di aggiornamento deve disporre sia di un parametro di input che di un tipo di oggetto SDK che corrisponda al tipo esterno della risorsa personalizzata.

Schema delle proprietà delle risorse personalizzate

È possibile modificare e visualizzare lo schema delle proprietà delle risorse personalizzate selezionando la scheda **Proprietà**. Lo schema include il nome, il tipo di dati, il tipo di proprietà e, se disponibile, la descrizione di una determinata proprietà. Lo schema definisce anche se una proprietà specifica è obbligatoria o facoltativa nel modello cloud.

Nota Per lo schema della proprietà delle risorse personalizzate dell'azione di estendibilità, tutte le proprietà sono obbligatorie nel modello cloud.

Quando si aggiungono i workflow di vRealize Orchestrator alla risorsa personalizzata, i relativi parametri di input e output vengono aggiunti come proprietà. Per le risorse personalizzate dell'azione di estendibilità, è necessario creare manualmente lo schema delle proprietà delle risorse personalizzate dell'azione di estendibilità nella scheda **Proprietà**. Da questa scheda, è inoltre possibile modificare e formattare le proprietà di vRealize Orchestrator o le risorse personalizzate basate sull'azione di estendibilità. Ad esempio, è possibile modificare il nome visualizzato di una determinata proprietà o aggiungere vincoli.

Nota Quando si aggiungono vincoli alla sezione dell'elemento dei campi dell'array o alla sezione delle proprietà dei campi degli oggetti nello schema delle proprietà, verificare di aver convalidato questi vincoli perché vincoli applicati in modo errato possono causare problemi con la risorsa personalizzata. Ad esempio, quando si aggiunge un vincolo massimo a un array di numeri, è necessario verificare che questo vincolo non interrompa il valore predefinito della proprietà.

È possibile modificare lo schema della proprietà per le risorse personalizzate andando alla scheda **Proprietà** e utilizzando la scheda **Codice** o **Modulo**.

- **Codice:** consente di modificare lo schema della proprietà utilizzando il contenuto YAML.
- **Modulo:** facendo clic su **Nuova proprietà**, è possibile creare una nuova proprietà configurandone il nome, il nome visualizzato, la descrizione, il tipo di proprietà e il valore predefinito. È inoltre possibile nascondere le proprietà non obbligatorie e non elaborate dallo schema facendo clic su **Rimuovi proprietà**.

Moduli di richiesta personalizzati per operazioni giorno 2

È possibile semplificare il modulo di richiesta delle operazioni giorno 2 incluse nella risorsa personalizzata aggiungendo e modificando diversi tipi di proprietà delle risorse.

Ad esempio, è possibile associare il valore di un parametro di input nel modulo di richiesta a un'origine esterna, ad esempio un'azione di vRealize Orchestrator che recupera il nome di una distribuzione o del progetto. È inoltre possibile associare il valore di uno specifico parametro di input al valore calcolato di altre due caselle di testo incluse nello stesso modulo di richiesta.

Nota Questa funzionalità è disponibile sia per le risorse personalizzate che per le azioni risorsa. È possibile personalizzare il valore delle proprietà di input del modulo di richiesta nella scheda **Valori** della pagina **Parametri richiesta** dell'editor delle risorse personalizzate o delle azioni risorsa.

Convalida del modulo di richiesta delle operazioni giorno 2

È possibile convalidare il modulo di richiesta delle operazioni giorno 2 aggiungendo una convalida esterna. Utilizzando una convalida esterna, si impedisce all'utente di inviare il modulo di richiesta finché i parametri di convalida non vengono soddisfatti. È possibile aggiungere una convalida esterna dalla scheda **Convalide** della pagina **Parametri richiesta** dell'editor della risorsa personalizzata o dell'azione risorsa. Dopo aver selezionato la scheda, è possibile trascinare un elemento di **Convalida Orchestrator** nella tela e aggiungere un'azione vRealize Orchestrator che si desidera utilizzare per la convalida.

Ad esempio, è possibile creare una risorsa personalizzata che includa un'operazione giorno 2 per la modifica di una password utente. Per questo caso d'uso, è possibile aggiungere un'azione vRealize Orchestrator con i parametri di input `newPassword` e `confirmPassword` che utilizzano il tipo `SecureString`.

Nota Questo è uno script di esempio per la convalida della password di un utente. Per il proprio caso d'uso, è possibile decidere di utilizzare uno script diverso.

```
if (newPassword != confirmPassword) {
    return 'passwords are different';
}
if (newPassword.length < 7) {
    return 'password must be at least 10 symbols';
}
return null;
```

Come creare un modello di Cloud Assembly per aggiungere utenti ad Active Directory

Oltre alle risorse del modello cloud di Cloud Assembly utilizzate durante la creazione dei modelli cloud, è anche possibile creare risorse personalizzate.

Le risorse personalizzate sono oggetti di vRealize Orchestrator o dell'azione di estendibilità gestiti tramite vRealize Automation con le azioni del ciclo di vita definite nella risorsa personalizzata. Il servizio del modello cloud richiama automaticamente le azioni di estendibilità o i workflow di vRealize Orchestrator appropriati quando viene attivata l'operazione associata a un'azione del ciclo di vita specifica. È possibile estendere la funzionalità del tipo di risorsa selezionando anche le azioni di estendibilità o i workflow di vRealize Orchestrator che possono essere utilizzati come operazioni giorno 2.

Questo caso d'uso utilizza i workflow integrati forniti nella libreria di vRealize Orchestrator. Include stringhe o valori prescrittivi che dimostrano come eseguire il processo. È possibile modificarli per adattarli all'ambiente in uso.

A scopo di riferimento, questo caso d'uso utilizza un progetto denominato **DevOpsTesting**. È possibile sostituire questo progetto di esempio con qualsiasi progetto nell'ambiente in uso.

Prerequisiti

- Verificare di aver configurato un'integrazione di vRealize Orchestrator. Vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).
- Verificare che i workflow utilizzati per le azioni di creazione, aggiornamento, eliminazione e giorno 2 esistano e vengano eseguiti correttamente in vRealize Orchestrator.
- In vRealize Orchestrator, individuare il tipo di risorsa utilizzato dai workflow. I workflow inclusi in questa risorsa personalizzata devono utilizzare lo stesso tipo di risorsa. In questo caso d'uso, il tipo di risorsa è `AD:User`. Per ulteriori informazioni sulla convalida dei tipi di risorse, vedere [Tipi di risorse personalizzate per i modelli cloud di Cloud Assembly](#).

- Utilizzando i workflow di Active Directory incorporati nell'integrazione di vRealize Orchestrator, configurare un server di Active Directory.
- Assicurarsi di essere in grado di configurare e distribuire il modello cloud di una macchina.

Procedura

- 1 Creare una risorsa personalizzata di Active Directory per l'aggiunta di un utente in un gruppo.

Questo passaggio aggiunge la risorsa personalizzata alla tela di progettazione del modello cloud come tipo di risorse.

- a In Cloud Assembly, selezionare **Progettazione > Risorse personalizzate**, quindi fare clic su **Nuova risorsa personalizzata**.
- b Specificare i valori seguenti.

Tenere presente che, ad eccezione dei nomi dei workflow, si tratta di valori di esempio.

Impostazione	Valore di esempio
Nome	AD user Questo è il nome visualizzato nella tavolozza delle risorse dei modelli cloud.
Tipo di risorsa	Custom.ADUser Il tipo di risorsa deve iniziare con Custom. e ogni tipo di risorsa deve essere univoco. Sebbene l'inclusione di Custom. non sia convalidata nella casella di testo, la stringa viene aggiunta automaticamente se viene rimossa. Questo tipo di risorsa viene aggiunto alla tavolozza dei tipi di risorse affinché sia possibile utilizzarla nel modello cloud.

- c Per abilitare questo tipo di risorsa nell'elenco dei tipi di risorse dei modelli cloud, verificare che l'opzione **Attiva** sia attivata.
- d Selezionare l'impostazione **Ambito** che rende il tipo di risorsa disponibile per qualsiasi progetto.
- e In **Basato su**, verificare che **Inventario di vRO** sia selezionato come provider di azioni del ciclo di vita.

- f Selezionare i workflow che definiscono la risorsa e le azioni giorno 2.

Nota I workflow del giorno 2 selezionati devono avere un parametro di input dello stesso tipo del tipo esterno. L'input del tipo esterno non viene visualizzato nel modulo personalizzato del giorno 2 richiesto dall'utente, poiché viene automaticamente associato alla risorsa personalizzata.

Impostazione	Valore di esempio
Azioni del ciclo di vita - Crea	<p>Selezionare il workflow Crea utente con password in un'unità organizzativa.</p> <p>Se si dispone di più integrazioni di vRealize Orchestrator, selezionare il workflow nell'istanza di integrazione utilizzato per eseguire queste risorse personalizzate.</p> <p>Dopo aver selezionato il workflow, il menu a discesa Tipo esterno diventa disponibile e viene impostato automaticamente su <code>AD:User</code>.</p> <p>Nota Un tipo di origine esterna può essere utilizzato solo una volta se condiviso e una volta per progetto. In questo caso d'uso, si sta fornendo la stessa risorsa personalizzata per tutti i progetti. Ciò significa che non è possibile utilizzare <code>AD:User</code> per qualsiasi altro tipo di risorsa per tutti i progetti. Se sono presenti altri workflow che richiedono il tipo <code>AD:User</code>, è necessario creare singole risorse personalizzate per ogni progetto.</p>
Azioni del ciclo di vita - Elimina	Selezionare il workflow Elimina utente .
Azioni aggiuntive	<p>Selezionare il workflow Modifica password utente.</p> <p>Nella finestra Aggiungi azione, assegnare un nome all'azione, ad esempio <code>password_change</code>, quindi fare clic su Aggiungi.</p> <p>Per modificare il modulo di richiesta dell'azione a cui l'utente risponde quando richiede l'azione, fare clic sull'icona Parametri richiesta.</p> <p>Nota Per ulteriori workflow di azione, verificare che il workflow disponga di un parametro di input dello stesso tipo del tipo esterno.</p>

In questo esempio, non è presente alcuna applicazione appropriata di un workflow di aggiornamento. Un esempio comune di un workflow di aggiornamento, che apporta modifiche alla risorsa personalizzata sottoposta a provisioning, è rappresentato dalla scalabilità verticale oppure orizzontale di una distribuzione.

- g Rivedere la chiave dello schema e i valori del tipo nella scheda **Proprietà** per comprendere gli input del workflow e configurarli nel modello cloud.

Lo schema elenca i valori di input obbligatori e facoltativi definiti nel workflow. I valori di input richiesti sono inclusi nel file YAML del modello cloud.

Nel workflow **Crea utente**, `accountName`, `displayName` e `ouContainer` sono valori di input obbligatori. Le altre proprietà dello schema non sono obbligatorie. È inoltre possibile utilizzare lo schema per determinare dove si desidera creare associazioni con altri valori di campi, workflow o azioni. Le associazioni non sono incluse in questo caso d'uso.

- h Per completare la creazione della risorsa personalizzata, fare clic su **Crea**.

2 Creare un modello cloud che aggiunga l'utente a una macchina durante la distribuzione.

- a Selezionare **Progettazione > Modelli cloud** e fare clic su **Nuovo da > Tela vuota**.
- b Assegnare al modello cloud il nome **Macchina con un utente AD**.
- c Selezionare il progetto **DevOpsTesting** e fare clic su **Crea**.
- d Aggiungere e configurare una macchina vSphere.
- e Dall'elenco di risorse personalizzate a sinistra della pagina di progettazione del modello cloud, trascinare il tipo di risorse **AD user** sulla tela.

Nota È possibile selezionare la risorsa personalizzata scorrendo verso il basso e selezionandola dal riquadro a sinistra oppure cercandola nella casella di testo **Cerca tipi di risorse**. Se la risorsa personalizzata non viene visualizzata, fare clic sul pulsante **Aggiorna** accanto alla casella di testo **Cerca tipi di risorse**.

- f A destra, modificare il codice YAML per aggiungere la password e i valori di input obbligatori.

Aggiungere una sezione `inputs` nel codice affinché gli utenti possano fornire il nome degli utenti che stanno aggiungendo. Nell'esempio seguente, alcuni di questi valori sono dati di esempio. I valori potrebbero essere diversi.

```
inputs:
  accountName:
    type: string
    title: Account name
    encrypted: true
  displayName:
    type: string
    title: Display name
  password:
    type: string
    title: Password
    encrypted: true
  confirmPassword:
    type: string
    title: Password
    encrypted: true
  ouContainer:
    type: object
    title: AD OU container
    $data: 'vro/data/inventory/AD:OrganizationalUnit'
    properties:
      id:
        type: string
      type:
        type: string
```

- g Nella sezione `resources`, aggiungere il codice `${input.input-name}` per richiedere la selezione dell'utente.

```
resources:
  Custom_ADUser_1:
    type: Custom.ADUser
    properties:
      accountName: '${input.accountName}'
      displayName: '${input.displayName}'
      ouContainer: '${input.ouContainer}'
      password: '${input.password}'
      confirmPassword: '${input.confirmPassword}'
```

3 Distribuire il modello cloud.

- a Nella pagina del progettista del modello cloud, fare clic su **Distribuisci**.
- b Nel campo **Nome della distribuzione**, immettere **AD User Scott**.

- c Selezionare la versione del modello cloud in **Versione modello cloud**, quindi fare clic su **Avanti**.
 - d Completare gli input della distribuzione.
 - e Fare clic su **Distribuisci**.
- 4 Monitorare la richiesta di provisioning nella pagina **Distribuzioni** per assicurarsi che l'utente venga aggiunto ad Active Directory e che la distribuzione venga eseguita correttamente.

Operazioni successive

Quando il modello cloud testato è in uso, è possibile iniziare a utilizzare la risorsa personalizzata **AD user** con altri modelli cloud.

Come creare un modello di Cloud Assembly che includa SSH

È possibile creare risorse personalizzate utilizzabili per modelli cloud mediante workflow di vRealize Orchestrator. In questo caso d'uso, si aggiunge una risorsa personalizzata che aggiunge un host SSH. La risorsa può quindi essere inclusa nei modelli cloud. Questa procedura aggiunge anche un workflow di aggiornamento in modo che gli utenti possano modificare la configurazione SSH dopo la distribuzione anziché eseguire singole azioni giorno 2.

Le risorse personalizzate sono oggetti di vRealize Orchestrator o dell'azione di estendibilità gestiti tramite vRealize Automation con le azioni del ciclo di vita definite nella risorsa personalizzata. Il servizio del modello cloud richiama automaticamente le azioni di estendibilità o i workflow di vRealize Orchestrator appropriati quando viene attivata l'operazione associata a un'azione del ciclo di vita specifica. È possibile estendere la funzionalità del tipo di risorsa selezionando anche le azioni di estendibilità o i workflow di vRealize Orchestrator che possono essere utilizzati come operazioni giorno 2.

Questo caso d'uso utilizza i workflow integrati forniti nella libreria di vRealize Orchestrator. Include stringhe o valori prescrittivi che dimostrano come eseguire il processo. È possibile modificarli per adattarli all'ambiente in uso.

A scopo di riferimento, questo caso d'uso utilizza un progetto denominato **DevOpsTesting**. È possibile sostituire il progetto con uno già esistente.

Prerequisiti

- Verificare di aver configurato un'integrazione di vRealize Orchestrator. Vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).
- Verificare che i workflow utilizzati per le azioni di creazione, aggiornamento, eliminazione e giorno 2 esistano e vengano eseguiti correttamente in vRealize Orchestrator.
- In vRealize Orchestrator, individuare il tipo di risorsa utilizzato dai workflow. I workflow inclusi in questa risorsa personalizzata devono utilizzare lo stesso tipo di risorsa. In questo caso d'uso, il tipo di risorsa è `SSH:Host`. Per ulteriori informazioni sulla convalida dei tipi di risorse, vedere [Tipi di risorse personalizzate per i modelli cloud di Cloud Assembly](#).
- Assicurarsi di essere in grado di configurare e distribuire il modello cloud di una macchina.

Procedura

- 1 Creare una risorsa personalizzata dell'host SSH per l'aggiunta di SSH a un modello cloud.

Questo passaggio aggiunge la risorsa personalizzata alla tela di progettazione del modello cloud come tipo di risorsa.

- a In Cloud Assembly, selezionare **Progettazione > Risorse personalizzate**, quindi fare clic su **Nuova risorsa personalizzata**.
- b Specificare i valori seguenti.

Tenere presente che, ad eccezione dei nomi dei workflow, si tratta di valori di esempio.

Tabella 6-3.

Impostazione	Valore di esempio
Nome	SSH Host - DevOpsTesting Project Questo è il nome visualizzato nella tavolozza delle risorse dei modelli cloud.
Tipo di risorsa	Custom.SSHHost Il tipo di risorsa deve iniziare con Custom. e ogni tipo di risorsa deve essere univoco. Sebbene l'inclusione di Custom. non sia convalidata nella casella di testo, la stringa viene aggiunta automaticamente se viene rimossa. Questo tipo di risorsa viene aggiunto alla tela di progettazione affinché sia possibile utilizzarla nel modello cloud.

- c Per abilitare questo tipo di risorsa nell'elenco dei tipi di risorse dei modelli cloud, verificare che l'opzione **Attiva** sia attivata.
- d Selezionare l'impostazione **Ambito** che rende il tipo di risorsa disponibile per il progetto **DevOpsTesting**.
- e In **Basato su**, verificare che **Inventario di vRO** sia selezionato come provider di azioni del ciclo di vita.

- f Selezionare i workflow che definiscono la risorsa.

Impostazione	Impostazione
Azioni del ciclo di vita - Crea	<p>Selezionare il workflow Aggiungi SSH Host.</p> <p>Se si dispone di più integrazioni di vRealize Orchestrator, selezionare il workflow nell'istanza di integrazione utilizzato per eseguire queste risorse personalizzate.</p> <p>Dopo aver selezionato il workflow, il menu a discesa Tipo esterno diventa disponibile e viene impostato automaticamente su <code>SSH:Host</code>. Un tipo di origine esterna può essere utilizzato solo una volta se condiviso e una volta per progetto. In questo caso d'uso, si fornisce la risorsa personalizzata solo per il progetto DevOpsTesting. Se sono presenti altri workflow che richiedono il tipo <code>SSH:Host</code>, è necessario creare singole risorse personalizzate per ogni progetto.</p>
Azioni del ciclo di vita - Aggiorna	Selezionare il workflow Aggiorna SSH Host .
Azioni del ciclo di vita - Elimina	Selezionare il workflow Rimuovi SSH Host .

- g Rivedere la chiave dello schema e i valori del tipo nella scheda **Proprietà** per comprendere gli input del workflow e configurarli nel modello cloud.

Lo schema elenca i valori di input obbligatori e facoltativi definiti nel workflow. I valori di input richiesti sono inclusi nel file YAML del modello cloud.

Nel workflow **Aggiungi SSH Host**, `hostname`, `port` e `username` sono valori di input obbligatori. Le altre proprietà dello schema non sono obbligatorie. È inoltre possibile utilizzare lo schema per determinare dove si desidera creare associazioni con altri valori di campi, workflow o azioni. Le associazioni non sono incluse in questo caso d'uso.

- h Per completare la creazione della risorsa personalizzata, fare clic su **Crea**.

- 2 Creare un modello cloud che aggiunga l'host SSH quando lo si distribuisce.
 - a Selezionare **Progettazione > Modelli cloud** e fare clic su **Nuovo da > Tela vuota**.
 - b Assegnare al modello cloud il nome **Macchina con SSH Host**.
 - c Selezionare il progetto **DevOpsTesting** e fare clic su **Crea**.
 - d Aggiungere e configurare una macchina vSphere.

- e Dall'elenco di risorse personalizzate a sinistra della pagina di progettazione del modello cloud, trascinare il tipo di risorsa **SSH Host - DevOpsTesting Project** sulla tela.

Nota È possibile selezionare la risorsa personalizzata scorrendo verso il basso e selezionandola dal riquadro a sinistra oppure cercandola nella casella di testo **Cerca tipi di risorse**. Se la risorsa personalizzata non viene visualizzata, fare clic sul pulsante **Aggiorna** accanto alla casella di testo **Cerca tipi di risorse**.

Si noti che il tipo di risorsa è disponibile perché è stato configurato per il progetto. Se si stesse creando un modello cloud per un altro progetto, il tipo di risorsa non sarebbe visibile.

- f A destra, modificare il codice YAML per aggiungere i valori di input obbligatori.

Aggiungere una sezione `inputs` nel codice, in modo che gli utenti possano fornire il nome utente e il nome host al momento della distribuzione. In questo esempio, la porta predefinita è 22. Nell'esempio seguente, alcuni di questi valori sono dati di esempio. I valori potrebbero essere diversi.

```
inputs:
  hostname:
    type: string
    title: The hostname of the SSH Host
  username:
    type: string
    title: Username
```

- g Nella sezione `resources`, aggiungere il codice `${input.input-name}` per richiedere la selezione dell'utente.

```
resources:
  Custom_SSHTHost_1:
    type: Custom.SSHTHost
    properties:
      port: 22
      hostname: '${input.hostname}'
      username: '${input.username}'
```

3 Distribuire il modello cloud.

- a Nella pagina del progettista del modello cloud, fare clic su **Distribuisci**.
- b Immettere il **Nome della distribuzione** **Test SSH Host**.
- c Selezionare la versione del modello cloud in **Versione modello cloud**, quindi fare clic su **Avanti**.
- d Completare gli input della distribuzione.
- e Fare clic su **Distribuisci**.

- 4 Monitorare la richiesta di provisioning nella pagina **Distribuzioni** per assicurarsi che l'host SSH sia incluso nella distribuzione e che la distribuzione venga eseguita correttamente.

Operazioni successive

Quando il modello cloud testato è in uso, è possibile iniziare a utilizzare la risorsa personalizzata SSH Host con altri modelli cloud.

Progettazioni di Cloud Assembly per prepararsi alle modifiche giorno 2

Oltre alle azioni giorno 2 già associate ai tipi di risorse di Cloud Assembly, sono disponibili opzioni di progettazione che consentono di preparare in anticipo gli aggiornamenti personalizzati che gli utenti potrebbero dover apportare.

Attenzione Per modificare una distribuzione, è possibile modificarne il modello cloud e riapplicarlo oppure utilizzare le azioni del giorno 2. Nella maggior parte dei casi, è comunque consigliabile evitare di combinare i due approcci.

Le modifiche del ciclo di vita del giorno 2, come l'accensione e lo spegnimento, sono in genere sicure, ma altre, come l'aggiunta di dischi, richiedono cautela.

Ad esempio, se si aggiungono dischi con un'azione del giorno 2 e quindi si adotta un approccio misto riapplicando il modello cloud, il modello cloud potrebbe sovrascrivere la modifica del giorno 2 rimuovendo i dischi e causando la perdita di dati.

La preparazione del giorno 2 può coinvolgere l'uso diretto del codice del modello cloud o l'interfaccia di progettazione di Cloud Assembly.

- È possibile utilizzare gli input nel codice del modello cloud in modo che, quando si aggiorna la distribuzione o la risorsa distribuita, l'interfaccia richieda valori aggiornati.
- È possibile utilizzare Cloud Assembly per progettare un'azione personalizzata basata su un'azione di estendibilità o un workflow di vRealize Orchestrator. L'esecuzione dell'azione personalizzata implica che l'azione di estendibilità o il workflow apporti modifiche alla distribuzione o alla risorsa distribuita.

Come utilizzare gli input del modello cloud per gli aggiornamenti giorno 2 di vRealize Automation

Quando si progettano i modelli cloud di vRealize Automation, i parametri di input consentono agli utenti giorno 2 di reimmettere le selezioni dalla richiesta di distribuzione iniziale.

Attenzione Alcune modifiche alle proprietà comportano la ricreazione di una risorsa.

Ad esempio, la modifica di `connection_string.name` in un `Cloud.Service.Azure.App.Service` comporta l'eliminazione della risorsa esistente e la creazione di una nuova risorsa.

Quando si progettano input per il supporto delle modifiche del giorno 2, lo schema dei [modelli contenuti in code.vmware.com](#) consente di individuare le proprietà che eliminano e ricreano le risorse.

Per informazioni sulla creazione degli input, vedere [Input dell'utente nelle richieste di vRealize Automation](#).

Per un esempio specifico del giorno 2, vedere la sezione seguente.

Spostamento di una macchina distribuita in un'altra rete

Pur mantenendo le distribuzioni e le reti, potrebbe essere necessario trasferire le macchine distribuite con Cloud Assembly.

Ad esempio, è possibile che si desideri distribuire prima in una rete di test per poi passare a una rete di produzione. La tecnica descritta qui consente di progettare un modello cloud in anticipo per preparare tali azioni giorno 2. Si noti che la macchina è stata spostata. Non viene eliminata e ridistribuita.

Questa procedura si applica solo alle risorse **Cloud.vSphere.Machine**. Non è valida per le macchine indipendenti dal cloud distribuite in vSphere.

Prerequisiti

- Il profilo di rete di Cloud Assembly deve includere tutte le subnet a cui la macchina si conatterà. In Cloud Assembly, è possibile controllare le reti passando a **Infrastruttura > Configura > Profili di rete**.
Il profilo di rete deve trovarsi in un account e in una regione che facciano parte del progetto di Cloud Assembly appropriato per gli utenti.
- Contrassegnare le due subnet con tag diversi. L'esempio che segue presuppone che **test** e **prod** siano i nomi dei tag.
- La macchina distribuita deve avere lo stesso tipo di assegnazione IP. Non può passare da static a DHCP o viceversa durante il passaggio a un'altra rete.

Procedura

- 1 In Cloud Assembly, passare a **Progettazione** e creare un modello cloud per la distribuzione.

- 2 Nella sezione inputs del codice, aggiungere una voce che consenta all'utente di selezionare una rete.

```
inputs:
  net-tagging:
    type: string
    enum:
      - test
      - prod
    title: Select a network
```

- 3 Nella sezione resources del codice, aggiungere la rete **Cloud.Network** e connettere la macchina vSphere a essa.
- 4 In **Cloud.Network**, creare un vincolo che faccia riferimento alla selezione dagli input.

```
resources:
  ABCServer:
    type: Cloud.vSphere.Machine
    properties:
      name: abc-server
      . . .
    networks:
      - network: '${resource["ABCNet"].id}'
  ABCNet:
    type: Cloud.Network
    properties:
      name: abc-network
      . . .
    constraints:
      - tag: '${input.net-tagging}'
```

- 5 Continuare con la progettazione e distribuirla normalmente. Durante la distribuzione, l'interfaccia richiede di selezionare la rete **test** o **prod**.
- 6 Quando è necessario apportare una modifica al giorno 2, passare a **Risorse > Distribuzioni** e individuare la distribuzione associata al modello cloud.
- 7 A destra della distribuzione, fare clic su **Azioni > Aggiorna**.
- 8 Nel pannello Aggiorna, anche in questo caso l'interfaccia richiede di selezionare la rete **test** o **prod**.
- 9 Per modificare le reti, effettuare la selezione, fare clic su **Avanti**, quindi fare clic su **Invia**.

Come creare un'azione risorsa di Cloud Assembly in una macchina virtuale vMotion

Dopo aver distribuito un modello cloud, è possibile eseguire azioni giorno 2 che modificano la distribuzione. Cloud Assembly include molte azioni giorno 2, tuttavia è possibile utilizzarne altre. È possibile creare azioni di risorse personalizzate e renderle disponibili per gli utenti come azioni giorno 2.

Le azioni di risorse personalizzate si basano sui workflow di vRealize Orchestrator.

Questo esempio di azione risorsa del giorno 2 personalizzata ha lo scopo di introdurre il processo di creazione. Per utilizzare le azioni risorsa in modo efficace, è necessario essere in grado di creare workflow e azioni di vRealize Orchestrator che eseguono le attività necessarie.

Prerequisiti

- Verificare di aver configurato un'integrazione di vRealize Orchestrator. Vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).
- Verificare che il workflow utilizzato per l'azione giorno 2 esista in vRealize Orchestrator e che venga eseguito correttamente.

Procedura

- 1 Creare un'azione di risorsa personalizzata che utilizzi vMotion per spostare una macchina virtuale vSphere da un host a un altro.
 - a In Cloud Assembly, selezionare **Progettazione > Azioni risorsa** e fare clic su **Nuova azione risorsa**.
 - b Specificare i valori seguenti.

Tenere presente che, ad eccezione dei nomi dei workflow, si tratta di valori di esempio.

Impostazione	Valore di esempio
Nome	vSphere_VM_vMotion Questo è il nome visualizzato nell'elenco Azioni risorsa.
Nome visualizzato	Move VM Questo è il nome visualizzato dagli utenti nel menu Azioni di distribuzione.

- c Fare clic sull'opzione **Attiva** per abilitare questa azione nel menu Azioni giorno 2 per le risorse che corrispondono al tipo di risorsa.
- d Selezionare il tipo di risorsa e il workflow che definiscono l'azione giorno 2.

Impostazione	Valore di esempio
Tipo di risorsa	<p>Selezionare il tipo di risorsa Cloud.vSphere.Machine. Questo è il tipo di risorsa distribuito come componente del modello cloud, non necessariamente quello che si trova nel modello cloud. Ad esempio, è possibile che nel modello cloud sia presente una macchina indipendente dal cloud, ma quando questa viene distribuita in un vCenter Server, la macchina è Cloud.vSphere.Machine. Poiché l'azione si applica al tipo distribuito, non utilizzare tipi indipendenti dal cloud quando si definiscono le azioni risorsa.</p> <p>In questo esempio, vMotion funziona solo per le macchine vSphere, ma è possibile che si verifichino altre azioni che si desidera eseguire su più tipi di risorse. È necessario creare un'azione per ogni tipo di risorsa.</p>
Workflow	<p>Selezionare il workflow Migrate virtual machine with vMotion.</p> <p>Se si dispone di più integrazioni di vRealize Orchestrator, selezionare il workflow nell'istanza di integrazione utilizzato per eseguire queste azioni di risorse personalizzate.</p>

- 2 Creare un binding per le proprietà di vRealize Orchestrator con le proprietà dello schema di Cloud Assembly. Le azioni giorno 2 di Cloud Assembly supportano tre tipi di binding.

Tipo di binding	Descrizione
in request	Il tipo di binding del valore predefinito. Quando questa opzione è selezionata, la proprietà di input viene visualizzata nel modulo di richiesta e il relativo valore deve essere fornito dall'utente al momento della richiesta.
with binding action	<p>Questa opzione è disponibile solo per gli input del tipo di riferimento, come ad esempio:</p> <ul style="list-style-type: none"> ■ VC:VirtualMachine ■ VC:Folder <p>L'utente seleziona un'azione che esegue il binding. L'azione selezionata deve restituire lo stesso tipo del parametro di input. La definizione della proprietà corretta è <code>\${properties.someProperty}</code>.</p>
direct	Questa opzione è disponibile per le proprietà di input che utilizzano tipi di dati primitivi. Se questa opzione è selezionata, la proprietà, con il tipo appropriato, viene mappata direttamente dallo schema della proprietà di input. L'utente seleziona la proprietà dalla struttura dello schema. Le proprietà con tipi diversi sono disabilitate.

In questo caso d'uso, il binding è un'azione di vRealize Orchestrator che crea la connessione tra il tipo di input `VC:VirtualMachine` di vRealize Orchestrator utilizzato nel workflow e il tipo di risorsa `Cloud.vSphere.Machine` di Cloud Assembly. Impostando il binding, è possibile rendere l'azione giorno 2 semplice per l'utente che richiede l'azione `vMotion` in una macchina virtuale vSphere. Il sistema fornisce il nome nel workflow al posto dell'utente.

- a Dopo aver selezionato il workflow **Migrate virtual machine with vMotion**, passare al riquadro **Binding proprietà**.
- b Selezionare il binding della proprietà di input `vm`.
- c In **Binding**, selezionare **with binding action**.

L'azione **findVcVmByVcAndVmUuid** viene selezionata automaticamente. Questa azione è preconfigurata con l'integrazione di vRealize Orchestrator in Cloud Assembly.

- d Fare clic su **Salva**.

- 3 Per salvare le modifiche apportate all'azione giorno 2, fare clic su **Crea**.

- 4 Per tenere conto degli altri parametri di input nel workflow, è possibile personalizzare il modulo di richiesta che gli utenti visualizzano quando richiedono l'azione.

- a Da **Azioni risorsa**, selezionare l'azione giorno 2 appena creata.
- b Fare clic su **Modifica parametri richiesta**.

È possibile personalizzare la modalità con cui viene la pagina di richiesta viene visualizzata per gli utenti.

Nome campo predefinito	Aspetto	Valori	Vincoli
Pool di risorse di destinazione per la macchina virtuale. L'impostazione predefinita è il pool di risorse corrente.	<ul style="list-style-type: none"> ■ Etichetta = Pool di risorse di destinazione ■ Visualizza tipo = Selezione valore 		
Host di destinazione in cui eseguire la migrazione della macchina virtuale	<ul style="list-style-type: none"> ■ Etichetta = Host di destinazione ■ Visualizza tipo = Selezione valore 		Obbligatorio = Sì
Priorità dell'attività di migrazione	Etichetta = Priorità dell'attività	Opzioni valore <ul style="list-style-type: none"> ■ Origine valore = Costante <p>Nella casella di testo, immettere un elenco separato da virgole.</p> <pre>lowPriority Low,defaultPri ority Default,highPr iority High</pre>	Obbligatorio = Sì
(Facoltativo) Eseguire la migrazione della macchina virtuale solo se lo stato di accensione corrisponde allo stato specificato	Eliminare questa casella di testo. vMotion può spostare le macchine in qualsiasi stato di accensione.		

- c Fare clic su **Salva**.

- 5 Per limitare la disponibilità dell'azione, è possibile configurare le condizioni.

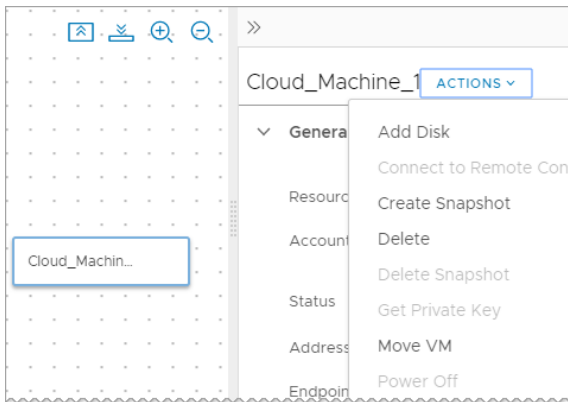
Ad esempio, si desidera che l'azione vMotion sia disponibile solo quando la macchina dispone di quattro CPU al massimo.

- a Attivare **Richiede condizione**.
- b Immettere la condizione.

Key	Operatore	Valore
\${properties.cpuCount}	lessThan	4

Se sono necessarie condizioni complesse, vedere [Come creare condizioni avanzate per le azioni personalizzate di Cloud Assembly](#).

- c Fare clic su **Aggiorna**.
- 6 Verificare che l'azione Move VM sia disponibile per le macchine distribuite che soddisfano i criteri.
- a Selezionare **Distribuzioni**.
 - b Individuare una distribuzione che includa una macchina distribuita corrispondente ai criteri definiti.
 - c Aprire la distribuzione e selezionare la macchina.
 - d Fare clic su Azioni nel riquadro destro e verificare che l'azione `Move VM` esista.



- e Eseguire l'azione.

Come creare condizioni avanzate per le azioni personalizzate di Cloud Assembly

In alternativa all'elenco di condizioni semplici in Cloud Assembly, l'editor avanzato consente di assemblare espressioni di criteri più complesse per controllare quando l'azione è disponibile.

Quando si crea una nuova azione risorsa, selezionare **Richiede condizione** e **Usa editor avanzato**. Immettere quindi l'espressione dei criteri desiderata.



L'espressione è una clausola o un elenco di clausole, ognuna delle quali è nel formato key-operator-value. Nella figura precedente sono illustrati i criteri in cui la destinazione deve essere accesa e presente.

Clausole

Clausola	Descrizione	Esempio
e	Affinché il risultato dell'espressione sia true, tutte le clausole secondarie devono essere true.	<div>Viene valutato come true solo quando properties.powerState è ON e syncStatus non è MISSING.</div> <pre>matchCondition: - and: - key: properties.powerState operator: eq value: ON - key: syncStatus operator: notEq value: MISSING</pre>
o	Affinché il risultato dell'espressione sia true, una o più clausole secondarie devono essere true.	<div>Viene valutato come true se properties.powerState è ON oppure OFF.</div> <pre>matchCondition: - or: - key: properties.powerState operator: eq value: ON - key: properties.powerState operator: eq value: OFF</pre>

Operatori

Operatore	Descrizione	Esempio
eq	Uguale. Cerca una corrispondenza esatta.	Viene valutato come true quando properties.powerState è ON. <pre>matchExpression: - and: - key: properties.powerState operator: eq value: ON</pre>
notEq	Non uguale. Evita una corrispondenza esatta.	Viene valutato come true quando properties.powerState non è OFF. <pre>matchExpression: - and: - key: properties.powerState operator: notEq value: OFF</pre>
hasAny	Cerca una corrispondenza in una raccolta di oggetti.	Viene valutato come true quando l'array storage.disks include un oggetto EBS di 100 IOPS. <pre>matchExpression: - key: storage.disks operator: hasAny value: matchExpression: - and: - key: iops operator: eq value: 100 - key: service operator: eq value: ebs</pre>
in	Cerca una corrispondenza in un set di valori.	Viene valutato come true quando properties.powerState è OFF o SUSPEND. <pre>matchExpression: - and: - key: properties.powerState operator: in value: OFF, SUSPEND</pre>
notIn	Evita una corrispondenze di un set di valori.	Viene valutato come true quando properties.powerState non è né OFF né SUSPEND. <pre>matchExpression: - and: - key: properties.powerState operator: notIn value: OFF, SUSPEND</pre>

Operatore	Descrizione	Esempio
greaterThan	Cerca una corrispondenza oltre una determinata soglia. Si applica solo a valori numerici.	Viene valutato come true quando il primo oggetto nell'array storage.disks presenta un valore di IOPS superiore a 50. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: greaterThan value: 50</pre>
lessThan	Cerca una corrispondenza inferiore a una determinata soglia. Si applica solo a valori numerici.	Viene valutato come true quando il primo oggetto nell'array storage.disks presenta un valore di IOPS inferiore a 200. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: lessThan value: 200</pre>
greaterThanEquals	Cerca una corrispondenza pari o superiore a una determinata soglia. Si applica solo a valori numerici.	Viene valutato come true quando il primo oggetto nell'array storage.disks presenta un valore di IOPS pari o superiore a 100. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: greaterThanEquals value: 100</pre>
lessThanEquals	Cerca una corrispondenza pari o inferiore a una determinata soglia. Si applica solo a valori numerici.	Viene valutato come true quando il primo oggetto nell'array storage.disks presenta un valore di IOPS pari o inferiore a 100. <pre>matchExpression: - and: - key: storage.disks[0].iops operator: lessThanEquals value: 100</pre>
matchesRegex	Utilizza un'espressione regolare per cercare una corrispondenza.	Viene valutato come true quando properties.zone è us-east-1a o us-east-1c. <pre>matchExpression: - and: - key: properties.zone operator: matchesRegex value: (us-east-1)+(a c) {1,2}</pre>

Esempi

La seguente espressione di criteri viene valutata come true quando properties.tags include un tag con key `key1` e value `value1`.

L'espressione esterna utilizza `hasAny` perché `properties.tags` è un array e si desidera che venga valutato come `true` ogni volta che `key1=value1` viene visualizzato in qualsiasi coppia key-value nell'array.

Nell'espressione interna sono presenti due clausole, una per il campo `key` e una per il campo `value`. L'array `properties.tags` contiene coppie di tag key-value ed è necessario che corrisponda sia al campo `key` che al campo `value`.

```
matchExpression:
- key: properties.tags
  operator: hasAny
  value:
    matchExpression:
      - and:
        - key: key
          operator: eq
          value: key1
        - key: value
          operator: eq
          value: value1
```

La seguente espressione dei criteri è simile all'esempio precedente, ma ora viene valutata come `true` ogni volta che `properties.tags` include un tag `key1=value1` o `key2=value2`.

```
matchExpression:
- or:
  - key: properties.tags
    operator: hasAny
    value:
      matchExpression:
        - and:
          - key: key
            operator: eq
            value: key1
          - key: value
            operator: eq
            value: value1
  - key: properties.tags
    operator: hasAny
    value:
      matchExpression:
        - and:
          - key: key
            operator: eq
            value: key2
          - key: value
            operator: eq
            value: value2
```

Altri esempi di codice di Cloud Assembly

Il codice del modello cloud in Cloud Assembly ha combinazioni e applicazioni pressoché illimitate.

Spesso un esempio di codice riuscito è il punto di partenza migliore per un ulteriore sviluppo. Quando si segue un esempio, effettuare le opportune sostituzioni per applicare le impostazioni del proprio sito in termini di nomi di risorse, valori e così via.

Esempio di modello di Cloud Assembly documentato

Includendo un insieme accurato di commenti, questo esempio consente di rivedere la struttura e lo scopo delle sezioni in un modello di Cloud Assembly, precedentemente denominato blueprint.

```
# *****
#
# This WordPress cloud template is enhanced with comments to explain its
# parameters.
#
# Try cloning it and experimenting with its YAML code. If you're new to
# YAML, visit yaml.org for general information.
#
# The cloud template deploys a minimum of 3 virtual machines and runs scripts
# to install packages.
#
# *****
#
# -----
# Templates need a descriptive name and version if
# source controlled in git.
# -----
name: WordPress Template with Comments
formatVersion: 1
version: 1
#
# -----
# Inputs create user selections that appear at deployment time. Inputs
# can set placement decisions and configurations, and are referenced
# later, by the resources section.
# -----
inputs:
#
# -----
# Choose a cloud endpoint. 'Title' is the visible
# option text (oneOf allows for the friendly title). 'Const' is the
# tag that identifies the endpoint, which was set up earlier, under the
# Cloud Assembly Infrastructure tab.
# -----
platform:
  type: string
  title: Deploy to
  oneOf:
    - title: AWS
      const: aws
    - title: Azure
      const: azure
    - title: vSphere
      const: vsphere
  default: vsphere
```

```

#
# -----
# Choose the operating system. Note that the Cloud Assembly
# Infrastructure must also have an AWS, Azure, and vSphere Ubuntu image
# mapped. In this case, enum sets the option that you see, meaning there's
# no friendly title feature this time. Also, only Ubuntu is available
# here, but having this input stubbed in lets you add more operating
# systems later.
# -----
osimage:
  type: string
  title: Operating System
  description: Which OS to use
  enum:
    - Ubuntu
#
# -----
# Set the number of machines in the database cluster. Small and large
# correspond to 1 or 2 machines, respectively, which you see later,
# down in the resources section.
# -----
dbenvsize:
  type: string
  title: Database cluster size
  enum:
    - Small
    - Large
#
# -----
# Dynamically tag the machines that will be created. The
# 'array' of objects means you can create as many key-value pairs as
# needed. To see how array input looks when it's collected,
# open the cloud template and click TEST.
# -----
Mtags:
  type: array
  title: Tags
  description: Tags to apply to machines
  items:
    type: object
    properties:
      key:
        type: string
        title: Key
      value:
        type: string
        title: Value
#
# -----
# Create machine credentials. These credentials are needed in
# remote access configuration later, in the resources section.
# -----
username:
  type: string
  minLength: 4

```

```

    maxLength: 20
    pattern: '[a-z]+'
    title: Database Username
    description: Database Username
  userpassword:
    type: string
    pattern: '[a-z0-9A-Z@#\$]+'
    encrypted: true
    title: Database Password
    description: Database Password
#
# -----
# Set the database storage disk size.
# -----
databaseDiskSize:
  type: number
  default: 4
  maximum: 10
  title: MySQL Data Disk Size
  description: Size of database disk
#
# -----
# Set the number of machines in the web cluster. Small, medium, and large
# correspond to 2, 3, and 4 machines, respectively, which you see later,
# in the WebTier part of the resources section.
# -----
clusterSize:
  type: string
  enum:
    - small
    - medium
    - large
  title: Wordpress Cluster Size
  description: Wordpress Cluster Size
#
# -----
# Set the archive storage disk size.
# -----
archiveDiskSize:
  type: number
  default: 4
  maximum: 10
  title: Wordpress Archive Disk Size
  description: Size of Wordpress archive disk
#
# -----
# The resources section configures the deployment of machines, disks,
# networks, and other objects. In several places, the code pulls from
# the preceding interactive user inputs.
# -----
resources:
#
# -----
# Create the database server. Choose a cloud agnostic machine 'type' so
# that it can deploy to AWS, Azure, or vSphere. Then enter its property

```

```

# settings.
# -----
DBTier:
  type: Cloud.Machine
  properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: mysql
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead.
# image: '${input.osimage}'
# -----
    image: Ubuntu
#
# -----
# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
    flavor: small
#
# -----
# Tag the database machine to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with a site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
    constraints:
      - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Also tag the database machine with any free-form tags that were created
# during user input.
# -----
    tags: '${input.Mtags}'
#
# -----
# Set the database cluster size by referencing the dbenvsize user
# input. Small is one machine, and large defaults to two.
# -----
    count: '${input.dbenvsize == "Small" ? 1 : 2}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
    networks:
      - network: '${resource.WP_Network.id}'
#

```



```

# -----
# Enable remote access to the database server. Reference the credentials
# from the user input.
# -----
    remoteAccess:
      authentication: usernamePassword
      username: '${input.username}'
      password: '${input.userpassword}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
    ABC-Company-ID: 9393
#
# -----
# Run OS commands or scripts to further configure the database machine,
# via operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
    cloudConfig: |
      #cloud-config
      repo_update: true
      repo_upgrade: all
      packages:
        - mysql-server
      runcmd:
        - sed -e '/bind-address/ s/^#*\/#/' -i /etc/mysql/mysql.conf.d/mysqld.cnf
        - service mysql restart
        - mysql -e "GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'mysqlpassword';"
        - mysql -e "FLUSH PRIVILEGES;"
    attachedDisks: []
#
# -----
# Create the web server. Choose a cloud agnostic machine 'type' so that it
# can deploy to AWS, Azure, or vSphere. Then enter its property settings.
# -----
    WebTier:
      type: Cloud.Machine
      properties:
#
# -----
# Descriptive name for the virtual machine. Does not become the hostname
# upon deployment.
# -----
    name: wordpress
#
# -----
# Hard-coded operating system image to use. To pull from user input above,
# enter the following instead:
# image: '${input.osimage}'
# -----
    image: Ubuntu
#
# -----

```

```

# Hard-coded capacity to use. Note that the Cloud Assembly
# Infrastructure must also have AWS, Azure, and vSphere flavors
# such as small, medium, and large mapped.
# -----
#     flavor: small
#
# -----
# Set the web server cluster size by referencing the clusterSize user
# input. Small is 2 machines, medium is 3, and large defaults to 4.
# -----
#     count: '${input.clusterSize== "small" ? 2 : (input.clusterSize == "medium" ? 3 : 4)}'
#
# -----
# Set an environment variable to display object information under the
# Properties tab, post-deployment. Another example might be
# {env.blueprintID}
# -----
#     tags:
#       - key: cas.requestedBy
#         value: '${env.requestedBy}'
#
# -----
# You are free to add custom properties, which might be used to initiate
# an extensibility subscription, for example.
# -----
#     ABC-Company-ID: 9393
#
# -----
# Tag the web server to deploy to the cloud vendor chosen from the
# user input. Tags are case-sensitive, so 'to_lower' forces the tag to
# lowercase to ensure a match with your site's tagging convention. It's
# important if platform input were to contain any upper case characters.
# -----
#     constraints:
#       - tag: '${"env:" + to_lower(input.platform)}'
#
# -----
# Add a variable to connect the machine to a network resource based on
# a property binding to another resource. In this case, it's the
# 'WP_Network' network that gets defined further below.
# -----
#     networks:
#       - network: '${resource.WP_Network.id}'
#
# -----
# Run OS commands or scripts to further configure the web server,
# with operations such as setting a hostname, generating SSH private keys,
# or installing packages.
# -----
#     cloudConfig: |
#       #cloud-config
#       repo_update: true
#       repo_upgrade: all
#       packages:
#         - apache2

```

```

- php
- php-mysql
- libapache2-mod-php
- php-mcrypt
- mysql-client
runcmd:
  - mkdir -p /var/www/html/mywordpresssite && cd /var/www/html && wget
https://wordpress.org/latest.tar.gz && tar -xzf /var/www/html/latest.tar.gz -C /var/www/html/
mywordpresssite --strip-components 1
  - i=0; while [ $i -le 5 ]; do mysql --connect-timeout=3 -h $
{DBTier.networks[0].address} -u root -pmysqlpassword -e "SHOW STATUS;" && break || sleep 15;
i=$((i+1)); done
  - mysql -u root -pmysqlpassword -h ${resource.DBTier.networks[0].address} -e
"create database wordpress_blog;"
  - mv /var/www/html/mywordpresssite/wp-config-sample.php /var/www/html/
mywordpresssite/wp-config.php
  - sed -i -e s/"define('DB_NAME', 'database_name_here');"/"define('DB_NAME',
'wordpress_blog');"/ /var/www/html/mywordpresssite/wp-config.php && sed -i
-e s/"define('DB_USER', 'username_here');"/"define('DB_USER', 'root');"/ /var/www/html/
mywordpresssite/wp-config.php && sed -i -e s/"define('DB_PASSWORD',
'password_here');"/"define('DB_PASSWORD', 'mysqlpassword');"/ /var/www/html/mywordpresssite/
wp-config.php && sed -i -e s/"define('DB_HOST', 'localhost');"/"define('DB_HOST', '$
{resource.DBTier.networks[0].address}');"/ /var/www/html/mywordpresssite/wp-config.php
  - service apache2 reload
#
# -----
# Create the network that the database and web servers connect to.
# Choose a cloud agnostic network 'type' so that it can deploy to AWS,
# Azure, or vSphere. Then enter its property settings.
# -----
WP_Network:
  type: Cloud.Network
  properties:
#
# -----
# Descriptive name for the network. Does not become the network name
# upon deployment.
# -----
    name: WP_Network
#
# -----
# Set the networkType to an existing network. You could also use a
# constraint tag to target a specific, like-tagged network.
# The other network types are private or public.
# -----
    networkType: existing
#
# *****
#
# VMware hopes that you found this commented template useful. Note that
# you can also access an API to create templates, or query for input
# schema that you intend to request. See the following Swagger
# documentation.

```

```
#
# www.mgmt.cloud.vmware.com/blueprint/api/swagger/swagger-ui.html
#
# *****
```

Esempi di risorse di vSphere in Cloud Assembly

Questi esempi di codice illustrano risorse macchine di vSphere all'interno di modelli cloud di Cloud Assembly.

Risorsa	Modello cloud di esempio
Macchina virtuale di vSphere con CPU, memoria e sistema operativo	<pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 1 totalMemoryMB: 1024 image: ubuntu</pre>
Macchina di vSphere con una risorsa datastore	<pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: 'HDD' capacityGb: 10 dataStore: 'datastore-01' provisioningType: thick</pre>
Macchina di vSphere con un disco collegato	<pre>resources: demo-vsphere-disk-001: type: Cloud.vSphere.Disk properties: name: DISK_001 type: HDD capacityGb: 10 dataStore: 'datastore-01' provisioningType: thin demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 2048 imageRef: >- https://packages.vmware.com/photon/4.0/ Rev1/ova/photon-ova-4.0-ca7c9e9330.ova attachedDisks: - source: '\${demo-vsphere-disk-001.id}'</pre>

Risorsa	Modello cloud di esempio
<p>Macchina di vSphere con un numero di dischi dinamico</p>	<pre>inputs: disks: type: array title: disks items: title: disks type: integer maxItems: 15 resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: image: Centos flavor: small attachedDisks: '\$ {map_to_object(resource.Cloud_Volume_1[*].id, "source")}' Cloud_Volume_1: type: Cloud.Volume allocatePerInstance: true properties: capacityGb: '\${input.disks[count.index]}' count: '\${length(input.disks)}'</pre>
<p>Macchina di vSphere da un'immagine snapshot. Aggiungere in coda una barra e il nome dello snapshot. L'immagine dello snapshot può essere un clone collegato.</p>	<pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: imageRef: 'demo-machine/snapshot-01' cpuCount: 1 totalMemoryMB: 1024</pre>
<p>Macchina di vSphere in una cartella specifica in vCenter</p>	<pre>resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine cpuCount: 2 totalMemoryMB: 1024 imageRef: ubuntu resourceGroupName: 'myFolder'</pre>

Risorsa	Modello cloud di esempio
Macchina vSphere con più NIC	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: '\${network-01.name}' deviceIndex: 0 - network: '\${network-02.name}' deviceIndex: 1 network-01: type: Cloud.vSphere.Network properties: name: network-01 network-02: type: Cloud.vSphere.Network properties: name: network-02 </pre>
Macchina di vSphere con tag collegato in vCenter	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu tags: - key: env value: demo </pre>

Risorsa	Modello cloud di esempio
Macchina di vSphere con una specifica di personalizzazione	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: name: demo-machine image: ubuntu flavor: small customizationSpec: Linux </pre>
Macchina di vSphere con accesso remoto	<pre> inputs: username: type: string title: Username description: Username default: testUser password: type: string title: Password default: VMware@123 encrypted: true description: Password for the given username resources: demo-machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/ 16.04/release-20170307/ubuntu-16.04-server-cloudimg- amd64.ova cloudConfig: ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' runcmd: - echo "Defaults:\${input.username} ! requiretty" >> /etc/sudoers.d/\${input.username} </pre>

Core per socket e conteggio CPU in Cloud Assembly

Il codice del modello di Cloud Assembly consente di specificare un numero di core per socket per una risorsa macchina di vSphere.

È possibile specificare il numero di core per socket virtuale o il numero totale di socket. Ad esempio, è possibile che i termini di licenza limitino il software autorizzato per ciascun socket oppure che i sistemi operativi disponibili riconoscano solo un determinato numero di socket e che quindi sia necessario eseguire il provisioning di altre CPU come core aggiuntivi.

Aggiungere la proprietà `coreCount` a un modello cloud nella risorsa macchina vSphere.

Il valore di `coreCount` deve essere minore o uguale al valore del conteggio CPU (`cpuCount`) specificato nella mappatura delle caratteristiche o nel codice della risorsa macchina vSphere nel modello cloud. Per informazioni correlate, vedere [l'articolo relativo all'impostazione del numero di core per CPU in una macchina virtuale \(1010184\)](#).

La proprietà `coreCount` è facoltativa e disponibile solo per le risorse macchina vSphere.

Di seguito è disponibile un esempio di frammento di codice della risorsa macchina vSphere.

```
Cloud_vSphere_Machine_1:
  type: Cloud.vSphere.Machine
  properties:
    cpuCount: 8
    coreCount: 4
```

Ulteriori informazioni sulle impostazioni di socket e core per socket sono disponibili nell'articolo del blog [Virtual Machine vCPU and vNUMA Rightsizing – Guidelines](#).

Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation

È possibile utilizzare le risorse e le impostazioni di rete, sicurezza e bilanciamento del carico nei progetti di modelli cloud e nelle distribuzioni.

Per un riepilogo delle opzioni del codice di progettazione del modello cloud, vedere [Schema dei tipi di risorse di vRealize Automation](#).

Per informazioni correlate, vedere:

- [Ulteriori informazioni sulle risorse di rete nei modelli cloud di vRealize Automation](#)
- [Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation](#)
- [Ulteriori informazioni sulle risorse di bilanciamento del carico nei modelli cloud di vRealize Automation](#)

Questi esempi illustrano risorse di rete, sicurezza e bilanciamento del carico in progettazioni di modelli cloud di base.

Reti

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>Macchina vSphere con più NIC connesse a reti vSphere e NSX con assegnazione IP DHCP</p>	<pre> resources: demo-machine: type: Cloud.vSphere.Machine properties: image: ubuntu flavor: small networks: - network: \${resource["demo-vSphere- Network"].id} deviceIndex: 0 - network: \${resource["demo-NSX- Network"].id} deviceIndex: 1 demo-vSphere-Network: type: Cloud.vSphere.Network properties: networkType: existing demo-NSX-Network: type: Cloud.NSX.Network properties: networkType: outbound </pre>
<p>Aggiunta di una rete privata con un indirizzo IP statico per una distribuzione di macchine virtuali Azure</p>	<pre> formatVersion: 1 inputs: {} resources: Cloud_Azure_Machine_1: type: Cloud.Azure.Machine properties: image: photon flavor: Standard_B1ls networks: - network: '\${ {resource.Cloud_Network_1.id}' assignment: static address: 10.0.0.45 assignPublicIpAddress: false Cloud_Network_1: type: Cloud.Network properties: networkType: existing </pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>È possibile utilizzare l'assegnazione di un IP statico con l'IPAM di vRealize (interno fornito da vRealize Automation o esterno basato sull'SDK dell'IPAM di vRA come per uno dei plug-in Infoblox disponibili in VMware Marketplace). Non sono supportati altri utilizzi di <code>assignment: static</code>, come descritto nella sezione relativa alle <i>avvertenze</i> di Ulteriori informazioni sulle risorse di rete nei modelli cloud di vRealize Automation.</p>	<pre>resources: demo_vm: type: Cloud.vSphere.Machine properties: image: 'photon' cpuCount: 1 totalMemoryMB: 1024 networks: - network: \${resource.demo_nw.id} assignment: static demo_nw: type: Cloud.vSphere.Network properties: networkType: existing</pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>Aggiungere o modificare le regole di inoltro delle porte NAT e DNAT in una risorsa Cloud.NSX.NAT per una distribuzione esistente.</p>	<pre> resources: gw: type: Cloud.NSX.Gateway properties: networks: - \${resource.akout.id} nat: type: Cloud.NSX.Nat properties: networks: - \${resource.akout.id} natRules: - translatedInstance: \$ {resource.centos.networks[0].id} index: 0 protocol: TCP kind: NAT44 type: DNAT sourceIPs: any sourcePorts: 80 translatedPorts: 8080 destinationPorts: 8080 description: edit - translatedInstance: \$ {resource.centos.networks[0].id} index: 1 protocol: TCP kind: NAT44 type: DNAT sourceIPs: any sourcePorts: 90 translatedPorts: 9090 destinationPorts: 9090 description: add gateway: \${resource.gw.id} centos: type: Cloud.vSphere.Machine properties: image: WebTinyCentOS65x86 flavor: small customizationSpec: Linux networks: - network: \${resource.akout.id} assignment: static akout: type: Cloud.NSX.Network properties: networkType: outbound constraints: - tag: nsxt-nat-1-M2 </pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>Una macchina cloud pubblica per l'utilizzo di un IP interno anziché un IP pubblico. Questo esempio utilizza un ID di rete specifico.</p> <p>Nota: l'opzione <code>network</code>: viene utilizzata nell'impostazione <code>networks</code>: per specificare un ID di rete di destinazione. L'opzione <code>name</code>: nell'impostazione <code>networks</code>: è stata deprecata e non deve essere utilizzata.</p>	<pre>resources: wf_proxy: type: Cloud.Machine properties: image: ubuntu 16.04 flavor: small constraints: - tag: 'platform:vsphere' networks: - network: '\${resource.wf_net.id}' assignPublicIpAddress: false</pre>
<p>Rete instradata per NSX-V o NSX-T utilizzando il tipo di risorsa di rete NSX.</p>	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: routed</pre>
<p>Aggiungere un tag a una risorsa NIC della macchina nel modello cloud.</p>	<pre>formatVersion: 1 inputs: {} resources: Cloud_Machine_1: type: Cloud.vSphere.Machine properties: flavor: small image: ubuntu networks: - name: '\${resource.Cloud_Network_1.name}' deviceIndex: 0 tags: - key: 'nic0' value: null - key: internal value: true - name: '\${resource.Cloud_Network_2.name}' deviceIndex: 1 tags: - key: 'nic1' value: null - key: internal value: false</pre>
<p>Contrassegnare con tag i commutatori logici NSX-T per una rete in uscita.</p> <p>I tag sono supportati per NSX-T e VMware Cloud on AWS.</p> <p>Per ulteriori informazioni su questo scenario, vedere il post del blog della community Creating Tags in NSX with Cloud Assembly.</p>	<pre>Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: outbound tags: - key: app value: opencart</pre>

Gruppi di sicurezza

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>Gruppo di sicurezza esistente con un tag di vincolo applicato a una scheda NIC di una macchina.</p> <p>Per utilizzare un gruppo di sicurezza esistente, immettere <i>existing</i> per la proprietà <code>securityGroupType</code>.</p> <p>È possibile assegnare tag a una risorsa <code>Cloud.SecurityGroup</code> per allocare i gruppi di sicurezza esistenti utilizzando vincoli di tag. I gruppi di sicurezza che non contengono tag non possono essere utilizzati nella progettazione del modello cloud.</p> <p>I tag di vincolo devono essere impostati per le risorse del gruppo di sicurezza <code>securityGroupType: existing</code>. Questi vincoli devono corrispondere ai tag impostati nei gruppi di sicurezza esistenti. Non è possibile impostare tag di vincolo per le risorse del gruppo di sicurezza <code>securityGroupType: new</code>.</p>	<pre>formatVersion: 1 inputs: {} resources: allowSsh_sg: type: Cloud.SecurityGroup properties: securityGroupType: existing constraints: - tag: allowSsh compute: type: Cloud.Machine properties: image: centos flavor: small networks: - network: '\${resource.prod-net.id}' securityGroups: - '\${resource.allowSsh_sg.id}' prod-net: type: Cloud.Network properties: networkType: existing</pre>
<p>Gruppo di sicurezza su richiesta con due regole del firewall che illustrano le opzioni di accesso Allow e Deny.</p>	<pre>resources: Cloud_SecurityGroup_1: type: Cloud.SecurityGroup properties: securityGroupType: new rules: - ports: 5000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Allow direction: inbound name: allow_5000 protocol: TCP - ports: 7000 source: 'fc00:10:000:000:000:56ff:fe89:48b4' access: Deny direction: inbound name: deny_7000 protocol: TCP Cloud_vSphere_Machine_1: type: Cloud.vSphere.Machine properties:</pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
	<pre> image: photon cpuCount: 1 totalMemoryMB: 256 networks: - network: '\$ {resource.Cloud_Network_1.id}' assignIPv6Address: true assignment: static securityGroups: - '\$ {resource.Cloud_SecurityGroup_1.id}' Cloud_Network_1: type: Cloud.Network properties: networkType: existing </pre>
<p>Modello cloud complesso con 2 gruppi di sicurezza, tra cui:</p> <ul style="list-style-type: none"> ■ 1 gruppo di sicurezza esistente ■ 1 gruppo di sicurezza su richiesta con più esempi di regole del firewall ■ 1 macchina vSphere ■ 1 rete esistente <p>Questo esempio illustra diverse combinazioni di protocolli e porte, servizi, CIDR IP come source e destination, intervallo IP come source o destination e opzioni per any, IPv6 e (::/0).</p> <p>Per le schede NIC delle macchine, è possibile specificare la rete connessa e i gruppi di sicurezza. È possibile specificare anche l'indice della NIC o un indirizzo IP.</p>	<pre> formatVersion: 1 inputs: {} resources: DEMO_ESG : <i>existing security group - security group 1</i>) type: Cloud.SecurityGroup properties: constraints: - tag: BlockAll securityGroupType: existing (<i>designation of existing for security group 1</i>) DEMO_ODSG: (<i>on-demand security group - security group 2</i>) type: Cloud.SecurityGroup properties: rules: (<i>multiple firewall rules in this section</i>) - name: IN-ANY (<i>rule 1</i>) source: any service: any direction: inbound access: Deny - name: IN-SSH (<i>rule 2</i>) source: any service: SSH direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 3</i>) source: 33.33.33.1-33.33.33.250 protocol: TCP ports: 223 direction: inbound access: Allow - name: IPv-6-ANY-SOURCE (<i>rule 4</i>) source: ':::/0' protocol: TCP ports: 223 direction: inbound access: Allow - name: IN-SSH-IP (<i>rule 5</i>) source: 44.44.44.1/24 protocol: UDP ports: 22-25 direction: inbound access: Allow - name: IN-EXISTING-SG (<i>rule 6</i>) </pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
	<pre> source: '\${resource["DEMO_ESG"].id}' protocol: ICMPv6 direction: inbound access: Allow - name: OUT-ANY (rule 7) destination: any service: any direction: outbound access: Deny - name: OUT-TCP-IPv6 (rule 8) destination: '2001:0db8:85a3::8a2e:0370:7334/64' protocol: TCP ports: 22 direction: outbound access: Allow - name: IPv6-ANY-DESTINATION (rule 9) destination: ':::/0' protocol: UDP ports: 23 direction: outbound access: Allow - name: OUT-UDP-SERVICE (rule 10) destination: any service: NTP direction: outbound access: Allow securityGroupType: new (designation of on- demand for security group 2) DEMO_VC_MACHINE: (machine resource) type: Cloud.vSphere.Machine properties: image: PHOTON cpuCount: 1 totalMemoryMB: 1024 networks: (Machine network NICs) - network: '\${resource.DEMO_NW.id}' securityGroups: - '\${resource.DEMO_ODSG.id}' - '\${resource.DEMO_ESG.id}' DEMO_NETWORK: (network resource) type: Cloud.vSphere.Network properties: networkType: existing constraints: - tag: nsx62 </pre>

Bilanciamenti del carico

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>Specificare un livello di registrazione, un algoritmo e una dimensione del bilanciamento del carico.</p>	<p>Esempio di bilanciamento del carico NSX che mostra l'utilizzo del livello di registrazione, dell'algoritmo e della dimensione:</p> <pre data-bbox="619 373 1225 688">resources: Cloud_LoadBalancer_1: type: Cloud.NSX.LoadBalancer properties: name: myapp-lb network: '\${appnet-public.name}' instances: '\${wordpress.id}' routes: - protocol: HTTP port: '80' loggingLevel: CRITICAL algorithm: LEAST_CONNECTION type: MEDIUM</pre>
<p>Associare un bilanciamento del carico a una macchina denominata o a una scheda NIC di una macchina denominata. È possibile specificare <code>machine ID</code> o <code>machine network ID</code> per aggiungere la macchina al pool di bilanciamento del carico. La proprietà <code>instances</code> supporta entrambe le macchine (<code>machine by ID</code>) e le NIC (<code>machine by network ID</code>).</p> <p>Nel primo esempio, la distribuzione utilizza l'impostazione <code>machine by ID</code> per bilanciare il carico della macchina quando viene distribuita in una rete.</p> <p>Nel secondo esempio, la distribuzione utilizza l'impostazione <code>machine by network ID</code> per bilanciare il carico della macchina solo quando la macchina viene distribuita nella NIC della macchina denominata.</p> <p>Il terzo esempio mostra entrambe le impostazioni utilizzate nella stessa opzione <code>instances</code>.</p>	<p>È possibile utilizzare la proprietà <code>instances</code> per definire un ID macchina o un ID di rete della macchina:</p> <ul style="list-style-type: none"> ■ ID macchina <pre data-bbox="655 863 1362 1024">Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.id}'</pre> ■ ID rete macchina <pre data-bbox="655 1136 1362 1297">Cloud_LoadBalancer_1: type: Cloud.LoadBalancer properties: network: '\${resource.Cloud_Network_1.id}' instances: '\$ {resource.Cloud_Machine_1.networks[0].id}'</pre> ■ Una macchina specificata per l'inclusione del bilanciamento del carico e un'altra NIC della macchina specificata per l'inclusione del bilanciamento del carico: <pre data-bbox="655 1444 1350 1522">instances: - resource.Cloud_Machine_1.id - resource.Cloud_Machine_2.networks[2].id</pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>Aggiungere le impostazioni di controllo dello stato a un bilanciamento del carico NSX. Le opzioni aggiuntive includono <code>httpMethod</code>, <code>requestBody</code> e <code>responseBody</code>.</p>	<pre> myapp-lb: type: Cloud.NSX.LoadBalancer properties: name: myapp-lb network: '\${appnet-public.name}' instances: '\${wordpress.id}' routes: - protocol: HTTP port: '80' algorithm: ROUND_ROBIN instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /mywordpresssite/wp-admin/ install.php intervalSeconds: 60 timeoutSeconds: 10 unhealthyThreshold: 10 healthyThreshold: 2 connectionLimit: '50' connectionRateLimit: '50' maxConnections: '500' minConnections: '' internetFacing: true{code} </pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
<p>Rete su richiesta con un bilanciamento del carico a un solo braccio.</p>	<pre> inputs: {} resources: mp-existing: type: Cloud.Network properties: name: mp-existing networkType: existing mp-wordpress: type: Cloud.vSphere.Machine properties: name: wordpress count: 2 flavor: small image: tiny customizationSpec: Linux networks: - network: '\${resource["mp-private"].id}' mp-private: type: Cloud.NSX.Network properties: name: mp-private networkType: private constraints: - tag: nsxt mp-wordpress-lb: type: Cloud.LoadBalancer properties: name: wordpress-lb internetFacing: false network: '\${resource.mp-existing.id}' instances: '\${resource["mp-wordpress"].id}' routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.pl intervalSeconds: 60 timeoutSeconds: 30 unhealthyThreshold: 5 healthyThreshold: 2 </pre>
<p>Rete esistente con un bilanciamento del carico.</p>	<pre> formatVersion: 1 inputs: count: type: integer default: 1 resources: ubuntu-vm: type: Cloud.Machine properties: name: ubuntu flavor: small image: tiny count: '\${input.count}' networks: </pre>

Scenario risorsa	Esempio di codice di progettazione del modello di cloud
	<pre> - network: '\$ {resource.Cloud_NSX_Network_1.id}' Provider_LoadBalancer_1: type: Cloud.LoadBalancer properties: name: OC-LB routes: - protocol: HTTP port: '80' instanceProtocol: HTTP instancePort: '80' healthCheckConfiguration: protocol: HTTP port: '80' urlPath: /index.html intervalSeconds: 60 timeoutSeconds: 5 unhealthyThreshold: 5 healthyThreshold: 2 network: '\$ {resource.Cloud_NSX_Network_1.id}' internetFacing: false instances: '\${resource["ubuntu-vm"].id}' Cloud_NSX_Network_1: type: Cloud.NSX.Network properties: networkType: existing constraints: - tag: nsxt24prod </pre>

Ulteriori informazioni

Per gli scenari di implementazione della rete e del gruppo di sicurezza, vedere i blog di VMware, ad esempio:

- [vRealize Automation Cloud Assembly Load Balancer with NSX-T Deep Dive](#)
- [Network Automation with Cloud Assembly and NSX – Part 1](#) (include l'uso degli account cloud di NSX-T e vCenter e del CIDR della rete)
- [Network Automation with Cloud Assembly and NSX – Part 2](#) (include l'utilizzo dei tipi di rete esistenti e in uscita)
- [Network Automation with Cloud Assembly and NSX – Part 3](#) (include l'uso di gruppi di sicurezza esistenti e su richiesta)
- [Network Automation with Cloud Assembly and NSX – Part 4](#) (include l'utilizzo di bilanciamenti del carico esistenti e su richiesta)

Ulteriori informazioni sulle risorse di rete nei modelli cloud di vRealize Automation

Quando si creano o si modificano i modelli cloud di vRealize Automation, utilizzare le risorse di rete più appropriate per i propri obiettivi. Di seguito sono disponibili ulteriori informazioni sulle opzioni di rete NSX e indipendenti dal cloud disponibili nel modello cloud.

Selezionare uno dei tipi di risorse di rete disponibili in base alla macchina e alle condizioni correlate nel modello cloud di vRealize Automation.

Risorsa di rete indipendente dal cloud

È possibile aggiungere una rete indipendente dal cloud utilizzando la risorsa **Indipendente dal cloud > Rete** nella pagina **Progettazione** del modello cloud. La risorsa viene visualizzata nel codice del modello cloud come tipo di risorsa `Cloud.Network`. La risorsa predefinita viene visualizzata come:

```
Cloud_Network_1:
  type: Cloud.Network
  properties:
    networkType: existing
```

Utilizzare una rete indipendente dal cloud quando si desidera specificare le caratteristiche di rete per un tipo di macchina di destinazione che non è, o potrebbe non essere, connessa a una rete NSX.

La risorsa di rete indipendente dal cloud è disponibile per questi tipi di risorse:

- Macchina indipendente dal cloud
- vSphere
- Google Cloud Platform (GCP)
- Amazon Web Services (AWS)
- Microsoft Azure
- VMware Cloud on AWS (VMC)

La risorsa di rete indipendente dal cloud è disponibile per queste impostazioni del tipo di rete (`networkType`):

- public
- private
- outbound
- existing

Risorsa di rete di vSphere

È possibile aggiungere una rete di vSphere utilizzando la risorsa **vSphere > Rete** nella pagina **Progettazione** del modello cloud. La risorsa viene visualizzata nel codice del modello cloud come tipo di risorsa `Cloud.vSphere.Network`. La risorsa predefinita viene visualizzata come:

```
Cloud_vSphere_Network_1:
  type: Cloud.vSphere.Network
  properties:
    networkType: existing
```

Utilizzare una rete di vSphere quando si desidera specificare le caratteristiche di rete per un tipo di macchina vSphere (`Cloud.vSphere.Machine`).

La risorsa di rete di vSphere è disponibile solo per un tipo di macchina `Cloud.vSphere.Machine`.

La risorsa di vSphere è disponibile per queste impostazioni del tipo di rete (`networkType`):

- public
- private
- existing

Per alcuni esempi, vedere [Utilizzo delle impostazioni di rete in profili di rete e progettazioni di modelli cloud in vRealize Automation](#).

Risorsa di rete di NSX

È possibile aggiungere una rete NSX utilizzando la risorsa **NSX > Rete** nella pagina **Progettazione** del modello cloud. La risorsa viene visualizzata nel codice del modello cloud come tipo di risorsa `Cloud.NSX.Network`. La risorsa predefinita viene visualizzata come:

```
Cloud_NSX_Network_1:
  type: Cloud.NSX.Network
  properties:
    networkType: existing
```

Utilizzare una rete NSX quando si desidera collegare una risorsa di rete a una o più macchine associate a un account cloud di NSX-V o NSX-T. La risorsa di rete di NSX consente di specificare le caratteristiche di rete di NSX per una risorsa macchina vSphere associata a un account cloud NSX-V o NSX-T.

La risorsa di `Cloud.NSX.Network` è disponibile per queste impostazioni del tipo di rete (`networkType`):

- public
- private
- outbound
- existing
- instradata - Le reti instradate sono disponibili solo per NSX-V e NSX-T.

Se si desidera che più reti in uscita o instradate condividano lo stesso router NSX-T di livello 1 o Edge Service Gateway (ESG) NSX-V, connettere una singola risorsa gateway NSX (`Cloud.NSX.Gateway`) alle reti connesse nel modello prima della distribuzione iniziale. Se il gateway viene aggiunto dopo la distribuzione come operazione di sviluppo giorno 2 o iterativa, ogni rete crea il proprio router.

È possibile utilizzare la risorsa NAT NSX nel modello per supportare le regole di inoltro delle porte NAT e DNAT.

Risorsa di rete indipendente dal cloud con finalità di distribuzione di Azure, AWS o GCP

Le macchine virtuali del provider di cloud pubblico possono richiedere combinazioni di proprietà specifiche del modello cloud che non sono necessariamente obbligatorie nelle distribuzioni di NSX o di macchine basate su vSphere. Per esempi di codice di modello cloud che supportano alcuni di questi scenari, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Risorsa gateway NSX

È possibile riutilizzare o condividere un singolo router NSX-T di livello 1 o un Edge Service Gateway (ESG) NSX-V in una singola distribuzione utilizzando una risorsa gateway (`Cloud.NSX.Gateway`) nel modello cloud. La risorsa gateway rappresenta il livello 1 o ESG e può essere connessa a più reti nella distribuzione. La risorsa gateway può essere utilizzata solo con reti in uscita o instradate.

La risorsa `Cloud.NSX.Gateway` consente di condividere il router NSX-T di livello 1 o Edge Service Gateway (ESG) NSX-V tra reti in uscita o instradate connesse in una distribuzione.

Il gateway viene spesso collegato a una singola rete in uscita o instradata. Tuttavia, se il gateway viene collegato a più reti, le reti devono essere dello stesso tipo, ad esempio tutte in uscita o tutte instradate. Il gateway può essere connesso a più macchine o bilanciamenti del carico connessi alle stesse reti in uscita o instradate. Il gateway deve essere connesso a un bilanciamento del carico nella rete su richiesta condivisa in modo che possa riutilizzare il router NSX-T di livello 1 o Edge Service Gateway (ESG) NSX-V creato dal gateway.

Per consentire a più reti in uscita o instradate di condividere lo stesso router di livello 1 o edge, connettere inizialmente una singola risorsa gateway `Cloud.NSX.Gateway` a tutte le reti. Tutte le reti previste e il singolo gateway devono essere connessi tra loro prima di distribuire il modello cloud. In caso contrario, ogni rete crea il proprio router.

Per una rete NSX che contiene una risorsa gateway di elaborazione associata, le impostazioni del gateway vengono applicate a tutte le reti associate nella distribuzione. Viene creato un singolo router logico NSX-T di livello 1 per ogni distribuzione, che viene quindi condiviso da tutte le reti su richiesta e i bilanciamenti del carico nella distribuzione. Viene creato un singolo edge NSX-V per ogni distribuzione, che viene quindi condiviso da tutte le reti su richiesta e i bilanciamenti del carico nella distribuzione.

È possibile collegare la risorsa gateway a una rete come aggiornamento della distribuzione iterativa. Tuttavia, non viene creato un router di livello 1 o edge. La distribuzione di rete iniziale crea il router.

Per le reti NSX-T che non utilizzano una risorsa gateway associata, più reti su richiesta nel modello cloud continuano a creare più router logici di livello 1 nella distribuzione.

Se il gateway contiene regole NAT, è possibile riconfigurare o eliminare le regole NAT o DNAT per il router di livello 1 o il router edge. Se il gateway viene inizialmente distribuito senza regole NAT, non dispone di azioni giorno 2.

Risorsa NAT NSX

La risorsa `Cloud.NSX.NAT` consente di collegare le regole DNAT e l'inoltro della porta a tutte le reti in uscita connesse tramite la risorsa gateway. È possibile collegare una risorsa NAT a una risorsa gateway per cui è necessario configurare le regole DNAT.

Nota La risorsa `Cloud.NSX.Gateway` era originariamente disponibile per le regole DNAT. Tuttavia, l'utilizzo di `Cloud.NSX.Gateway` per definire le regole DNAT e l'inoltro della porta è diventato obsoleto. Rimane disponibile per la compatibilità con le versioni precedenti. Utilizzare la risorsa del modello cloud `Cloud.NSX.NAT` per le regole DNAT e l'inoltro della porta. Nel modello cloud viene visualizzato un avviso se si tenta di utilizzare il tipo di risorsa `Cloud.NSX.Gateway` con le specifiche della regola NAT.

La risorsa `Cloud.NSX.NAT` supporta le regole DNAT e l'inoltro della porta quando è connessa a una rete NSX-V o NSX-T in uscita.

L'impostazione delle regole NAT nella risorsa è `natRules`. È possibile collegare la risorsa NAT alla risorsa gateway per configurare le voci `natRules` nel gateway. Le regole DNAT specificate nella risorsa utilizzano le macchine o i bilanciamenti del carico associati come destinazione.

È possibile riconfigurare la NIC di una macchina o un gateway di elaborazione in una distribuzione esistente per modificare le impostazioni di `natRules`: aggiungendo, riordinando, modificando o eliminando le regole di inoltro della porta DNAT. Non è possibile utilizzare regole DNAT con macchine in cluster. È possibile specificare regole DNAT per singole macchine nel cluster come parte di un'operazione giorno 2.

Opzioni di integrazione IPAM esterna

Per informazioni sulle proprietà disponibili per l'utilizzo con le integrazioni IPAM di Infoblox in progettazioni e distribuzioni di modelli cloud, vedere [Utilizzo delle proprietà specifiche di Infoblox e attributi estendibili per le integrazioni IPAM nei modelli cloud di vRealize Automation](#).

Avvertenze per l'utilizzo dell'assegnazione di un IP statico in un modello cloud

È possibile utilizzare l'assegnazione di un IP statico in un modello cloud di vRealize Automation solo quando si utilizza l'IPAM di vRealize Automation, ovvero l'IPAM interno fornito da vRealize Automation o l'IPAM derivato da un plug-in del provider esterno creato tramite l'SDK dell'IPAM di vRealize Automation, ad esempio uno dei plug-in Infoblox disponibili per il download da vRealize Automation Marketplace. L'utilizzo dell'assegnazione di un IP statico (`assignment:static`) non è supportato in un modello cloud quando si utilizza un argomento dell'evento Configurazione rete (che viene usato da un'azione di estendibilità di Cloud Assembly (ABX) o da un workflow di vRealize Orchestrator). Le assegnazioni di IP statici non supportate causano un errore di distribuzione.

Valore Indirizzo nella sezione Generale del modello cloud distribuito

Quando si esamina un modello cloud distribuito, il valore **Indirizzo** nella sezione **Generale** del modello è l'indirizzo IP primario della macchina. L'indirizzo primario è spesso l'indirizzo della macchina pubblico o accessibile in altro modo. Per le distribuzioni di vSphere, l'indirizzo IP primario viene calcolato da vRealize Automation. Per determinare l'indirizzo IP primario, vengono considerati e classificati tutti gli indirizzi IP per tutte le schede NIC, incluse le proprietà pubbliche, private, IPv6, statiche e dinamiche. Per le distribuzioni non di vSphere, l'indirizzo IP primario della macchina viene calcolato dal sistema di classificazione di ciascun fornitore del cloud.

Operazioni giorno 2 disponibili

Per un elenco delle operazioni giorno 2 comuni disponibili per le risorse di modello cloud e distribuzione, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Per un esempio che illustra come passare da una rete all'altra, vedere [Spostamento di una macchina distribuita in un'altra rete](#).

Ulteriori informazioni

Per informazioni ed esempi correlati che illustrano le impostazioni e le risorse di rete di esempio, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Per informazioni sulla definizione delle risorse di rete, vedere [Risorse di rete in vRealize Automation](#).

Per informazioni sulla definizione dei profili di rete, vedere [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

Ulteriori informazioni sulle risorse di tag e gruppi di sicurezza nei modelli cloud di vRealize Automation

Quando si creano o si modificano i modelli cloud di vRealize Automation, utilizzare le opzioni delle risorse di sicurezza più appropriate per i propri obiettivi.

Risorsa del gruppo di sicurezza indipendente dal cloud

È possibile aggiungere una risorsa del gruppo di sicurezza utilizzando la risorsa **Indipendente dal cloud > Gruppo di sicurezza** nella pagina di progettazione del modello cloud. La risorsa viene visualizzata nel codice del modello cloud come tipo di risorsa `Cloud.SecurityGroup`. La risorsa predefinita viene visualizzata come:

```
Cloud_SecurityGroup_1:
  type: Cloud.SecurityGroup
  properties:
    constraints: []
    securityGroupType: existing
```

È possibile specificare una risorsa del gruppo di sicurezza in una progettazione di modelli cloud come esistente (`securityGroupType: existing`) o su richiesta (`securityGroupType: new`).

È possibile aggiungere un gruppo di sicurezza esistente al modello cloud oppure utilizzare un gruppo di sicurezza esistente che è stato aggiunto a un profilo di rete.

Per NSX-V e NSX-T, oltre a NSX-T con il commutatore di gestione dei criteri abilitato in combinazione con VMware Cloud on AWS, è possibile aggiungere un gruppo di sicurezza esistente o definire un nuovo gruppo di sicurezza quando si progetta o si modifica il modello cloud. I gruppi di sicurezza su richiesta sono supportati per NSX-T, NSX-V e VMware Cloud on AWS quando viene utilizzato con la gestione dei criteri di NSX-T.

Per tutti i tipi di account cloud, ad eccezione di Microsoft Azure, è possibile associare uno o più gruppi di sicurezza alla scheda NIC di una macchina. La scheda NIC di una macchina virtuale di Microsoft Azure (*machineName*) può essere associata a un solo gruppo di sicurezza.

Per impostazione predefinita, la proprietà del gruppo di sicurezza `securityGroupType` è impostata su `existing`. Per creare un gruppo di sicurezza su richiesta, immettere `new` per la proprietà `securityGroupType`. Per specificare le regole del firewall per un gruppo di sicurezza su richiesta, utilizzare la proprietà `rules` nella sezione `Cloud.SecurityGroup` della risorsa del gruppo di sicurezza.

Gruppi di sicurezza esistenti

I gruppi di sicurezza esistenti vengono creati in una risorsa di account cloud di origine, ad esempio NSX-T o Amazon Web Services. Sono dati raccolti da vRealize Automation dall'origine. È possibile selezionare un gruppo di sicurezza esistente in un elenco di risorse disponibili come parte di un profilo di rete di vRealize Automation. In una progettazione di modelli cloud, è possibile specificare un gruppo di sicurezza esistente, intrinsecamente tramite la relativa appartenenza a un profilo di rete specificato o in modo specifico in base al nome, utilizzando l'impostazione `securityGroupType: existing` in una risorsa del gruppo di sicurezza. Se si aggiunge un gruppo di sicurezza a un profilo di rete, aggiungere almeno un tag di funzionalità al profilo di rete. Le risorse del gruppo di sicurezza su richiesta richiedono un tag di vincolo quando vengono utilizzate nella progettazione di un modello cloud.

È possibile associare una risorsa del gruppo di sicurezza della progettazione del modello cloud a una o più risorse di macchina.

Nota Se si intende utilizzare una risorsa macchina nella progettazione del modello cloud per eseguire il provisioning nella scheda NIC di una macchina virtuale di Microsoft Azure (*machineName*), è necessario associare la risorsa macchina a un singolo gruppo di sicurezza.

Gruppi di sicurezza su richiesta

È possibile definire gruppi di sicurezza su richiesta quando si definisce o si modifica una progettazione di modelli cloud utilizzando l'impostazione `securityGroupType: new` nel codice di risorsa del gruppo di sicurezza.

È possibile utilizzare un gruppo di sicurezza su richiesta per NSX-V e NSX-T, nonché per Amazon Web Services quando viene utilizzato con il tipo di criterio di NSX-T, per applicare un set specifico di regole del firewall a una risorsa macchina di rete oppure a un set di risorse raggruppate. Ogni gruppo di sicurezza può contenere più regole del firewall denominate. È possibile utilizzare un

gruppo di sicurezza su richiesta per specificare servizi o protocolli e porte. Si noti che è possibile specificare un servizio o un protocollo, ma non entrambi. È possibile specificare una porta oltre a un protocollo. Non è possibile specificare una porta se si specifica un servizio. Se la regola non contiene un servizio o un protocollo, il valore predefinito del servizio è Qualsiasi.

Nelle regole del firewall, è inoltre possibile specificare gli indirizzi IP e gli intervalli IP. Alcuni esempi di regole del firewall sono illustrati in [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Quando si creano regole del firewall in un gruppo di sicurezza su richiesta di NSX-V o NSX-T, il comportamento predefinito è consentire il traffico di rete specificato, ma anche altro traffico di rete. Per controllare il traffico di rete, è necessario specificare un tipo di accesso per ogni regola. I tipi di accesso alla regola sono:

- **Allow** (impostazione predefinita): consente il traffico di rete specificato in questa regola del firewall.
- **Deny**: blocca il traffico di rete specificato in questa regola del firewall. Comunica attivamente al client che la connessione è stata rifiutata.
- **Drop**: rifiuta il traffico di rete specificato in questa regola del firewall. Interrompe in modo invisibile il pacchetto come se il listener non fosse online.

Per un esempio di progettazione che utilizza una regole del firewall `access: Allow` e `access: Deny`, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Nota Un amministratore del cloud può creare una progettazione di modelli cloud che contenga solo un gruppo di sicurezza su richiesta di NSX e può distribuire tale progetto per creare una risorsa del gruppo di sicurezza riutilizzabile esistente che i membri dell'organizzazione possono aggiungere ai profili di rete e alle progettazioni di modelli cloud come gruppo di sicurezza esistente.

Le regole del firewall supportano i valori CIDR in formato IPv4 o IPv6 per gli indirizzi IP di origine e di destinazione. Per un esempio di progettazione che utilizza i valori CIDR IPv6 in una regola del firewall, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Gruppi di sicurezza su richiesta ed esistenti per VMware Cloud on AWS

È possibile definire un gruppo di sicurezza su richiesta per una macchina di VMware Cloud on AWS in un modello cloud utilizzando l'impostazione `securityGroupType: new` nel codice di risorsa del gruppo di sicurezza.

Di seguito viene illustrato un frammento di codice di esempio per un gruppo di sicurezza su richiesta:

```
resources:
  Cloud_SecurityGroup_1:
    type: Cloud.SecurityGroup
    properties:
      name: vmc-odsg
      securityGroupType: new
```

```
rules:
  - name: datapath
    direction: inbound
    protocol: TCP
    ports: 5011
    access: Allow
    source: any
```

È inoltre possibile definire un gruppo di sicurezza esistente per una macchina VMware Cloud on AWS di rete e includere facoltativamente tag di vincolo, come illustrato negli esempi seguenti:

```
Cloud_SecurityGroup_2:
  type: Cloud.SecurityGroup
  properties:
    constraints: [xyz]
    securityGroupType: existing
```

```
Cloud_SecurityGroup_3:
  type: Cloud.SecurityGroup
  properties:
    securityGroupType: existing
    constraints:
      - tag: xyz
```

Lo sviluppo di modelli cloud iterativi è supportato.

- Se un gruppo di sicurezza è associato a una o più macchine nella distribuzione e si esegue un'azione di eliminazione, viene visualizzato un messaggio che indica che il gruppo di sicurezza non può essere eliminato.
- Se un gruppo di sicurezza non è associato ad alcuna macchina nella distribuzione e si esegue un'azione di eliminazione, viene visualizzato un messaggio che indica che il gruppo di sicurezza verrà eliminato da questa distribuzione e l'azione non potrà essere annullata. Un gruppo di sicurezza esistente viene eliminato dal modello cloud, mentre un gruppo di sicurezza su richiesta viene eliminato definitivamente.

Utilizzo dei tag di sicurezza di NSX-V e dei tag di macchina virtuale di NSX-T

È possibile visualizzare e utilizzare tag di sicurezza di NSX-V, NSX-T e NSX-T con i tag di macchina virtuale del criterio dalle risorse gestite nei modelli cloud di vRealize Automation.

I tag di sicurezza di NSX-V e NSX-T sono supportati per l'utilizzo con vSphere. I tag di sicurezza di NSX-T sono supportati anche per l'utilizzo con VMware Cloud on AWS.

Nota Come per le macchine virtuali distribuite in vSphere, è possibile configurare i tag delle macchine per una macchina virtuale da distribuire in VMware Cloud on AWS. È inoltre possibile aggiornare il tag della macchina dopo la distribuzione iniziale. Questi tag della macchina consentono a vRealize Automation di assegnare dinamicamente una macchina virtuale a un gruppo di sicurezza di NSX-T appropriato durante la distribuzione.

È possibile specificare tag di sicurezza di NSX-V utilizzando `key: nsxSecurityTag` e un valore di tag nella risorsa di elaborazione del modello cloud, come illustrato nell'esempio seguente, a condizione che la macchina sia connessa a una rete di NSX-V:

```
tags:
  - key: nsxSecurityTag
    value: security_tag_1
  - key: nsxSecurityTag
    value: security_tag_2
```

Il valore specificato deve corrispondere a un tag di sicurezza di NSX-V. Se non sono presenti tag di sicurezza in NSX-V che corrispondono al valore della chiave `nsxSecurityTag` specificato, la distribuzione non riesce.

Nota L'assegnazione dei tag di sicurezza di NSX-V richiede che la macchina sia connessa a una rete di NSX-V. Se la macchina è connessa a una rete di vSphere, l'assegnazione dei tag di sicurezza di NSX-V viene ignorata. In entrambi i casi, viene assegnato un tag anche alla macchina vSphere.

NSX-T non dispone di un tag di sicurezza separato. Qualsiasi tag specificato nella risorsa di elaborazione del modello cloud comporta l'associazione della macchina virtuale distribuita con tutti i tag specificati in NSX-T. Per NSX-T, incluso NSX-T con criterio, i tag di macchina virtuale vengono espressi anche come coppia chiave-valore nel modello cloud. L'impostazione `key` corrisponde all'impostazione `scope` in NSX-T e l'impostazione `value` corrisponde al `Tag Name` specificato in NSX-T.

Si tenga presente che se si utilizza l'assistente migrazione di vRealize Automation V2T per eseguire la migrazione degli account cloud da NSX-V a NSX-T, incluso NSX-T con criterio, l'assistente migrazione crea una coppia chiave-valore `nsxSecurityTag`. In questo scenario o se `nsxSecurityTag` è per qualsiasi motivo specificato esplicitamente in un modello cloud per l'utilizzo con NSX-T, incluso NSX-T con criterio, la distribuzione crea un tag di macchina virtuale con un'impostazione Ambito vuota con un nome di tag che corrisponde al `value` specificato. Quando si visualizzano tali tag in NSX-T, la colonna Ambito sarà vuota.

Per evitare confusione, non utilizzare coppie chiave-valore `nsxSecurityTag` nel caso di NSX-T. Se si specifica una coppia chiave-valore `nsxSecurityTag` da utilizzare con NSX-T, incluso NSX-T con criterio, la distribuzione crea un tag di macchina virtuale con un'impostazione Ambito vuota con un nome di tag che corrisponde al `value` specificato. Quando si visualizzano tali tag in NSX-T, la colonna Ambito sarà vuota.

Utilizzo dei criteri di isolamento app nelle regole del firewall del gruppo di sicurezza su richiesta

È possibile utilizzare un criterio di isolamento app per consentire solo il traffico interno tra le risorse di cui il modello cloud esegue il provisioning. Con l'isolamento app, le macchine sottoposte a provisioning dal modello cloud possono comunicare tra loro ma non possono connettersi all'esterno del firewall. È possibile creare un criterio di isolamento app nel profilo di rete. È inoltre possibile specificare l'isolamento app nella progettazione di un modello cloud utilizzando un gruppo di sicurezza su richiesta con una regola del firewall Nega oppure una rete privata o in uscita.

Un criterio di isolamento app viene creato con una precedenza inferiore. Se si applicano più criteri, i criteri con il peso superiore avranno la precedenza.

Quando si crea un criterio di isolamento applicazione, viene generato automaticamente un nome di criterio. Il criterio viene inoltre reso disponibile per il riutilizzo in altre progettazioni di modelli cloud e iterazioni specifiche dell'endpoint e del progetto della risorsa associata. Il nome del criterio di isolamento app non è visibile nel modello cloud, ma è visibile come proprietà personalizzata nella pagina del progetto (**Infrastruttura > Amministrazione > Progetti**) dopo la distribuzione della progettazione del modello cloud.

Per lo stesso endpoint associato in un progetto, tutte le distribuzioni che richiedono un gruppo di sicurezza su richiesta per l'isolamento app possono utilizzare lo stesso criterio di isolamento app. Una volta creato, il criterio non viene eliminato. Quando si specifica un criterio di isolamento app, vRealize Automation cerca il criterio all'interno del progetto e relativamente all'endpoint associato. Se lo trova, lo riutilizza. Se non lo trova, lo crea. Il nome del criterio di isolamento app è visibile solo dopo la sua distribuzione iniziale nell'elenco delle proprietà personalizzate del progetto.

Utilizzo dei gruppi di sicurezza nello sviluppo di modelli cloud iterativi

Quando si modificano i vincoli del gruppo di sicurezza durante lo sviluppo iterativo e il gruppo di sicurezza non è associato a una macchina nel modello cloud, il gruppo di sicurezza viene aggiornato nell'iterazione come specificato. Tuttavia, quando il gruppo di sicurezza è già associato a una macchina, la ridistribuzione non riesce. È necessario scollegare i gruppi di sicurezza esistenti e/o le proprietà della risorsa `securityGroupType` dalle macchine associate durante lo sviluppo iterativo del modello cloud e associarli nuovamente tra una ridistribuzione e l'altra. Il workflow necessario è il seguente, presupponendo che il modello cloud sia stato distribuito inizialmente.

- 1 Nella funzionalità di progettazione del modello di Cloud Assembly, scollegare il gruppo di sicurezza da tutte le relative macchine associate nel modello cloud.
- 2 Ridistribuire il modello facendo clic su **Aggiorna una distribuzione esistente**.
- 3 Rimuovere i tag di vincolo del gruppo di sicurezza esistenti e/o le proprietà `securityGroupType` nel modello.
- 4 Aggiungere i nuovi tag di vincolo del gruppo di sicurezza e/o le proprietà `securityGroupType` nel modello.
- 5 Associare i nuovi tag di vincolo del gruppo di sicurezza e/o le istanze della proprietà `securityGroupType` alle macchine nel modello.

6 Ridistribuire il modello facendo clic su **Aggiorna una distribuzione esistente**.

Operazioni giorno 2 disponibili

Per un elenco delle operazioni giorno 2 comuni disponibili per le risorse di modello cloud e distribuzione, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Ulteriori informazioni

Per informazioni sull'utilizzo di un gruppo di sicurezza per l'isolamento di rete, vedere [Risorse di sicurezza in vRealize Automation](#).

Per informazioni sull'utilizzo dei gruppi di sicurezza nei profili di rete, vedere [Ulteriori informazioni sui profili di rete in vRealize Automation](#) e [Utilizzo delle impostazioni dei gruppi di sicurezza in profili di rete e progettazioni di modelli cloud in vRealize Automation](#).

Per esempi di utilizzo dei gruppi di sicurezza nei modelli cloud, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Ulteriori informazioni sulle risorse di bilanciamento del carico nei modelli cloud di vRealize Automation

Quando si creano o si modificano i modelli cloud di vRealize Automation, utilizzare le risorse di bilanciamento del carico più appropriate per i propri obiettivi.

È possibile utilizzare NSX e risorse di bilanciamento del carico indipendenti dal cloud in un modello cloud per controllare il bilanciamento del carico in una distribuzione.

Il bilanciamento del carico indipendente dal cloud può essere distribuito in più cloud. Un bilanciamento del carico specifico del cloud consente la definizione di impostazioni e funzionalità avanzate disponibili solo per un cloud o una topologia specifici. Le proprietà specifiche del cloud sono disponibili nel tipo di risorsa bilanciamento del carico NSX (Cloud.NSX.LoadBalancer). Se si aggiungono queste proprietà in un bilanciamento del carico indipendente dal cloud (Cloud.LoadBalancer), vengono ignorate se ad esempio viene eseguito il provisioning di un bilanciamento del carico Amazon Web Services o Microsoft Azure, ma vengono rispettate se viene eseguito il provisioning di un bilanciamento del carico NSX-V o NSX-T. Scegliere uno dei tipi di risorse di bilanciamento del carico disponibili in base alle condizioni del modello cloud di vRealize Automation.

Non è possibile connettere una risorsa di bilanciamento del carico direttamente a una risorsa del gruppo di sicurezza nella tela di progettazione.

Risorsa di bilanciamento del carico indipendente dal cloud

Utilizzare un bilanciamento del carico indipendente dal cloud quando si desidera specificare le caratteristiche di rete per qualsiasi tipo di macchina di destinazione.

È possibile aggiungere un bilanciamento del carico indipendente dal cloud utilizzando la risorsa **Indipendente dal cloud > Bilanciamento del carico** nella pagina di progettazione del modello cloud. La risorsa viene visualizzata nel codice del modello cloud come tipo di risorsa `Cloud.LoadBalancer`. La risorsa predefinita viene visualizzata come:

```
Cloud_LoadBalancer_1:
  type: Cloud.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
    internetFacing: false
```

Risorsa di bilanciamento del carico di NSX

Utilizzare un bilanciamento del carico NSX quando il modello cloud contiene caratteristiche specifiche di NSX-V o NSX-T (metodi Policy API o Manager API). È possibile collegare uno o più bilanciamenti del carico a una rete NSX-V o NSX-T oppure a macchine associate a una rete NSX-V o NSX-T.

È possibile aggiungere un bilanciamento del carico NSX utilizzando la risorsa **NSX > Bilanciamento del carico**. La risorsa viene visualizzata nel codice del modello cloud come tipo di risorsa `Cloud.NSX.LoadBalancer`. La risorsa predefinita viene visualizzata come:

```
Cloud_NSX_LoadBalancer_1:
  type: Cloud.NSX.LoadBalancer
  properties:
    routes: []
    network: ''
    instances: []
```

Opzioni del bilanciamento del carico nel codice del modello cloud

L'aggiunta di una o più risorse del bilanciamento del carico al modello cloud consente di specificare le impostazioni seguenti. Alcuni esempi sono disponibili nella sezione [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Il protocollo HTTP è supportato per tutti i bilanciamenti del carico su richiesta.

Il protocollo HTTPS è supportato solo per i bilanciamenti del carico su richiesta associati a un account cloud di NSX-T la cui modalità NSX è impostata su **Criterio**. Gli account cloud di NSX-T la cui modalità NSX è impostata su **Manager** non possono utilizzare il protocollo HTTPS.

■ Definizione della macchina

È possibile specificare le risorse denominate della macchina che devono partecipare a un pool di bilanciamento del carico. In alternativa, è possibile specificare che la scheda NIC di una macchina specifica partecipi al pool di bilanciamento del carico.

Questa opzione è disponibile solo per la risorsa bilanciamento del carico **NSX** (`Cloud.NSX.LoadBalancer`).

- `resource.Cloud_Machine_1.id`

Specifica che il bilanciamento del carico include la macchina identificata nel codice del modello cloud come *Cloud_Machine_1*.

- `resource.Cloud_Machine_2.networks[2].id`

Specifica che il bilanciamento del carico include la macchina identificata nel codice del modello cloud come *Cloud_Machine_2* solo quando viene distribuita nella scheda NIC della macchina *Cloud_Machine_2.networks[2]*.

- Livello di registrazione

Il valore del livello di registrazione specifica un livello di gravità per il registro degli errori.

Le opzioni sono nessuna NONE, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, INFO, DEBUG e NOTICE. Il valore del livello di registrazione si applica a tutti i bilanciamenti del carico nel modello cloud. Questa opzione è specifica di NSX. Per i bilanciamenti del carico con un elemento principale, l'impostazione del livello di registrazione principale sostituisce qualsiasi impostazione del livello di registrazione nei relativi elementi secondari.

Per informazioni correlate, vedere argomenti come [l'aggiunta di bilanciamenti del carico](#) nella documentazione di prodotto di NSX.

- Tipo

Utilizzare un tipo di bilanciamento del carico per specificare una dimensione di scala. Il valore predefinito è small. Questa opzione è specifica di NSX. Per i bilanciamenti del carico con un elemento principale, l'impostazione del tipo principale sostituisce qualsiasi impostazione di tipo nei relativi elementi secondari.

- Piccolo

Correlato a compact in NSX-V e small in NSX-T.

- Medio

Correlato a large in NSX-V e medium in NSX-T.

- Grande

Correlato a quad-large in NSX-V e large in NSX-T.

- Molto grande

Correlato a xlarge in NSX-V e large in NSX-T.

Per informazioni correlate, vedere argomenti come il [ridimensionamento delle risorse del bilanciamento del carico](#) nella documentazione di prodotto di NSX.

Questa opzione è disponibile per la risorsa di bilanciamento del carico **NSX** (`Cloud.NSX.LoadBalancer`).

- Algoritmo (pool di server)

Utilizzare un metodo di bilanciamento algoritmo per controllare il modo in cui le connessioni in entrata vengono distribuite tra i membri del pool di server. L'algoritmo può essere utilizzato in un pool di server o direttamente in un server. Tutti gli algoritmi di bilanciamento del carico ignorano i server che soddisfano una delle seguenti condizioni:

- Lo stato dell'amministratore è impostato su DISABLED.
- Lo stato dell'amministratore è impostato su GRACEFUL_DISABLED e non è presente alcuna voce di persistenza corrispondente.
- Lo stato del controllo di integrità attivo o passivo è DOWN.
- È stato raggiunto il limite massimo di connessioni simultanee del pool di server.

Questa opzione è specifica di NSX.

- IP_HASH

Seleziona un server in base a un hash dell'indirizzo IP di origine e al peso totale di tutti i server in esecuzione.

È correlato a IP-HASH in NSX-V e NSX-T.

- LEAST_CONNECTION

Distribuisce le richieste del client a più server in base al numero di connessioni già presenti nel server. Le nuove connessioni vengono inviate al server con il minor numero di connessioni. Ignora i pesi dei membri del pool di server anche se sono configurati.

È correlato a LEASTCONN in NSX-V e LEAST_CONNECTION in NSX-T.

- ROUND_ROBIN

Le richieste dei client in entrata vengono assegnate a un elenco di server disponibili in grado di gestirle, uno alla volta e ciclicamente. Con questa opzione, il peso dei membri del pool di server viene ignorato anche se è configurato. Questa è l'impostazione predefinita.

È correlato a ROUND_ROBIN in NSX-V e NSX-T.

- WEIGHTED_LEAST_CONNECTION

A ciascun server viene assegnato un valore di peso che indica le prestazioni del server rispetto agli altri server nel pool. Tale valore determina il numero di richieste dei client inviate a un server rispetto agli altri server nel pool. Questo algoritmo di bilanciamento del carico utilizza il valore del peso per distribuire equamente il carico tra le risorse server disponibili. Per impostazione predefinita, il valore del peso è 1 se tale valore non viene configurato e l'opzione di avvio lento è abilitata.

È correlato a WEIGHTED_LEAST_CONNECTION in NSX-T. Non c'è correlazione in NSX-V.

- WEIGHTED_ROUND_ROBIN

A ciascun server viene assegnato un valore di peso che fornisce che indica le prestazioni del server rispetto agli altri server nel pool. Tale valore determina il numero di richieste dei client inviate a un server rispetto agli altri server nel pool. L'obiettivo di questo algoritmo di bilanciamento del carico è quello di distribuire equamente il carico tra le risorse server disponibili.

È correlato a WEIGHTED_ROUND_ROBIN in NSX-T. Non c'è correlazione in NSX-V.

■ URI

Tramite la parte sinistra dell'URI viene calcolato un hash che viene quindi diviso per il peso totale dei server in esecuzione. Il risultato indica il server che riceverà la richiesta. Ciò assicura che un URI venga sempre indirizzato allo stesso server purché nessun altro server diventi attivo o inattivo. Il parametro dell'algoritmo URI ha due opzioni, ovvero `uriLength=<len>` e `uriDepth=<dep>`. L'intervallo del parametro della lunghezza deve essere $1 \leq len < 256$. L'intervallo del parametro della profondità deve essere $1 \leq dep < 10$. I parametri di lunghezza e profondità sono seguiti da un numero intero positivo. Queste opzioni possono bilanciare i server solo in base alla parte iniziale dell'URI. Il parametro della lunghezza indica che l'algoritmo deve prendere in considerazione solo i caratteri definiti all'inizio dell'URI per calcolare l'hash. Il parametro della profondità indica la profondità di directory massima da utilizzare per calcolare l'hash. Viene conteggiato un livello per ciascuna barra presente nella richiesta. Se sono specificati entrambi i parametri, la valutazione termina quando viene raggiunto uno dei parametri.

È correlato a URI in NSX-V. Non c'è correlazione in NSX-T.

■ HTTPHEADER

In ciascuna richiesta HTTP viene cercato il nome dell'intestazione HTTP. Per il nome dell'intestazione tra parentesi non viene fatta distinzione tra maiuscole e minuscole. Se l'intestazione è assente o non contiene alcun valore, viene applicato l'algoritmo round robin. Il parametro dell'algoritmo HTTPHEADER ha un'unica opzione, ovvero `headerName=<name>`.

È correlato a HTTPHEADER in NSX-V. Non c'è correlazione in NSX-T.

■ URL

Nella stringa di query di ciascuna richiesta HTTP GET viene cercato il parametro URL specificato nell'argomento. Se il parametro è seguito da un segno di uguale = e da un valore, viene calcolato l'hash del valore, il quale viene poi diviso per il peso totale dei server in esecuzione. Il risultato indica il server che riceverà la richiesta. Questo processo viene utilizzato per tenere traccia degli identificatori utente nelle richieste e assicurare che lo stesso ID utente venga sempre inviato allo stesso server purché nessun altro server diventi attivo o inattivo. Se non viene trovato alcun valore o parametro, viene applicato un algoritmo round robin. Il parametro dell'algoritmo URL ha un'unica opzione, ovvero `urlParam=<url>`.

È correlato a URL in NSX-V. Non c'è correlazione in NSX-T.

Per informazioni correlate, vedere argomenti come [l'aggiunta di un pool di server per il bilanciamento del carico](#) nella documentazione di prodotto di NSX.

■ Monitoraggio dell'integrità

Utilizzare le opzioni di monitoraggio dell'integrità per verificare se un server è disponibile. È supportato il monitoraggio dell'integrità attivo per i protocolli HTTP, ICMP, TCP e UDP. Il monitoraggio dell'integrità passivo è disponibile solo per NSX-T.

Questa opzione è specifica di NSX.

■ httpMethod

Metodo HTTP da utilizzare per rilevare lo stato del server per la richiesta di controllo dell'integrità. I metodi sono GET, HEAD, OPTIONS, PUT e POST.

■ requestBody

Contenuto del corpo della richiesta di controllo dell'integrità. Utilizzato e necessario per i protocolli HTTP, TCP e UDP.

■ responseBody

Contenuto del corpo della risposta prevista dal controllo dell'integrità. Se la stringa ricevuta corrisponde a questo corpo della risposta, il server viene considerato integro. Utilizzato e necessario per i protocolli HTTP, TCP e UDP.

Nota Se si utilizza il protocollo di monitoraggio UDP, i parametri `UDP Data Sent` e `UDP Data Expected` sono necessari. Le proprietà `requestBody` e `responseBody` vengono mappate a questi parametri.

Questa opzione è disponibile per la risorsa bilanciamento del carico di NSX (`Cloud.NSX.LoadBalancer`).

Per informazioni correlate, vedere argomenti come la [configurazione del monitoraggio dell'integrità attivo](#) nella documentazione di prodotto di NSX.

■ Controllo dell'integrità

Utilizzare le opzioni di controllo dell'integrità per specificare in che modo il bilanciamento del carico esegue il controllo dell'integrità.

Questa opzione è disponibile solo per la risorsa bilanciamento del carico di NSX (`Cloud.NSX.LoadBalancer`).

Per un esempio di impostazioni di controllo dell'integrità disponibili, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Tipi di rete e opzioni di bilanciamento del carico di NSX-V e NSX-T

Le opzioni di bilanciamento del carico dipendono dalla rete a cui è associata la risorsa di bilanciamento del carico nel modello cloud. È possibile configurare un bilanciamento del carico relativo al tipo di rete e alle condizioni della rete.

■ Rete su richiesta

Se le risorse di elaborazione del bilanciamento del carico sono collegate a una rete su richiesta, viene creato un nuovo router di livello 1, che viene collegato al router di livello 0 specificato nel profilo di rete. Il bilanciamento del carico viene quindi collegato al router di livello 1. L'annuncio VIP del router di livello 1 è attivato se il VIP si trova su una rete esistente. Se una rete su richiesta è configurata per DHCP, la rete su richiesta e il bilanciamento del carico condividono il router di livello 1.

■ Rete esistente

Se il bilanciamento del carico è collegato a una rete esistente, viene creato un bilanciamento del carico per il router di livello 1 della rete esistente. Viene creato un nuovo bilanciamento del carico se al router di livello 1 non è collegato alcun servizio di bilanciamento del carico. Se il bilanciamento del carico esiste già, i nuovi server virtuali vengono collegati a tale bilanciamento del carico. Se la rete esistente non è collegata a un router di livello 1, un nuovo router di livello 1 viene creato e collegato a un router di livello 0 definito nel profilo di rete. L'annuncio VIP del router di livello 1 non è abilitato.

vRealize Automation non supporta un bilanciamento del carico a due bracci (bilanciamento del carico inline) di NSX-T su due reti esistenti diverse. Si tenga presente che in uno scenario di bilanciamento del carico a due bracci, l'uplink VIP si trova in una rete esistente, mentre le macchine che fanno parte del pool sono connesse a una rete su richiesta. Per specificare il bilanciamento del carico quando si utilizza una rete esistente, è necessario configurare un bilanciamento del carico a un braccio in cui la stessa rete esistente viene utilizzata per il VIP del bilanciamento del carico e per le macchine che fanno parte del pool. Tuttavia, a partire da vRealize Automation 8.4.2, se si utilizza un bilanciamento del carico selezionato nel profilo di rete, è possibile bilanciare il carico tra le macchine su due reti esistenti diverse se è presente la connettività tra le due reti esistenti.

■ Isolamento di rete definito nel profilo di rete

Per i tipi di rete `outbound` o `private`, è possibile specificare le impostazioni di isolamento di rete in un profilo di rete per emulare un nuovo gruppo di sicurezza. Poiché le macchine sono collegate a una rete esistente e le impostazioni di isolamento sono definite nel profilo, questa opzione è simile a un bilanciamento del carico creato in una rete esistente. La differenza è che per attivare il percorso dei dati, l'IP della porta di uplink di livello 1 viene aggiunto al gruppo di sicurezza di isolamento.

È possibile specificare le impostazioni di bilanciamento del carico per le reti associate a NSX utilizzando una risorsa di bilanciamento del carico di NSX nella progettazione del modello cloud.

Per ulteriori informazioni, vedere il post [vRA Cloud Assembly Load Balancer with NSX-T Deep Dive](#) nel blog di VMware.

Riconfigurazione delle impostazioni del livello o del tipo di registrazione quando più bilanciamenti del carico condividono un NSX-T di livello 1 o un edge NSX-V

Quando si utilizza un modello cloud che contiene più bilanciamenti del carico che condividono un router di livello 1 nell'endpoint di NSX-T o un router edge nell'endpoint di NSX-V, la riconfigurazione delle impostazioni del livello o del tipo di registrazione in una delle risorse del bilanciamento del carico non aggiorna le impostazioni per gli altri bilanciamenti del carico. Le impostazioni non corrispondenti causano incoerenze in NSX. Per evitare incoerenze quando si riconfigurano queste impostazioni del livello e/o del tipo di registrazione, utilizzare gli stessi valori di riconfigurazione per tutte le risorse del bilanciamento del carico nel modello cloud che condividono un router di livello 1 o un nell'endpoint NSX associato.

Operazioni giorno 2 disponibili

Quando si esegue la scalabilità verticale o la scalabilità orizzontale di una distribuzione che contiene un bilanciamento del carico, il bilanciamento del carico viene configurato in modo da includere le macchine appena aggiunte o interrompere le macchine di bilanciamento del carico destinate alla disinstallazione.

Per un elenco delle operazioni giorno 2 comuni disponibili per i modelli cloud e le distribuzioni, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Ulteriori informazioni

Per informazioni sulla definizione delle impostazioni di bilanciamento del carico in un profilo di rete, vedere [Ulteriori informazioni sui profili di rete in vRealize Automation](#).

Per esempi di progettazioni di modelli cloud che includono bilanciamenti del carico, vedere [Reti, risorse di sicurezza e bilanciamenti del carico in vRealize Automation](#).

Modello cloud abilitato per Puppet con accesso tramite nome utente e password

In questo esempio è possibile aggiungere la gestione della configurazione Puppet a un modello cloud distribuito su una risorsa di elaborazione di vCenter con accesso tramite nome utente e password.

Questa procedura mostra un esempio di creazione di una risorsa distribuibile abilitata a Puppet che richiede l'autenticazione con nome utente e password. L'accesso tramite nome utente e password significa che l'utente deve eseguire manualmente l'accesso dalla risorsa di elaborazione alla macchina primaria di Puppet per richiamare la gestione della configurazione Puppet.

Facoltativamente, è possibile configurare l'autenticazione dell'accesso remoto che configura la gestione della configurazione in un modello cloud, in modo che la risorsa di elaborazione gestisca l'autenticazione con la macchina primaria di Puppet. Con l'accesso remoto attivato, la risorsa di elaborazione genera automaticamente una chiave per soddisfare il requisito di autenticazione con password. È ancora necessario un nome utente valido.

Vedere [Esempi di modelli cloud di gestione della configurazione di Puppet in AWS](#) e [Esempi di modelli cloud di configurazione Puppet di vCenter](#) per ulteriori esempi di configurazione di scenari Puppet differenti nei blueprint di Cloud Assembly.

Prerequisiti

- Configurare un'istanza di Puppet Enterprise su una rete valida.
- Aggiungere l'istanza di Puppet Enterprise a Cloud Assembly utilizzando la funzionalità Integrazioni. Vedere [Configurazione dell'integrazione di Puppet Enterprise in Cloud Assembly](#).
- Configurare un account di vSphere e una risorsa di elaborazione di vCenter.

Procedura

- 1 Aggiungere un componente di gestione della configurazione Puppet a una risorsa di elaborazione di vSphere sulla tela per il modello cloud desiderato.
 - a Selezionare **Infrastruttura > Gestisci > Integrazioni**.
 - b Fare clic su **Aggiungi integrazione** e selezionare Puppet.
 - c Immettere le informazioni appropriate nella pagina di configurazione Puppet.

Configurazione	Descrizione	Valore di esempio
Nome host	Nome host o indirizzo IP della macchina primaria di Puppet	Puppet-Ubuntu
Porta SSH	Porta SSH di comunicazione tra Cloud Assembly e la macchina prima di Puppet. (Facoltativa)	NA
Segreto per firma automatica	Il segreto condiviso configurato nella macchina primaria di Puppet che i nodi devono fornire per supportare le richieste di certificato firmato automaticamente.	Specifico dell'utente
Posizione	Indicare se la macchina prima di Puppet si trova in un cloud privato o pubblico. Nota La distribuzione tra cloud è supportata solo se è presente la connettività tra le risorse di elaborazione della distribuzione e la macchina primaria di Puppet.	
Cloud proxy	Non richiesto per gli account cloud pubblici, ad esempio Microsoft Azure o Amazon Web Services. Se si utilizza un account cloud basato su vCenter, selezionare il cloud proxy appropriato per l'account.	NA
Nome utente	Nome utente SSH e RBAC per la macchina primaria di Puppet.	Specifico dell'utente. Il valore YAML è '\$ {input. username}'
Password	Password SSH e RBAC per la macchina primaria di Puppet.	Il valore YAML specifico dell'utente è '\$ {input. password}'
Usa comandi sudo per questo utente	Selezionare per utilizzare i comandi sudo per procidd.	true
Nome	Nome della macchina primaria di Puppet.	PEMasterOnPrem
Descrizione		

- 2 Aggiungere le proprietà username e password al codice YAML di Puppet come mostrato nell'esempio seguente.

- 3 Assicurarsi che il valore della proprietà `remoteAccess` per il codice YAML di del modello cloud Puppet sia impostato su `authentication: username and password`, come illustrato nell'esempio riportato di seguito.

Esempio: Codice YAML di nome utente e password di vCenter

Nell'esempio seguente viene mostrato il codice YAML rappresentativo per l'aggiunta dell'autenticazione con nome utente e password su una risorsa di elaborazione di vCenter.

```
inputs:
  username:
    type: string
    title: Username
    description: Username to use to install Puppet agent
    default: puppet
  password:
    type: string
    title: Password
    default: VMware@123
    encrypted: true
    description: Password for the given username to install Puppet agent
resources:
  Puppet-Ubuntu:
    type: Cloud.vSphere.Machine
    properties:
      flavor: small
      imageRef: >-
        https://cloud-images.ubuntu.com/releases/16.04/release-20170307/ubuntu-16.04-server-
cloudimg-amd64.ova
      remoteAccess:
        authentication: usernamePassword
        username: '${input.username}'
        password: '${input.password}'
  Puppet_Agent:
    type: Cloud.Puppet
    properties:
      provider: PEMasterOnPrem
      environment: production
      role: 'role::linux_webserver'
      username: '${input.username}'
      password: '${input.password}'
      host: '${Puppet-Ubuntu.*}'
      useSudo: true
      agentConfiguration:
        certName: '${Puppet-Ubuntu.address}'
```

Esempi di modelli cloud di gestione della configurazione di Puppet in AWS

Sono disponibili diverse opzioni per la configurazione dei modelli cloud per il supporto della gestione della configurazione basata su Puppet sulle risorse di elaborazione AWS.

Gestione Puppet su AWS con nome utente e password

Esempio di...	Campione di YAML del blueprint
<p>autenticazione della configurazione del cloud sulle Amazon Machine Image supportate.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6/+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} !requiretty" >> /etc/sudoers.d/\${input.username} Puppet_Agent: type: Cloud.Puppet properties: provider: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre>
<p>Autenticazione della configurazione del cloud su una Amazon Machine Image personalizzata con un utente esistente.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 </pre>

Esempio di...	Campione di YAML del blueprint
	<pre> resources: Webserver: type: Cloud.AWS.EC2.Instance properties: flavor: small image: centos cloudConfig: #cloud-config runcmd: - sudo sed -e 's/.*PasswordAuthentication no.*/PasswordAuthentication yes/' -i /etc/ssh/sshd_config - sudo service sshd restart Puppet_Agent: type: Cloud.Puppet properties: provider: PEOAWS environment: production role: 'role::linux_webserver' host: '\${Webserver.*}' osType: linux username: '\${input.username}' password: '\${input.password}' useSudo: true </pre>

Gestione di Puppet su AWS con PublicPrivateKey generata

Esempio di...	Campione di YAML del blueprint
Autenticazione remoteAccess.authentication su AWS con accesso generatedPublicPrivateKey.	<pre> inputs: {} resources: Machine: type: Cloud.AWS.EC2.Instance properties: flavor: small imageRef: ami-a4dc46db remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' useSudo: true </pre>

Esempi di modelli cloud di configurazione Puppet di vCenter

Sono disponibili diverse opzioni per la configurazione dei modelli cloud per il supporto della gestione della configurazione basata su Puppet sulle risorse di elaborazione di vCenter.

Puppet su vSphere con autenticazione con nome utente e password

Nell'esempio seguente viene mostrato l'esempio di codice YAML per Puppet in un'istanza OVA di vSphere con autenticazione con nome utente e password.

Tabella 6-4.

Esempio di...	Campione di YAML del blueprint
<p>Codice YAML per Puppet in un'istanza OVA di vSphere con autenticazione nome utente e password.</p>	<pre> inputs: username: type: string title: Username default: puppet password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre>
<p>Codice YAML per Puppet in un'istanza OVA di vSphere con autenticazione nome utente e password nella risorsa di elaborazione.</p>	<pre> inputs: username: type: string title: Username default: puppet </pre>

Tabella 6-4. (continua)

Esempio di...	Campione di YAML del blueprint
	<pre> password: type: string title: Password encrypted: true default: VMware@123 resources: Puppet_Agent: type: Cloud.Puppet properties: provider: PEonAWS environment: dev role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' useSudo: true host: '\${Webserver.*}' osType: linux agentConfiguration: runInterval: 15m certName: '\${Machine.address}' Webserver: type: Cloud.vSphere.Machine properties: cpuCount: 1 totalMemoryMB: 1024 imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova cloudConfig: #cloud-config ssh_pwauth: yes chpasswd: list: \${input.username}:\${input.password} expire: false users: - default - name: \${input.username} lock_passwd: false sudo: ['ALL=(ALL) NOPASSWD:ALL'] groups: [wheel, sudo, admin] shell: '/bin/bash' ssh-authorized-keys: - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDytVL+Q6+vGbmKXoRpX dmettem@dmettem-m01.vmware.com runcmd: - echo "Defaults:\${input.username} </pre>
<p>Codice YAML per Puppet in un'istanza OVA di vCenter con autenticazione con password mediante accesso remoto nella risorsa di elaborazione.</p>	<pre> inputs: username: type: string title: Username description: Username to use to install Puppet agent default: puppet password: type: string title: Password default: VMware@123 encrypted: true </pre>

Tabella 6-4. (continua)

Esempio di...	Campione di YAML del blueprint
	<pre> description: Password for the given username to install Puppet agent resources: Puppet-Ubuntu: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: usernamePassword username: '\${input.username}' password: '\${input.password}' Puppet_Agent: type: Cloud.Puppet properties: provider: PEMasterOnPrem environment: production role: 'role::linux_webserver' username: '\${input.username}' password: '\${input.password}' host: '\${Puppet-Ubuntu.*}' useSudo: true agentConfiguration: certName: '\${Puppet-Ubuntu.address}' </pre>

Puppet su vSphere con autenticazione PublicPrivateKey generata

Tabella 6-5.

Esempio di...	Campione di YAML del blueprint
Codice YAML per Puppet in un'istanza OVA di vSphere con autenticazione PublicPrivateKey generata nella risorsa di elaborazione.	<pre> inputs: {} resources: Machine: type: Cloud.vSphere.Machine properties: flavor: small imageRef: >- https://cloud-images.ubuntu.com/releases/16.04/ release-20170307/ubuntu-16.04-server-cloudimg-amd64.ova remoteAccess: authentication: generatedPublicPrivateKey Puppet_Agent: type: Cloud.Puppet properties: provider: puppet-BlueprintProvisioningITSuite environment: production role: 'role::linux_webserver' host: '\${Machine.*}' osType: linux username: ubuntu useSudo: true agentConfiguration: runInterval: 15m certName: '\${Machine.address}' - echo "Defaults:\${input.username}" </pre>

Schema delle proprietà delle risorse di vRealize Automation

L'editor infrastructure-as-code di vRealize Automation consente di fare clic o passare il puntatore per la sintassi e la guida per la compilazione del codice. Per visualizzare il set completo di proprietà delle risorse del modello cloud, a volte denominate proprietà personalizzate, fare riferimento allo schema di risorse consolidato.

Lo schema è disponibile nel sito VMware {code}. Seguire il collegamento e fare clic su **Modelli** per visualizzare un elenco degli oggetti risorsa disponibili per i modelli cloud, denominati in precedenza blueprint.

- [Schema del tipo di risorse di vRealize Automation in VMware {code}](#)

Proprietà Cloud Assembly speciali

Cloud Assembly supporta un numero limitato di proprietà che potrebbero essere utili al di fuori degli ambienti di produzione o in altre situazioni speciali. Le proprietà non vengono visualizzate nello schema.

Attenzione Le seguenti proprietà devono essere applicate solo nei casi in cui la personalizzazione del sistema operativo guest non viene testata o prevista.

awaitIp	<p>Per impostazione predefinita, lo stato del provisioning di vRealize Automation non viene segnalato come completato finché il sistema operativo guest non è completamente acceso e la configurazione non è stata completata.</p> <p>L'utilizzo di <code>awaitIp: false</code> consente il completamento del provisioning anche se la configurazione completa non è stata eseguita.</p> <p>ATTENZIONE: l'utilizzo di questa impostazione consente di completare il processo di provisioning prima, ma potrebbe causare la mancata configurazione di una macchina senza indirizzo IP.</p>
awaitHostName	<p>Analogamente ad <code>awaitIp</code>, l'uso di <code>awaitHostName: false</code> consente il completamento del provisioning anche se la macchina potrebbe non essere stata configurata con un nome host.</p>

Altri modi per creare modelli di Cloud Assembly

Oltre a creare un modello di Cloud Assembly da una tela vuota, è possibile sfruttare il codice esistente.

Clonazione del modello cloud

Per clonare un modello, passare a **Progettazione**, selezionare un'origine e fare clic su **Clona**. Si clona un modello cloud per creare una copia in base all'origine, quindi si assegna il clone a un nuovo progetto o si utilizza come codice di avvio per una nuova applicazione.

Caricamento e download

È possibile caricare, scaricare e condividere il codice YAML del modello cloud in qualsiasi modo utile per il proprio sito. È anche possibile modificare il codice del modello utilizzando editor esterni e ambienti di sviluppo.

Nota Un buon metodo per convalidare il codice del modello condiviso consiste nell'esaminarlo nell'editor di codice di Cloud Assembly nella pagina di progettazione.

Integrazione di Cloud Assembly con un repository

Un repository di controllo dell'origine Git integrato può rendere i modelli cloud disponibili per gli utenti idonei come base per una nuova distribuzione. Vedere [Come utilizzare l'integrazione di Git in Cloud Assembly](#).

Estensione e automazione dei cicli di vita delle applicazioni con l'estendibilità

È possibile estendere i cicli di vita dell'applicazione utilizzando le azioni di estendibilità o i workflow di vRealize Orchestrator con le sottoscrizioni di estendibilità.

Con Cloud Assembly Extensibility, è possibile assegnare un'azione di estendibilità o un workflow di vRealize Orchestrator a un evento utilizzando le sottoscrizioni. Quando si verifica l'evento specificato, la sottoscrizione avvia l'azione o il workflow da eseguire e tutti i sottoscrittori vengono informati.

Azioni di estendibilità

Le azioni di estendibilità sono script di codice piccoli e leggeri utilizzati per specificare un'azione e la modalità di esecuzione di tale azione. È possibile importare azioni di estendibilità dai modelli di azioni di Cloud Assembly predefiniti o da un file ZIP. È inoltre possibile utilizzare l'editor delle azioni per creare script personalizzati per le azioni di estendibilità. Quando più script di azione sono collegati tra loro in uno script, si crea un flusso di azione. Utilizzando i flussi di azione, è possibile creare una sequenza di azioni. Per informazioni sull'utilizzo dei flussi di azione, vedere [Che cos'è un flusso di azione](#).

Workflow di vRealize Orchestrator

Integrando Cloud Assembly con l'ambiente vRealize Orchestrator esistente, è possibile utilizzare i workflow nelle sottoscrizioni di estendibilità.

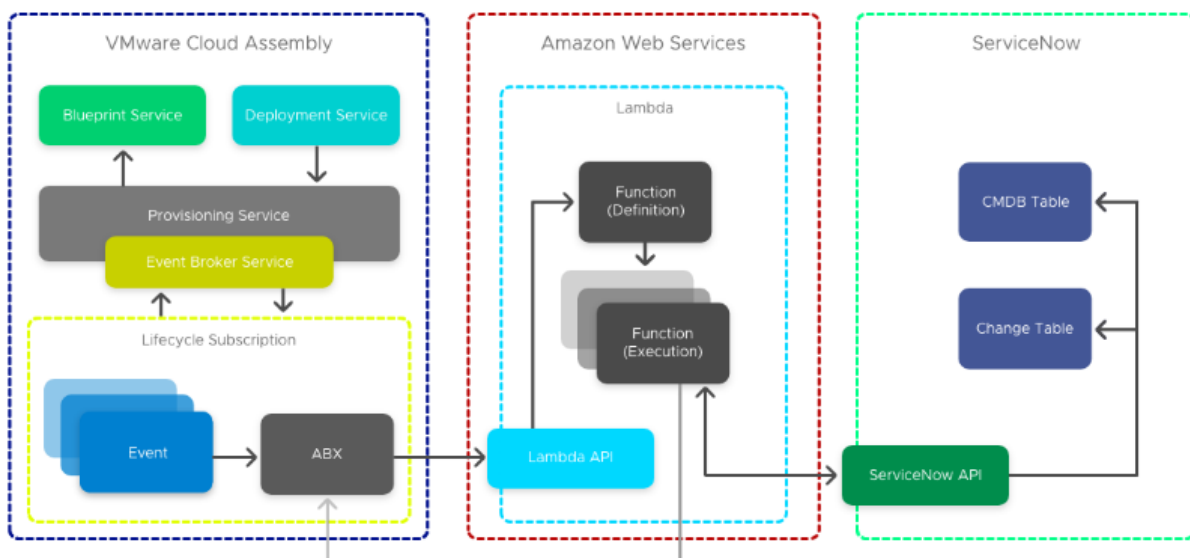
Sottoscrizioni dell'azione di estendibilità

È possibile assegnare un'azione di estendibilità a una sottoscrizione di Cloud Assembly per estendere il ciclo di vita dell'applicazione.

Nota Le seguenti sottoscrizioni sono esempi di casi d'uso e non prendono in esame tutte le funzionalità dell'azione di estendibilità.

Come integrare Cloud Assembly con ServiceNow utilizzando le azioni di estendibilità

Utilizzando le azioni di estendibilità è possibile integrare Cloud Assembly con una ITSM aziendale, come ServiceNow.

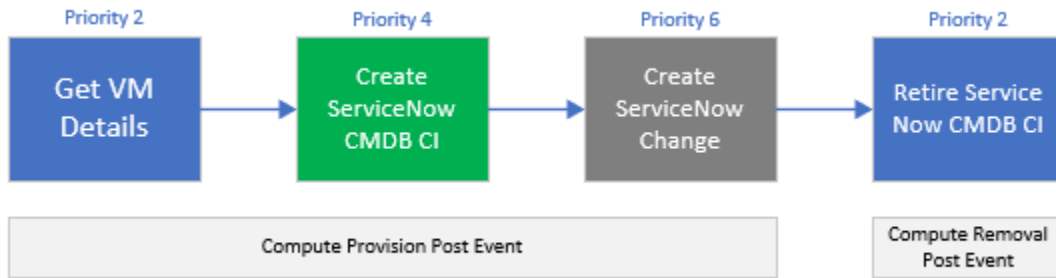


In genere gli utenti aziendali integrano la propria piattaforma di gestione del cloud con una piattaforma di gestione dei servizi IT (ITSM, IT Service Management) e un database di gestione della configurazione (CMDB, Configuration Management Database) a scopo di conformità. Seguendo questo esempio è possibile integrare Cloud Assembly con ServiceNow per CMDB e ITSM utilizzando gli script dell'azione di estendibilità.

Nota È inoltre possibile integrare ServiceNow con Cloud Assembly utilizzando i workflow di vRealize Orchestrator. Per informazioni sull'integrazione di ServiceNow tramite workflow, vedere [Come integrare Cloud Assembly per ITSM con ServiceNow utilizzando i workflow di vRealize Orchestrator](#).

Per creare questa integrazione, si utilizzano quattro script dell'azione di estendibilità. I primi tre script vengono avviati in sequenza durante il provisioning, nell'evento successivo al provisioning della risorsa di elaborazione. Il quarto script viene attivato nell'evento successivo alla rimozione della risorsa di elaborazione.

Per ulteriori informazioni sugli argomenti degli eventi, fare riferimento a [Argomenti degli eventi](#) forniti con Cloud Assembly.



Recupera dettagli della macchina virtuale

Lo script Recupera dettagli della macchina virtuale acquisisce ulteriori dettagli del payload, necessari per la creazione di CI e un token di identità archiviato in Amazon Web Services Systems Manager Parameter Store (SSM). Inoltre, questo script aggiorna `customProperties` con proprietà aggiuntive per un uso successivo.

Crea CI CMDB di ServiceNow

Lo script Crea CI CMDB di ServiceNow passa l'URL dell'istanza di ServiceNow come input e archivia l'istanza in SSM per soddisfare i requisiti di sicurezza. Questo script legge anche la risposta dell'identificatore univoco del record CMDB di ServiceNow (`sys_id`). Lo passa come output e scrive la proprietà personalizzata `serviceNowSysId` durante la creazione. Questo valore viene utilizzato per contrassegnare CI come ritirato quando l'istanza viene eliminata.

Nota È possibile che sia necessario allocare autorizzazioni aggiuntive al ruolo vRealize Automation services Amazon Web Services per consentire a Lambda di accedere a SSM Parameter Store.

Crea modifica ServiceNow

Questo script completa l'integrazione di ITSM passando l'URL dell'istanza di ServiceNow come input e archiviando le credenziali di ServiceNow come SSM per soddisfare i requisiti di sicurezza.

Crea modifica ServiceNow

Lo script Ritira CI CMDB di ServiceNow richiede l'interruzione di ServiceNow e contrassegna CI come ritirato in base alla proprietà personalizzata `serviceNowSysId` creata nello script di creazione.

Prerequisiti

- Prima di configurare questa integrazione, filtrare tutte le sottoscrizioni agli eventi con la proprietà condizionale del modello cloud: `event.data["customProperties"] ["enable_servicenow"] == "true"`

Nota Questa proprietà è presente nei modelli cloud che richiedono un'integrazione di ServiceNow.

- Scaricare e installare Python.

Per ulteriori informazioni su come filtrare le sottoscrizioni, vedere [Creazione di una sottoscrizione di estendibilità](#).

Procedura

- 1 Aprire un prompt della riga di comando dalla macchina virtuale.
- 2 Eseguire lo script Recupera dettagli della macchina virtuale.

```
from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    baseUrl = inputs['url']
    casToken = client.get_parameter(Name="casToken",WithDecryption=True)

    url = baseUrl + "/iaas/login"
    headers = {"Accept":"application/json","Content-Type":"application/json"}
    payload = {"refreshToken":casToken['Parameter']['Value']}

    results = requests.post(url,json=payload,headers=headers)

    bearer = "Bearer "
    bearer = bearer + results.json()["token"]

    deploymentId = inputs['deploymentId']
    resourceId = inputs['resourceIds'][0]

    print("deploymentId: " + deploymentId)
    print("resourceId:" + resourceId)

    machineUri = baseUrl + "/iaas/machines/" + resourceId
    headers = {"Accept":"application/json","Content-Type":"application/json",
    "Authorization":bearer }
    resultMachine = requests.get(machineUri,headers=headers)
    print("machine: " + resultMachine.text)

    print( "serviceNowCPUCount: " + json.loads(resultMachine.text)["customProperties"]
    ["cpuCount"] )
    print( "serviceNowMemoryInMB: " + json.loads(resultMachine.text)["customProperties"]
    ["memoryInMB"] )
```

```

#update customProperties
outputs = {}
outputs['customProperties'] = inputs['customProperties']
outputs['customProperties']['serviceNowCPUCount'] = int(json.loads(resultMachine.text)
["customProperties"]["cpuCount"])
outputs['customProperties']['serviceNowMemoryInMB'] = json.loads(resultMachine.text)
["customProperties"]["memoryInMB"]
return outputs

```

3 Eseguire l'azione di creazione dell'elemento di configurazione CMDB.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):

    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    table_name = "cmdb_ci_vmware_instance"
    url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'name': inputs['customProperties']['serviceNowHostname'],
        'cpus': int(inputs['customProperties']['serviceNowCPUCount']),
        'memory': inputs['customProperties']['serviceNowMemoryInMB'],
        'correlation_id': inputs['deploymentId'],
        'disks_size': int(inputs['customProperties']['provisionGB']),
        'location': "Sydney",
        'vcenter_uuid': inputs['customProperties']['vcUuid'],
        'state': 'On',
        'sys_created_by': inputs['__metadata']['userName'],
        'owned_by': inputs['__metadata']['userName']
    }
    results = requests.post(
        url,
        json=payload,
        headers=headers,
        auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
    )
    print(results.text)

    #parse response for the sys_id of CMDB CI reference
    if json.loads(results.text)['result']:
        serviceNowResponse = json.loads(results.text)['result']
        serviceNowSysId = serviceNowResponse['sys_id']
        print(serviceNowSysId)

    #update the serviceNowSysId customProperty

```

```

outputs = {}
outputs['customProperties'] = inputs['customProperties']
outputs['customProperties']['serviceNowSysId'] = serviceNowSysId;
return outputs

```

4 Eseguire lo script dell'azione di creazione.

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    table_name = "change_request"
    url = "https://" + inputs['instanceUrl'] + "/api/now/table/{0}".format(table_name)
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'short_description': 'Provision CAS VM Instance'
    }
    results = requests.post(
        url,
        json=payload,
        headers=headers,
        auth=(snowUser['Parameter']['Value'], snowPass['Parameter']['Value'])
    )
    print(results.text)

```

Risultati

Cloud Assembly è stato integrato correttamente con ITSM ServiceNow.

Operazioni successive

Quando desiderato, è possibile ritirare CI utilizzando l'azione di ritiro dell'elemento di configurazione CMDB:

```

from botocore.vendored import requests
import json
import boto3
client = boto3.client('ssm','ap-southeast-2')

def handler(context, inputs):
    snowUser = client.get_parameter(Name="serviceNowUserName",WithDecryption=False)
    snowPass = client.get_parameter(Name="serviceNowPassword",WithDecryption=True)
    tableName = "cmdb_ci_vmware_instance"
    sys_id = inputs['customProperties']['serviceNowSysId']
    url = "https://" + inputs['instanceUrl'] + "/api/now/" + tableName + "/" + sys_id
    headers = {'Content-type': 'application/json', 'Accept': 'application/json'}
    payload = {
        'state': 'Retired'
    }

```

```

results = requests.put(
    url,
    json=payload,
    headers=headers,
    auth=(inputs['username'], inputs['password'])
)
print(results.text)

```

Per ulteriori informazioni su come utilizzare le azioni di estendibilità per integrare ServiceNow in Cloud Assembly, vedere [Estensione di Cloud Assembly con l'estendibilità basata su azione per l'integrazione di ServiceNow](#).

Come assegnare un tag alle macchine virtuali durante il provisioning utilizzando le azioni di estendibilità

È possibile utilizzare le azioni di estendibilità in combinazione con le sottoscrizioni per automatizzare e semplificare l'assegnazione di tag alle macchine virtuali.

L'amministratore del cloud può creare distribuzioni che vengono contrassegnate automaticamente con input e output specificati utilizzando le azioni di estendibilità e le sottoscrizioni dell'estendibilità. Quando viene creata una nuova distribuzione correlata al progetto contenente il tag Sottoscrizione macchina virtuale, l'evento di distribuzione attiva l'esecuzione dello script **Assegna tag a macchina virtuale** e i tag vengono applicati automaticamente. Questa operazione consente di risparmiare tempo e promuove l'efficienza consentendo una gestione semplificata della distribuzione.

Prerequisiti

- Accedere alle credenziali dell'amministratore del cloud.
- Ruolo di Amazon Web Services per le funzioni Lambda.

Procedura

- 1 Passare a **Estendibilità > Libreria > Azioni > Nuova azione** e creare una nuova azione con i seguenti parametri.

Parametro	Descrizione
Nome azione	Nome dell'azione di estendibilità, preferibilmente con TagVM come prefisso o suffisso.
Progetto	Progetto in cui testare l'azione di estendibilità.
Modello di azione	Assegna tag a macchina virtuale
Runtime	Python
Origine script	Scrivi script

- 2 Immettere **Handler** come **Funzione principale**.

- 3 Aggiungere input di tag per testare l'azione di estendibilità.

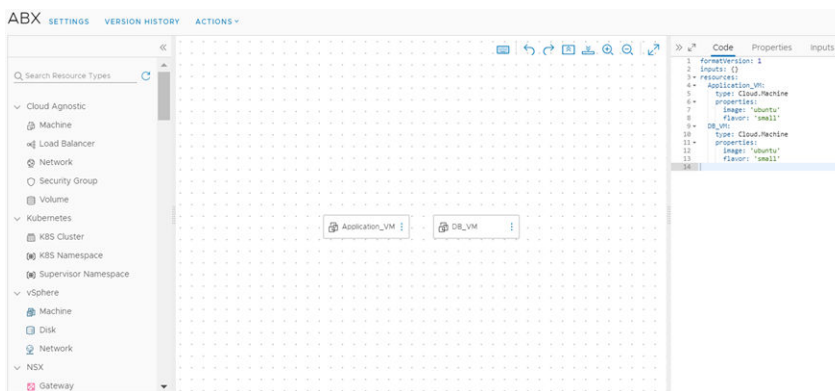
Ad esempio, `resourceNames = ["DB_VM"]` e `target = world`.

- 4 Per salvare l'azione, fare clic su **Salva**.
- 5 Per testare l'azione, fare clic su **Prova**.
- 6 Per uscire dall'editor delle azioni, fare clic su **Chiudi**.
- 7 Passare a **Estendibilità > Sottoscrizioni**.
- 8 Fare clic su **Nuova sottoscrizione**.
- 9 Immettere i seguenti dettagli della sottoscrizione.

Dettaglio	Impostazione
Argomento dell'evento	Selezionare un argomento dell'evento correlato alla fase di assegnazione dei tag della macchina virtuale. Ad esempio, Allocations resource elaboration.
Blocco	Impostare il timeout per la sottoscrizione su 1 minuto.
Azione/Workflow	Selezionare un tipo di azione di estendibilità eseguibile e selezionare l'azione di estendibilità personalizzata.

Nota I tag devono far parte dei parametri di evento dell'argomento dell'evento selezionato.

- 10 Per salvare la sottoscrizione dell'azione di estendibilità personalizzata, fare clic su **Salva**.
- 11 Passare a **Progettazione > Modelli cloud** e creare un modello cloud da una tela vuota.
- 12 Aggiungere due macchine virtuali al modello cloud: `Application_VM` e `DB_VM`.



- 13 Per distribuire le macchine virtuali, fare clic su **Distribuisci**.
- 14 Durante la distribuzione, verificare che l'evento venga avviato e che l'azione di estendibilità venga eseguita.
- 15 Per verificare che i tag siano stati applicati correttamente, andare in **Risorse > Risorse > Macchine virtuali**.

Come configurare il nome di un controller dell'interfaccia di rete utilizzando le azioni di estendibilità

È possibile configurare il nome dell'interfaccia di un controller dell'interfaccia di rete (NIC) utilizzando le chiamate API IaaS applicate tramite le azioni di estendibilità.

Per configurare il nome dell'interfaccia di una scheda NIC, è necessario effettuare chiamate `GET` e `PATCH` all'API IaaS di vRealize Automation. Eseguendo una chiamata `GET` a `https://your_vRA_fqdn/iaas/api/machines/{id}`, è possibile recuperare il collegamento della scheda NIC per la risorsa di elaborazione che si desidera modificare. È quindi possibile effettuare una chiamata `PATCH` a `https://your_vRA_fqdn/iaas/api/machines/{id}/network-interfaces/{nicId}`, che include il nome dell'interfaccia NIC come payload, per aggiungere il nuovo nome per la scheda NIC.

Lo scenario seguente utilizza uno script Python di esempio che può essere utilizzato per la configurazione del nome dell'interfaccia NIC. Per i propri casi d'uso, è possibile utilizzare uno script e un linguaggio di script diversi, ad esempio Node.js.

Prerequisiti

- È possibile configurare solo il nome dell'interfaccia NIC prima di eseguire il provisioning di una risorsa di elaborazione. Pertanto, è possibile selezionare solo l'argomento dell'evento **Provisioning risorsa di elaborazione** per le sottoscrizioni di estendibilità pertinenti.
- È possibile configurare solo i nomi dell'interfaccia NIC per le schede NIC che utilizzano Microsoft Azure come provider.

Procedura

- 1 Creare l'azione di estendibilità.
 - a Passare a **Estendibilità > Azioni**.
 - b Fare clic su **Nuova Azione**.
 - c Immettere un nome e un progetto per l'azione di estendibilità e fare clic su **Avanti**.

- d Aggiungere lo script di configurazione NIC.

Di seguito è disponibile uno script Python di esempio:

```
import json

def handler(context, inputs):

    # Get the machine info, which contains machine nic link
    response = context.request('/iaas/api/machines/'+inputs["resourceIds"][0], "GET",
    {})

    # Build PATCH machine nic payload here
    name = "customized-nic-02";
    data = {'name':name};

    # Convert machine data string to json object
    response_json = json.loads(response["content"])

    # Patch machine nic
    response_patch = context.request(response_json["_links"]["network-interfaces"]
    ["hrefs"][0] + "?apiVersion=2021-07-15", 'PATCH', data)

    # return value is empty since we are not changing any compute provisioning
    parameters
    outputs = {}
    return outputs
```

Lo script di esempio precedente esegue due operazioni primarie tramite l'API IaaS. Innanzitutto, lo script utilizza una chiamata `GET` per recuperare il collegamento alla scheda NIC e quindi utilizza una chiamata `PATCH` per applicare il nome dell'interfaccia. In questo esempio, il nome dell'interfaccia NIC è hardcoded nello script come "customized-nic-02".

- e Per completare la modifica dell'azione di estendibilità, fare clic su **Salva**.

2 Creare una sottoscrizione di estendibilità.

- a Passare a **Estendibilità > Sottoscrizioni**.
- b Fare clic su **Nuova sottoscrizione**.
- c Immettere un nome per la sottoscrizione di estendibilità.
- d In **Argomento dell'evento**, selezionare **Provisioning risorsa di elaborazione** come argomento dell'evento per la sottoscrizione di estendibilità.
- e In **Azione/Workflow**, selezionare l'azione di estendibilità creata per la configurazione della scheda NIC.
- f Abilitare il blocco degli eventi.

Abilitando il blocco, si verifica che il processo di provisioning sia bloccato finché l'azione di estendibilità non termina la sua esecuzione.

- g Per completare la modifica della sottoscrizione di estendibilità, fare clic su **Salva**.

Risultati

La nuova sottoscrizione di estendibilità viene eseguita quando viene attivato un evento di provisioning della risorsa di elaborazione e configura il nome dell'interfaccia NIC per le risorse di elaborazione da sottoporre a provisioning.

Ulteriori informazioni sulle azioni di estendibilità

L'estendibilità basata su azioni utilizza script di codice semplificati all'interno di Cloud Assembly per automatizzare le azioni di estendibilità.

L'estendibilità basata su azioni offre un'interfaccia del motore di runtime leggera e flessibile in cui è possibile definire piccole azioni di script e configurarle per l'avvio quando si verificano determinati eventi specificati nelle sottoscrizioni di estendibilità.

È possibile creare questi script di codice dell'azione di estendibilità all'interno di Cloud Assembly o nell'ambiente locale e assegnarli alle sottoscrizioni. Gli script dell'azione di estendibilità vengono utilizzati per semplificare e alleggerire l'automazione di attività e passaggi. Per ulteriori informazioni sull'integrazione di Cloud Assembly con un server di vRealize Orchestrator, vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).

L'estendibilità basata su azioni offre:

- Un'alternativa ai workflow di vRealize Orchestrator, con azioni di script piccole e riutilizzabili, per integrazioni e personalizzazioni leggere.
- Un modo per riutilizzare i modelli di azione, che contengono azioni parametrizzate riutilizzabili.

È possibile creare azioni di estendibilità scrivendo un codice di script di azione definito dall'utente o importando un codice di script predefinito come pacchetto ZIP. L'estendibilità basata su azioni supporta gli ambienti di runtime Node.js, Python e PowerShell. I runtime Node.js e Python si basano su Amazon Web Services Lambda. Pertanto, è necessario disporre di una sottoscrizione attiva con Amazon Web Services Identity and Access Management (IAM) e configurare Amazon Web Services come endpoint in Cloud Assembly. Per informazioni su come iniziare con Amazon Web Services Lambda, vedere [ABX: estendibilità senza server dei servizi di Cloud Assembly](#).

Nota Le azioni di estendibilità sono specifiche del progetto.

Come creare le azioni di estendibilità

Con Cloud Assembly, è possibile creare azioni di estendibilità per l'utilizzo nelle sottoscrizioni di estendibilità.

Le azioni di estendibilità sono metodi estremamente personalizzabili, leggeri e flessibili per estendere i cicli di vita delle applicazioni utilizzando codice di script e modelli di azione definiti dall'utente. I modelli di azione contengono parametri predefiniti che consentono di configurare le basi dell'azione di estendibilità.

Esistono due metodi per creare un'azione di estendibilità:

- Scrivere un codice definito dall'utente per uno script di azione di estendibilità.

Nota La compilazione del codice definito dall'utente nell'editor delle azioni di estendibilità potrebbe richiedere una connessione Internet attiva.

- L'importazione di un pacchetto di distribuzione come pacchetto ZIP per un'azione di estendibilità. Per informazioni sulla creazione di un pacchetto ZIP per le azioni di estendibilità, vedere [Creazione di un pacchetto ZIP per le azioni di estendibilità del runtime di Python](#), [Creazione di un pacchetto ZIP per le azioni di estendibilità del runtime di Node.js](#) o [Creazione di un pacchetto ZIP per le azioni di estendibilità del runtime di PowerShell](#).

I passaggi seguenti descrivono la procedura per la creazione di un'azione di estendibilità che utilizza Amazon Web Services come provider FaaS.

Prerequisiti

- Appartenenza a un progetto attivo e valido.
- Ruolo di Amazon Web Services configurato per le funzioni Lambda. Ad esempio `AWSLambdaBasicExecutionRole`.
- Ruolo di amministratore del cloud o autorizzazioni `iam:PassRole` abilitate.

Procedura

- 1 Selezionare **Estendibilità > Libreria > Azioni**.
- 2 Fare clic su **Nuova Azione**.
- 3 Immettere un nome per l'azione e selezionare un progetto.
- 4 (Facoltativo) Aggiungere una descrizione per l'azione.
- 5 Fare clic su **Avanti**.
- 6 Cercare e selezionare un modello di azione.

Nota Per creare un'azione personalizzata senza utilizzare un modello di azione, selezionare **Script personalizzato**.

Verranno visualizzati nuovi parametri configurabili.

- 7 Selezionare **Scrivi script** o **Importa pacchetto**.
- 8 Selezionare il runtime dell'azione.
- 9 Immettere un nome in **Funzione principale** per il punto di ingresso dell'azione.

Nota Per le azioni importate da un pacchetto ZIP, la funzione principale deve includere anche il nome del file di script che contiene il punto di ingresso. Ad esempio, se il file di script principale è denominato `main.py` e il punto di ingresso è `handler (context, inputs)`, il nome della funzione principale deve essere `main.handler`.

- 10 Definire i parametri di input e output dell'azione.
- 11 (Facoltativo) Aggiungere i segreti o le costanti dell'azione di estendibilità agli input predefiniti.

Nota Per ulteriori informazioni sui segreti e sulle costanti dell'azione di estendibilità, vedere [Come creare segreti da utilizzare nelle azioni di estendibilità](#) e [Come creare costanti dell'azione di estendibilità](#).

- 12 (Facoltativo) Aggiungere le dipendenze delle applicazioni all'azione.

Nota Per gli script di PowerShell, è possibile definire le dipendenze delle applicazioni in modo che vengano risolte nel repository del repository PowerShell Gallery. Per definire le dipendenze delle applicazioni in modo che siano risolvibili dal repository pubblico, utilizzare il formato seguente:

```
@{
    Name = 'Version'
}

e.g.

@{
    Pester = '4.3.1'
}
```

Nota Per le azioni importate da un pacchetto ZIP, le dipendenze delle applicazioni vengono aggiunte automaticamente.

- 13 Per definire i limiti di timeout e memoria, attivare l'opzione **Imposta timeout e limiti personalizzati**.
- 14 Per eseguire il test dell'azione, fare clic su **Salva** e quindi su **Test**.

Operazioni successive

Dopo aver creato e verificato l'azione di estendibilità, è possibile assegnarla a una sottoscrizione.

Nota Le sottoscrizioni di estendibilità utilizzano l'ultima versione rilasciata di un'azione di estendibilità. Dopo aver creato una nuova versione di un'azione, fare clic su **Versioni** nella parte superiore destra nella finestra dell'editor. Per rilasciare la versione dell'azione che si desidera utilizzare nella sottoscrizione, fare clic su **Rilascia**.

Creazione di un pacchetto ZIP per le azioni di estendibilità del runtime di Python

È possibile creare un pacchetto ZIP contenente lo script e le dipendenze di Python utilizzati dalle azioni di estendibilità di Cloud Assembly.

Sono disponibili due metodi per creare lo script per le azioni di estendibilità:

- Compilazione dello script direttamente nell'editor delle azioni di estendibilità in Cloud Assembly.

- Creazione dello script nell'ambiente locale e aggiunta di tale script, con eventuali dipendenze pertinenti, a un pacchetto ZIP.

Utilizzando un pacchetto ZIP, è possibile creare un modello personalizzato preconfigurato di script di azione e dipendenze che è possibile importare in Cloud Assembly per l'utilizzo nelle azioni di estendibilità.

È inoltre possibile utilizzare un pacchetto ZIP in scenari in cui i moduli associati alle dipendenze nello script di azione non possono essere risolti dal servizio Cloud Assembly, ad esempio quando l'ambiente non dispone di accesso a Internet.

È inoltre possibile utilizzare un pacchetto ZIP per creare azioni di estendibilità che contengano più file di script di Python. L'utilizzo di più file di script può essere utile per organizzare la struttura del codice dell'azione di estendibilità.

Prerequisiti

Se si utilizza Python 3.3 o versioni precedenti, scaricare e configurare il programma di installazione del pacchetto PIP. Vedere [Indice del pacchetto Python](#).

Procedura

- 1 Nella macchina locale, creare una cartella per lo script di azione e le dipendenze.
Ad esempio, `/home/user1/zip-action`.
- 2 Aggiungere lo script o gli script di azione di Python principali alla cartella.
Ad esempio, `/home/user1/zip-action/main.py`.
- 3 (Facoltativo) Aggiungere tutte le dipendenze per lo script di Python alla cartella.
 - a Creare un file `requirements.txt` contenente le dipendenze. Vedere [File dei requisiti](#).
 - b Aprire una shell Linux.

Nota Il runtime dell'estendibilità basata su azioni in Cloud Assembly è basato su Linux. Pertanto, tutte le dipendenze di Python compilate in un ambiente Windows potrebbero rendere i pacchetti ZIP generati inutilizzabili per la creazione di azioni di estendibilità. Pertanto, è necessario utilizzare una shell Linux.

- c Installare il file `requirements.txt` nella cartella dello script eseguendo il comando seguente:

```
pip install -r requirements.txt --target=home/user1/zip-action
```

- 4 Nella cartella assegnata, selezionare gli elementi dello script e, se applicabile, il file `requirements.txt` e comprimerli in un pacchetto ZIP.

Nota Gli elementi dello script e delle dipendenze devono essere archiviati al livello root del pacchetto ZIP. Quando si crea il pacchetto ZIP in un ambiente Linux, è possibile che si verifichi un problema perché il contenuto del pacchetto non viene archiviato al livello root. Se si verifica questo problema, creare il pacchetto eseguendo il comando `zip -r` nella shell della riga di comando.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Operazioni successive

Utilizzare il pacchetto ZIP per creare uno script di azione di estendibilità. Vedere [Come creare le azioni di estendibilità](#).

Creazione di un pacchetto ZIP per le azioni di estendibilità del runtime di Node.js

È possibile creare un pacchetto ZIP contenente lo script e le dipendenze di Node.js utilizzati dalle azioni di estendibilità di Cloud Assembly.

Sono disponibili due metodi per creare lo script per le azioni di estendibilità:

- Compilazione dello script direttamente nell'editor delle azioni di estendibilità in Cloud Assembly.
- Creazione dello script nell'ambiente locale e aggiunta di tale script, con eventuali dipendenze pertinenti, a un pacchetto ZIP.

Utilizzando un pacchetto ZIP, è possibile creare un modello personalizzato preconfigurato di script di azione e dipendenze che è possibile importare in Cloud Assembly per l'utilizzo nelle azioni di estendibilità.

È inoltre possibile utilizzare un pacchetto ZIP in scenari in cui i moduli associati alle dipendenze nello script di azione non possono essere risolti dal servizio Cloud Assembly, ad esempio quando l'ambiente non dispone di accesso a Internet.

È inoltre possibile utilizzare i pacchetti per creare azioni di estendibilità con più file di script di Node.js. L'utilizzo di più file di script può essere utile per organizzare la struttura del codice dell'azione di estendibilità.

Procedura

- 1 Nella macchina locale, creare una cartella per lo script di azione e le dipendenze.
Ad esempio, `/home/user1/zip-action`.
- 2 Aggiungere lo script o gli script di azione di Node.js principali alla cartella.
Ad esempio, `/home/user1/zip-action/main.js`.

3 (Facoltativo) Aggiungere tutte le dipendenze per lo script di Node.js alla cartella.

- a Creare un file `package.json` con le dipendenze nella cartella dello script. Vedere [Creazione di un file package.json](#) e [Come specificare dipendenze e devDependencies in un file package.json](#).
- b Aprire una shell della riga di comando.
- c Passare alla cartella creata per lo script di azione e le dipendenze.

```
cd /home/user1/zip-action
```

- d Installare il file `package.json` nella cartella dello script eseguendo il comando seguente:

```
npm install --production
```

Nota Questo comando crea una directory `node_modules` nella cartella.

- 4** Nella cartella assegnata, selezionare gli elementi dello script e, se applicabile, la directory `node_modules` e comprimerli in un pacchetto ZIP.

Nota Gli elementi dello script e delle dipendenze devono essere archiviati al livello root del pacchetto ZIP. Quando si crea il pacchetto ZIP in un ambiente Linux, è possibile che si verifichi un problema perché il contenuto del pacchetto non viene archiviato al livello root. Se si verifica questo problema, creare il pacchetto eseguendo il comando `zip -r` nella shell della riga di comando.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Operazioni successive

Utilizzare il pacchetto ZIP per creare uno script di azione di estendibilità. Vedere [Come creare le azioni di estendibilità](#).

Creazione di un pacchetto ZIP per le azioni di estendibilità del runtime di PowerShell

È possibile creare un pacchetto ZIP contenente i moduli di dipendenze e lo script di PowerShell da utilizzare nelle azioni di estendibilità.

Sono disponibili due metodi per creare lo script per le azioni di estendibilità:

- Compilazione dello script direttamente nell'editor delle azioni di estendibilità in Cloud Assembly.
- Creazione dello script nell'ambiente locale e aggiunta di tale script, con eventuali dipendenze pertinenti, a un pacchetto ZIP.

Utilizzando un pacchetto ZIP, è possibile creare un modello personalizzato preconfigurato di script di azione e dipendenze che è possibile importare in Cloud Assembly per l'utilizzo nelle azioni di estendibilità.

Nota Non è necessario definire i cmdlet di PowerCLI come dipendenze o aggregarli in un pacchetto ZIP. I cmdlet di PowerCLI vengono preconfigurati con il runtime PowerShell del servizio Cloud Assembly.

È inoltre possibile utilizzare un pacchetto ZIP in scenari in cui i moduli associati alle dipendenze nello script di azione non possono essere risolti dal servizio Cloud Assembly, ad esempio quando l'ambiente non dispone di accesso a Internet.

È inoltre possibile utilizzare un pacchetto ZIP per creare azioni di estendibilità che contengano più file di script di PowerShell. L'utilizzo di più file di script può essere utile per organizzare la struttura del codice dell'azione di estendibilità.

Prerequisiti

Assicurarsi di conoscere PowerShell e PowerCLI. È possibile trovare un'immagine Docker con PowerShell Core, PowerCLI 10, PowerNSX e diversi esempi di script e moduli della community in [Docker Hub](#).

Procedura

- 1 Nella macchina locale, creare una cartella per lo script di azione e le dipendenze.

Ad esempio, `/home/user1/zip-action`.

- 2 Aggiungere lo script PowerShell principale con estensione `.psm1` alla cartella.

Lo script seguente include una semplice funzione PowerShell denominata `main.psm1`:

```
function handler($context, $payload) {  
  
    Write-Host "Hello " $payload.target  
  
    return $payload  
}
```

Nota L'output di un'azione di estendibilità di PowerShell si basa sull'ultima variabile visualizzata nel corpo della funzione. Tutte le altre variabili nella funzione inclusa vengono eliminate.

- 3 (Facoltativo) Aggiungere una configurazione proxy allo script PowerShell principale utilizzando parametri `context`. Vedere [Utilizzo dei parametri context per aggiungere una configurazione proxy nello script di PowerShell](#).

4 (Facoltativo) Aggiungere le eventuali dipendenze dello script di PowerShell.

Nota Lo script delle dipendenze di PowerShell deve utilizzare l'estensione `.psm1`. Utilizzare lo stesso nome per lo script e la sottocartella in cui lo script viene salvato.

- a Accedere a una shell PowerShell di Linux.

Nota Il runtime dell'estendibilità basata su azioni in Cloud Assembly è basato su Linux. Tutte le dipendenze di PowerShell compilate in un ambiente Windows potrebbero rendere inutilizzabile il pacchetto ZIP generato. Qualsiasi dipendenza di terze parti installata deve essere compatibile con VMware Photon OS come script di PowerShell eseguiti in Photon OS.

- b Passare alla cartella `/home/user1/zip-action`.
- c Scaricare e salvare il modulo di PowerShell contenente le dipendenze eseguendo il cmdlet `Save-Module`.

```
Save-Module -Name <module name> -Path ./
```

- d Ripetere il passaggio secondario precedente per tutti i moduli di dipendenze aggiuntivi.

Importante Verificare che ogni modulo di dipendenze si trovi in una sottocartella separata. Per ulteriori informazioni sulla compilazione e la gestione dei moduli di PowerShell, vedere [Come compilare un modulo di script di PowerShell](#).

5 Nella cartella assegnata, selezionare gli elementi dello script e, se applicabile, le sottocartelle del modulo di dipendenze e compprimerle in un pacchetto ZIP.

Nota Le sottocartelle dello script e del modulo di dipendenze devono essere archiviate al livello root del pacchetto ZIP. Quando si crea il pacchetto ZIP in un ambiente Linux, è possibile che si verifichi un problema perché il contenuto del pacchetto non viene archiviato al livello root. Se si verifica questo problema, creare il pacchetto eseguendo il comando `zip -r` nella shell della riga di comando.

```
cd your_script_and_dependencies_folder
zip -r ../your_action_ZIP.zip *
```

Operazioni successive

Utilizzare il pacchetto ZIP per creare uno script di azione di estendibilità. Vedere [Come creare le azioni di estendibilità](#).

Utilizzo dei parametri context per aggiungere una configurazione proxy nello script di PowerShell. È possibile abilitare la comunicazione del proxy di rete nello script di PowerShell utilizzando i parametri `context`.

Alcuni cmdlet di PowerShell potrebbero richiedere l'impostazione di un proxy di rete come variabile di ambiente nella funzione PowerShell. Le configurazioni di proxy vengono fornite alla funzione PowerShell con i parametri `$context.proxy.host` e `$context.proxy.port`.

È possibile aggiungere questi parametri `context` all'inizio dello script di PowerShell.

```
$proxyString = "http://" + $context.proxy.host + ":" + $context.proxy.port
$Env:HTTP_PROXY = $proxyString
$Env:HTTPS_PROXY = $proxyString
```

Se i cmdlet supportano il parametro `-Proxy`, è possibile anche passare il valore del proxy direttamente ai cmdlet PowerShell specifici.

Configurazione delle azioni di estendibilità specifiche del cloud

È possibile configurare le azioni di estendibilità da utilizzare con gli account cloud.

Quando si crea un'azione di estendibilità, è possibile configurarla e collegarla a vari account basati su cloud:

- Microsoft Azure
- Amazon Web Services

Prerequisiti

È necessario un account cloud valido.

Procedura

- 1 Selezionare **Estendibilità > Libreria > Azione**.
- 2 Fare clic su **Nuova Azione**.
- 3 Immettere i parametri dell'azione necessari.
- 4 Nel menu a discesa **Provider FaaS**, selezionare il provider dell'account cloud o selezionare **Selezione automatica**.

Nota Se si seleziona **Automatico**, l'azione definisce automaticamente il provider FaaS.

- 5 Fare clic su **Salva**.

Risultati

L'azione di estendibilità è collegata per l'utilizzo con l'account cloud configurato.

Configurazione delle azioni di estendibilità locali

È possibile configurare le azioni di estendibilità in modo che utilizzino un provider FaaS locale anziché un account cloud di Amazon Web Services o Microsoft Azure.

Utilizzando un provider FaaS locale per le azioni di estendibilità, è possibile utilizzare servizi locali come LDAP, CMDB o data center di vCenter nelle sottoscrizioni di estendibilità di Cloud Assembly.

Procedura

- 1 Selezionare **Estendibilità > Libreria > Azioni**.

- 2 Fare clic su **Nuova Azione**.
- 3 Immettere un nome e un progetto per l'azione di estendibilità.
- 4 (Facoltativo) Immettere una descrizione per l'azione di estendibilità.
- 5 Fare clic su **Avanti**.
- 6 Creare o importare lo script dell'azione di estendibilità.
- 7 Fare clic sul menu a discesa **Provider FaaS** e selezionare **Locale**.
- 8 Per salvare la nuova azione di estendibilità, fare clic su **Salva**.

Operazioni successive

Utilizzare l'azione di estendibilità creata nelle sottoscrizioni di estendibilità di Cloud Assembly.

Come creare segreti da utilizzare nelle azioni di estendibilità

È possibile aggiungere input crittografati all'azione di estendibilità utilizzando i segreti a livello di progetto.

Con i segreti, è possibile aggiungere valori di input crittografati alle azioni di estendibilità. La crittografia è utile per casi d'uso in cui gli input vengono utilizzati per gestire dati sensibili, ad esempio password e certificati. I segreti sono disponibili per tutti i provider e i runtime FaaS.

Nota È inoltre possibile aggiungere valori di input crittografati utilizzando le costanti di azione. Vedere [Come creare costanti dell'azione di estendibilità](#).

L'accesso ai segreti dipende dal progetto in cui sono creati. I segreti creati nel progetto A, ad esempio, sono accessibili solo agli utenti inclusi nel progetto A.

I segreti utilizzano la funzione `context.getSecret()` per decrittografare il valore segreto quando viene aggiunto allo script. Questa funzione utilizza il nome del segreto come parametro. Ad esempio, è possibile utilizzare un segreto denominato `abxsecret` come parametro di input crittografato nell'azione. Per aggiungere questo parametro di input allo script di azione, è necessario utilizzare `context.getSecret(inputs["abxsecret"])`.

Procedura

- 1 Creare un nuovo segreto.
 - a Selezionare **Infrastruttura > Amministrazione > Segreti**.
 - b Selezionare **Nuovo segreto**.
 - c Immettere il nome del progetto a cui è assegnato il segreto.

Nota L'azione di estendibilità a cui si desidera assegnare il segreto deve far parte dello stesso progetto del segreto.

- d Assegnare un nome al segreto.
- e Immettere il valore che si desidera assegnare al segreto.

f (Facoltativo) Immettere una descrizione.

g Fare clic su **Crea**.

2 Aggiungere il segreto a un'azione di estendibilità.

a Selezionare un'azione di estendibilità esistente o crearne una nuova.

b In **Input predefiniti**, selezionare la casella di controllo **Segreto**.

c Cercare il segreto e aggiungerlo agli input dell'azione di estendibilità.

d Aggiungere il segreto allo script dell'azione di estendibilità utilizzando la funzione `context.getSecret()`.

e Per testare il segreto, fare clic su **Test**.

Come creare costanti dell'azione di estendibilità

È possibile creare e archiviare costanti da utilizzare nelle azioni di estendibilità.

Con le costanti dell'azione di estendibilità, è possibile aggiungere valori di input crittografati alle azioni di estendibilità. La crittografia è utile per casi d'uso in cui gli input vengono utilizzati per gestire dati sensibili, ad esempio password e certificati. Le costanti sono disponibili per tutti i provider e i runtime FaaS.

Nota A differenza dei segreti, le costanti dell'azione di estendibilità possono essere utilizzate solo per i segreti di estendibilità. Per ulteriori informazioni sulle costanti, vedere [Come creare segreti da utilizzare nelle azioni di estendibilità](#)

Le costanti dell'azione di estendibilità sono accessibili a tutti gli utenti inclusi nell'organizzazione.

Le costanti utilizzano la funzione `context.getSecret()` per essere eseguite come parte dello script. Questa funzione utilizza il nome della costante come parametro. Ad esempio, è possibile utilizzare una costante dell'azione di estendibilità denominata `abxconstant` come parametro di input crittografato nell'azione. Per aggiungere questo parametro di input allo script di azione, è necessario utilizzare `context.getSecret(inputs["abxconstant"])`.

Procedura

1 Creare una costante dell'azione di estendibilità.

a Passare a **Estendibilità > Libreria > Azioni**.

b Selezionare **Costanti azione**.

c Per creare una costante, fare clic **Nuova costante azione**.

d Immettere un nome e un valore per la costante, quindi fare clic su **Salva**.

2 Aggiungere la costante a un'azione di estendibilità.

a Selezionare un'azione di estendibilità esistente o crearne una nuova.

b In **Input predefiniti**, selezionare la casella di controllo **Segreto**.

- c Cercare la costante e aggiungerla agli input dell'azione di estendibilità.
- d Aggiungere la costante allo script dell'azione di estendibilità utilizzando la funzione `context.getSecret()`.
- e Per testare la costante dell'azione di estendibilità, fare clic su **Test**.

Creazione di azioni di estendibilità condivise

Un amministratore di Cloud Assembly può creare azioni di estendibilità che possono essere condivise tra i progetti senza esportare e importare l'azione.

Per informazioni sull'esportazione e l'importazione di azioni di estendibilità, vedere [Esportazione e importazione delle azioni di estendibilità](#).

Prerequisiti

Creare due o più progetti nell'organizzazione Cloud Assembly.

Procedura

- 1 Selezionare **Estendibilità > Libreria > Azioni**.
- 2 Fare clic su **Nuova Azione**.
- 3 Immettere il nome dell'azione di estendibilità.
- 4 (Facoltativo) Immettere la descrizione per l'azione di estendibilità.
- 5 Selezionare il progetto in cui viene creata l'azione di estendibilità.
- 6 Selezionare la casella di controllo **Condividi con tutti i progetti in questa organizzazione**.
- 7 Fare clic su **Avanti**.
- 8 Creare o importare lo script dell'azione e salvare l'azione di estendibilità.

Nota È possibile abilitare o disabilitare la condivisione da **Impostazioni**. Se l'azione di estendibilità viene utilizzata nelle sottoscrizioni, non è possibile disabilitare la condivisione. Per disabilitare la condivisione, è necessario rimuovere l'azione di estendibilità dalle sottoscrizioni.

- 9 Creare una sottoscrizione di estendibilità, aggiungere l'azione di estendibilità condivisa e impostare l'ambito della sottoscrizione su **Qualsiasi progetto**.

Nota Per ulteriori informazioni sulla creazione di sottoscrizioni di estendibilità, vedere [Creazione di una sottoscrizione di estendibilità](#).

La sottoscrizione di estendibilità viene attivata da eventi corrispondenti in tutti i progetti.

Operazioni successive

È inoltre possibile importare azioni di estendibilità condivise come origine contenuto nel catalogo di Service Broker. Quando si seleziona il progetto di origine, specificare il progetto in cui è stata creata l'azione di estendibilità. Per ulteriori informazioni sull'aggiunta di azioni di estendibilità a Service Broker, vedere l'argomento [sull'aggiunta di azioni di estendibilità al catalogo di Service Broker](#).

Registrazione di Azure per le azioni di estendibilità basate su Python

È ora possibile utilizzare le funzioni di registrazione di Microsoft Azure 3.x nello script dell'azione di estendibilità.

Le azioni di estendibilità in Cloud Assembly ora utilizzano l'API di scripting di Microsoft Azure 3.x che sostituisce la versione 1.x precedente. L'API di scripting di Microsoft Azure 3.x è basata su Linux e viene eseguita in un ambiente contenitore.

A causa di questa modifica della versione, le funzioni di registrazione inserite nello script delle azioni di estendibilità che utilizzano Microsoft Azure come provider FaaS (Function as a Service) funzionano in modo diverso. I due esempi di script seguenti dimostrano le diverse funzioni di registrazione utilizzate nelle due versioni dell'API.

Esempio di script di Microsoft Azure 1.x.

```
def handler(context, inputs):
    greeting = "Hello, {0}!".format(inputs["target"])
    print(greeting)

    outputs = {
        "greeting": greeting
    }

    return outputs
```

Esempio di script di Microsoft Azure 3.x.

```
import logging

def handler(context, inputs):
    greeting = "Hello, {0}!".format(inputs["target"])
    logging.info(greeting)

    outputs = {
        "greeting": greeting
    }

    return outputs
```

L'esempio precedente mostra che la versione 3.x aggiunge la funzione `import logging` all'inizio dello script, sostituendo la funzione `print()` con la funzione `logging.info()`. Per continuare a utilizzare la registrazione con le azioni di estendibilità create nell'API di Microsoft Azure 1.x, è necessario modificare le funzioni di registrazione nello script in modo che corrisponda all'esempio di Microsoft Azure 3.x.

Per ulteriori informazioni sulla registrazione, vedere la [guida per gli sviluppatori Python delle funzioni di Azure](#).

Esportazione e importazione delle azioni di estendibilità

Con Cloud Assembly, è possibile esportare e importare azioni di estendibilità da utilizzare in progetti diversi.

Prerequisiti

Un'azione di estendibilità esistente.

Procedura

1 Esportare un'azione di estendibilità.

- a Passare a **Estendibilità > Libreria > Azioni**.
- b Selezionare un'azione di estendibilità e fare clic su **Esporta**.

Lo script di azione e le relative dipendenze vengono salvati nell'ambiente locale come file ZIP.

2 Importare un'azione di estendibilità.

- a Passare a **Estendibilità > Libreria > Azioni**.
- b Fare clic su **Importa**.
- c Selezionare l'azione di estendibilità esportata e assegnarla a un progetto.
- d Fare clic su **Importa**.

Nota Se l'azione di estendibilità importata è già stata assegnata al progetto specificato, viene richiesto di selezionare un criterio di risoluzione dei conflitti.

Che cos'è un flusso di azione

I flussi di azione sono un insieme di script di azioni di estendibilità utilizzati per estendere ulteriormente i cicli di vita e l'automazione.

Tutti i flussi di azione iniziano con `flow_start` e terminano con `flow_end`. È possibile collegare diversi script di azione di estendibilità insieme, utilizzando i seguenti elementi di flusso di azione:

- **Flussi di azione sequenziali** - Più script di azione di estendibilità eseguiti in sequenza.
- **Flussi di azione Fork** - Più script o flussi di azione di estendibilità che si suddividono i percorsi per contribuire allo stesso output.

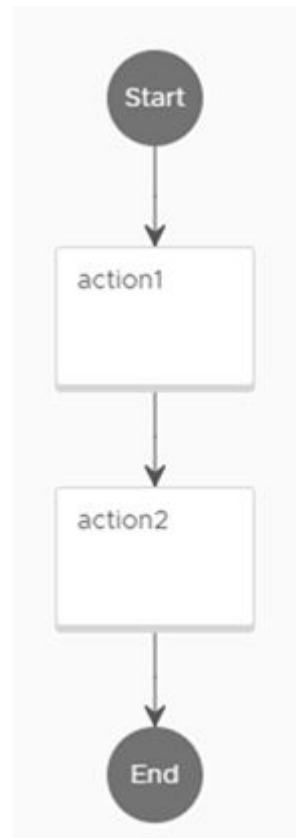
- **Flussi di azione Join** - Più script o flussi di azione di estendibilità che si uniscono e contribuiscono allo stesso output.
- **Flussi di azione condizionali** - Più script o flussi di azione di estendibilità che vengono eseguiti una volta soddisfatta una condizione.

Flussi di azione sequenziali

Più script di azione di estendibilità eseguiti in sequenza.

```
version: "1"
flow:
  flow_start:
    next: action1
  action1:
    action: <action_name>
    next: action2
  action2:
    action: <action_name>
    next: flow_end
```

Nota È possibile tornare a un'azione precedente assegnando l'azione come `next:`. In questo esempio, anziché `next: flow_end`, è possibile immettere `next: action1` per eseguire nuovamente l'azione 1 e riavviare la sequenza di azioni.



Flussi di azione Fork

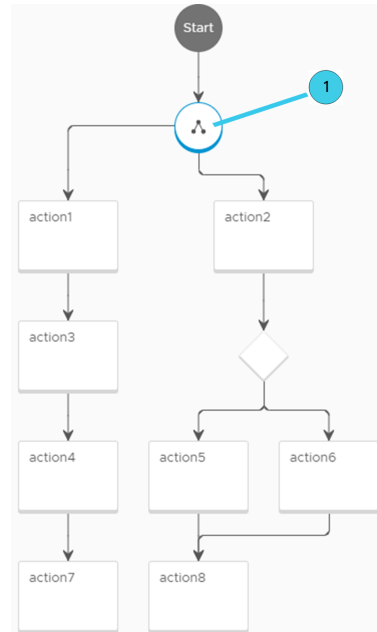
Più script o flussi di azione di estendibilità che suddividono percorsi per contribuire allo stesso output.


```

version: "1"
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
  action2:
    action: <action_name>

```

Nota È possibile tornare a un'azione precedente assegnando l'azione come `next:`. Ad esempio, anziché inserire `next: flow_end` per terminare il flusso di azione, è possibile immettere `next: action1` per eseguire nuovamente l'azione 1 e riavviare la sequenza di azioni.



① Elemento Fork

Flussi di azione Join

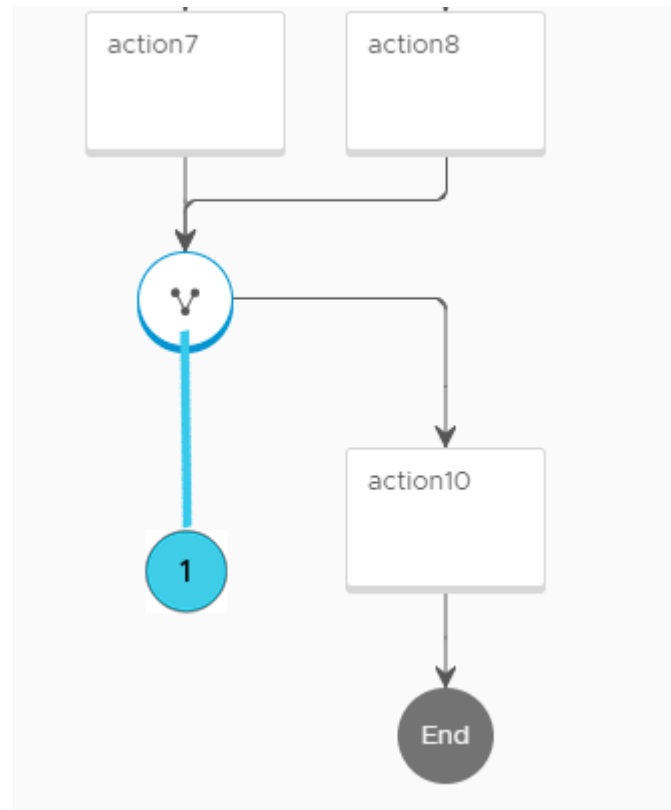
Più script o flussi di azione di estendibilità che uniscono percorsi e contribuiscono allo stesso output.

```

version: "1"
action7:
  action: <action_name>
  next: joinElement
action8:
  action: <action_name>
  next: joinElement
joinElement:
  join:
    type: all
    next: action10
action10:
  action: <action_name>
  next: flow_end

```

Nota È possibile tornare a un'azione precedente assegnando l'azione come `next:`. In questo esempio, anziché `next: flow_end`, è possibile immettere `next: action1` per eseguire nuovamente l'azione 1 e riavviare la sequenza di azioni.



① Elemento Join

Flussi di azione condizionali

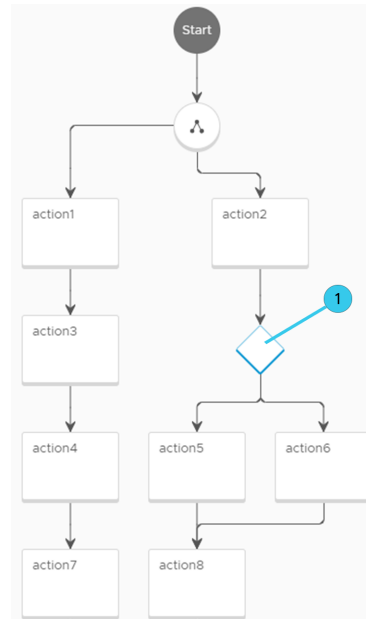
Più script o flussi di azione di estendibilità che vengono eseguiti quando una condizione viene soddisfatta utilizzando un elemento commutatore.

In alcuni casi, la condizione deve essere uguale a `true` per consentire l'esecuzione dell'azione. Altri casi, illustrati in questo esempio, richiedono che i valori dei parametri vengano soddisfatti prima che sia possibile eseguire un'azione. Se nessuna delle condizioni viene soddisfatta, il flusso di azione non riesce.

```

version: 1
id: 1234
name: Test
inputs: ...
outputs: ...
flow:
  flow_start:
    next: forkAction
  forkAction:
    fork:
      next: [action1, action2]
  action1:
    action: <action_name>
    next: action3
  action3:
    action: <action_name>
    next: action4
  action4:
    action: <action_name>
    next: action7
  action7:
    action: <action_name>
    next: joinElement
  action2:
    action: <action_name>
    next: switchAction
  switchAction:
    switch:
      "${1 == 1}": action5
      "${1 != 1}": action6
  action5:
    action: <action_name>
    next: action8
  action6:
    action: <action_name>
    next: action8
  action8:
    action: <action_name>

```



1 Elemento commutatore

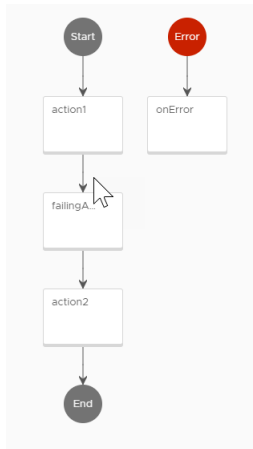
Nota È possibile tornare a un'azione precedente assegnando l'azione come `next:`. Ad esempio, anziché inserire `next: flow_end` per terminare il flusso di azione, è possibile immettere `next: action1` per eseguire nuovamente l'azione 1 e riavviare la sequenza di azioni.

Come utilizzare un gestore errori con i flussi di azione

È possibile configurare il flusso di azione in modo da segnalare un errore durante fasi specifiche del flusso utilizzando un elemento gestore errori.

Un elemento gestore errori richiede due input:

- Messaggio di errore specificato dell'azione non riuscita.
- Input del flusso di azione.



Se un'azione nel flusso non riesce e il flusso contiene un elemento gestore errori, viene visualizzato un messaggio di errore che segnala l'errore dell'azione. Il gestore errori è un'azione autonoma. Lo script seguente è un esempio di gestore errori che può essere utilizzato in un flusso di azione.

```
def handler(context, inputs):

    errorMsg = inputs["errorMsg"]
    flowInputs = inputs["flowInputs"]

    print("Flow execution failed with error {0}".format(errorMsg))
    print("Flow inputs were: {0}".format(flowInputs))

    outputs = {
        "errorMsg": errorMsg,
        "flowInputs": flowInputs
    }

    return outputs
```

È possibile visualizzare le esecuzioni riuscite e quelle non riuscite nella finestra Esecuzioni di azione.

	Status	Run ID	Action
<input type="checkbox"/>	Completed	8a76996b6839fe3c01684...	error-handler
<input type="checkbox"/>	Failed	8a76996b6839fe3c01684...	failing-action
<input type="checkbox"/>	Completed	8a76996b6839fe3c01684...	simple-hello
<input type="checkbox"/>	Completed	8a76996b6839fe3c01684...	flow-with-handler

In questo esempio, il flusso di azione flow-with-handler, che contiene un elemento gestore errori, è stato eseguito correttamente. Tuttavia, una delle azioni nel flusso non è riuscita e ha quindi avviato il gestore errori per la segnalazione di un errore.

Come monitorare le esecuzioni delle azioni

La scheda Esecuzioni di azione include un registro delle azioni di estendibilità attivate dalla sottoscrizione e il relativo stato.

È possibile visualizzare il registro delle esecuzioni delle azioni utilizzando **Estendibilità > Attività > Esecuzioni di azione**. È inoltre possibile filtrare l'elenco delle esecuzioni delle azioni in base a una o più proprietà alla volta.

Risoluzione dei problemi relativi alle esecuzioni non riuscite delle azioni di estendibilità

Se l'esecuzione dell'azione di estendibilità non riesce, è possibile eseguire i passaggi di risoluzione dei problemi per correggerla.

Quando l'esecuzione di un'azione non riesce, è possibile che venga visualizzato un messaggio di errore, uno stato Non riuscito e un registro Non riuscito. Se l'esecuzione dell'azione non riesce, è a causa di un errore della distribuzione o del codice.

Problema	Soluzione
Errore di distribuzione	Questi errori sono il risultato di problemi relativi alla configurazione dell'account cloud, alla distribuzione delle azioni o ad altre dipendenze che possono impedire la distribuzione dell'azione. Assicurarsi che il progetto utilizzato sia definito all'interno dell'account cloud configurato e che disponga delle autorizzazioni per l'esecuzione delle funzioni. Prima di avviare nuovamente l'azione, è possibile testare l'azione su un progetto specifico all'interno della pagina dei dettagli dell'azione.
Errore di codice	Questi errori sono il risultato di script o codici non validi. Utilizzare i registri di esecuzione delle azioni per risolvere i problemi e correggere gli script non validi.

Sottoscrizioni ai workflow di estendibilità

È possibile utilizzare i workflow di vRealize Orchestrator con Cloud Assembly per estendere il ciclo di vita dell'applicazione.

Come modificare le proprietà delle macchine virtuali utilizzando una sottoscrizione del workflow di vRealize Orchestrator

È possibile utilizzare un workflow di vRealize Orchestrator esistente per modificare le proprietà delle macchine virtuali e aggiungere macchine virtuali ad Active Directory.

I parametri dell'argomento dell'evento definiscono il formato del payload per i messaggi EBS (Event Broker Service). Per ricevere e utilizzare il payload dei messaggi EBS all'interno di un workflow, è necessario definire i parametri di input del workflow `inputProperties`.

Prerequisiti

- Ruolo utente amministratore del cloud
- Workflow locali di vRealize Orchestrator esistenti.

- Integrazione e connessione al server client vRealize Orchestrator riuscite.

Procedura

- 1 Selezionare **Estendibilità > Sottoscrizioni**.
- 2 Fare clic su **Nuova sottoscrizione**.
- 3 Creare una sottoscrizione con i seguenti parametri:

Parametro	Valore
Nome	RenameVM
Argomento dell'evento	Selezionare un argomento dell'evento adatto all'integrazione di vRealize Orchestrator desiderata. Ad esempio, Allocazione risorsa di elaborazione.
Di blocco/non di blocco	Non di blocco
Azione/Workflow	Selezionare un tipo eseguibile di vRealize Orchestrator. Selezionare il workflow desiderato. Ad esempio, Imposta nome macchina virtuale.

- 4 Per salvare la sottoscrizione, fare clic su **Salva**.
- 5 Assegnare e attivare la sottoscrizione creando un modello cloud o distribuendo un modello cloud esistente.

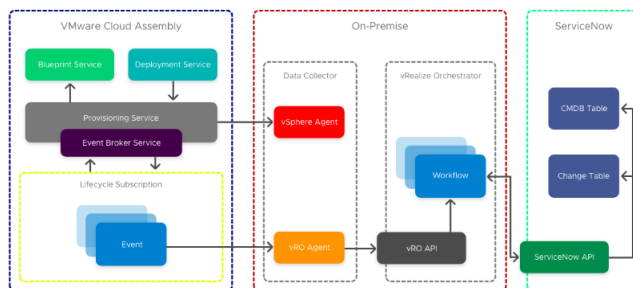
Operazioni successive

Verificare che il workflow sia stato avviato correttamente con uno dei seguenti metodi:

- Verificare il registro delle esecuzioni del workflow in **Estendibilità > Attività > Esecuzioni di workflow**.
- Aprire il client di vRealize Orchestrator e controllare lo stato del workflow passando al workflow e verificando lo stato o aprendo la scheda specifica dei registri.

Come integrare Cloud Assembly per ITSM con ServiceNow utilizzando i workflow di vRealize Orchestrator

Utilizzando i workflow di vRealize Orchestrator, è possibile integrare Cloud Assembly con ServiceNow per la conformità ITSM.



In genere gli utenti aziendali integrano la propria piattaforma di gestione del cloud con una piattaforma di gestione dei servizi IT (ITSM, IT Service Management) e un database di gestione della configurazione (CMDB, Configuration Management Database) a scopo di conformità. Seguendo questo esempio è possibile integrare Cloud Assembly con ServiceNow per CMDB e ITSM utilizzando i workflow di vRealize Orchestrator. Quando si utilizzano le integrazioni e i workflow di vRealize Orchestrator, i tag di funzionalità sono particolarmente utili se si dispone di più istanze per ambienti diversi. Per ulteriori informazioni sui tag di funzionalità, vedere [Utilizzo di tag di funzionalità in Cloud Assembly](#).

Nota È inoltre possibile integrare ServiceNow con Cloud Assembly utilizzando gli script dell'azione di estendibilità. Per informazioni sull'integrazione di ServiceNow utilizzando gli script dell'azione di estendibilità, vedere [Come integrare Cloud Assembly con ServiceNow utilizzando le azioni di estendibilità](#).

In questo esempio, l'integrazione di ServiceNow è composta da tre workflow di livello principale. Ogni workflow dispone delle proprie sottoscrizioni in modo che sia possibile aggiornare e iterare ciascun componente singolarmente.

- Punto di ingresso della sottoscrizione dell'evento - Registrazione di base, identifica l'utente richiedente e la macchina virtuale di vCenter, se applicabile.
- Workflow di integrazione - Separa gli oggetti e inserisce gli input nel workflow tecnico, gestisce gli aggiornamenti della registrazione, delle proprietà e dell'output.
- Workflow tecnico - Integrazione di sistema a valle per l'API di ServiceNow per creare l'API di CI CMDB, CR e Cloud Assembly IaaS con altre proprietà della macchina virtuale esterne al payload.

Prerequisiti

- Un ambiente vRealize Orchestrator standalone o in cluster.
- Un'integrazione di vRealize Orchestrator in Cloud Assembly. Per informazioni sull'integrazione di un vRealize Orchestrator standalone con Cloud Assembly, vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).

Procedura

- 1 Creare e salvare un file di configurazione in vRealize Orchestrator che contenga una configurazione comune utilizzata in più workflow.
- 2 Salvare il token dell'API Cloud Assembly nella stessa posizione del file di configurazione del passaggio 1.

Nota Il token dell'API Cloud Assembly ha una scadenza.

- 3 Creare un workflow in vRealize Orchestrator con l'elemento script specificato. Questo script fa riferimento a un host REST e lo individua. Inoltre, standardizza le azioni REST che utilizzano un parametro facoltativo di un token, aggiunto come ulteriore intestazione di autorizzazione.

```

var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "CASRestHost"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attribute
Name)

var ConfigurationElement =
System.getModule("au.com.cs.example").getConfigurationElementByName(configName,configPath);
System.debug("ConfigurationElement:" + ConfigurationElement);
var casToken = ConfigurationElement.getAttributeWithKey("CASToken")["value"]
if(!casToken){
    throw "no CAS Token";
}
//REST Template
var opName = "casLogin";
var opTemplate = "/iaas/login";
var opMethod = "POST";

// create the REST operation:
var opLogin =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cas API Token
var contentObject = {"refreshToken":casToken}
postContent = JSON.stringify(contentObject);

var loginResponse =
System.getModule("au.com.cs.example").executeOp(opLogin,null,postContent,null) ;

try{
    var tokenResponse = JSON.parse(loginResponse)['token']
    System.debug("token: " + tokenResponse);
} catch (ex) {
    throw ex + " No valid token";
}

//REST Template Machine Details
var opName = "machineDetails";
var opTemplate = "/iaas/machines/" + resourceId;
var opMethod = "GET";

var bearer = "Bearer " + tokenResponse;

var opMachine =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

// (Rest Operation, Params, Content, Auth Token)

```



```

var vmResponse =
System.getModule("au.com.cs.example").executeOp(opMachine,null,"",bearer) ;

try{
    var vm = JSON.parse(vmResponse);
} catch (ex) {
    throw ex + " failed to parse vm details"
}

System.log("cpuCount: " + vm["customProperties"]["cpuCount"]);
System.log("memoryInMB: " + vm["customProperties"]["memoryInMB"]);

cpuCount = vm["customProperties"]["cpuCount"];
memoryMB = vm["customProperties"]["memoryInMB"];

```

Questo script invia l'output `cpuCount` e `memoryMB` al workflow principale e aggiorna le proprietà `customProperties` esistenti. Questi valori possono essere utilizzati nei workflow successivi durante la creazione di CMDB.

- 4 Aggiungere l'elemento script Crea CI di CMDB ServiceNow al workflow. Questo elemento individua l'host REST ServiceNow utilizzando l'elemento di configurazione, crea un'operazione REST per la tabella `cmdb_ci_vmware_instance`, crea una stringa di oggetto contenuto in base agli input del workflow per i dati di pubblicazione e restituisce il valore `sys_id`.

```

var configPath = "CS"
var configName = "environmentConfig"
var attributeName = "serviceNowRestHost"
var tableName = "cmdb_ci_vmware_instance"

//get REST Host from configuration element
var restHost =
System.getModule("au.com.cs.example").getRestHostFromConfig(configPath,configName,attributeName)

//REST Template
var opName = "serviceNowCreatCI";
var opTemplate = "/api/now/table/" + tableName;
var opMethod = "POST";

// create the REST operation:
var opCI =
System.getModule("au.com.cs.example").createOp(restHost,opName,opMethod,opTemplate);

//cmdb_ci_vm_vmware table content to post;
var contentObject = {};
contentObject["name"] = hostname;
contentObject["cpus"] = cpuTotalCount;
contentObject["memory"] = MemoryInMB;
contentObject["correlation_id"] = deploymentId
contentObject["disks_size"] = diskProvisionGB
contentObject["location"] = "Sydney";
contentObject["vcenter_uuid"] = vcUuid;

```

```

contentObject["state"] = "On";
contentObject["owned_by"] = owner;

postContent = JSON.stringify(contentObject);
System.log("JSON: " + postContent);

// (Rest Operation, Params, Content, Auth Token)
var ciResponse =
System.getModule("au.com.cs.example").executeOp(opCI,null,postContent,null) ;

try{
    var cmdbCI = JSON.parse(ciResponse);
} catch (ex) {
    throw ex + " failed to parse ServiceNow CMDB response";
}

serviceNowSysId = cmdbCI['result']['sys_id'];

```

- 5 Mediante l'output del workflow secondario, creare un oggetto proprietà utilizzando il valore `customProperties` esistente e sovrascrivere la proprietà `serviceNowSysId` con il valore di ServiceNow. Questo ID univoco viene utilizzato in CMDB per contrassegnare un'istanza come ritirata dopo l'eliminazione.

Risultati

Cloud Assembly è stato integrato correttamente con ITSM ServiceNow. Per ulteriori informazioni su come utilizzare i workflow per integrare ServiceNow in Cloud Assembly, vedere [Estensione di Cloud Assembly con l'integrazione di vRealize Orchestrator per ServiceNow](#).

Ulteriori informazioni sulle sottoscrizioni ai workflow

Utilizzando un'integrazione di vRealize Orchestrator con Cloud Assembly, è possibile estendere i cicli di vita delle applicazioni con i workflow.

vRealize Automation include una distribuzione di vRealize Orchestrator incorporata. È possibile utilizzare la libreria di workflow della distribuzione di vRealize Orchestrator incorporata nelle sottoscrizioni. È possibile creare, modificare ed eliminare workflow utilizzando il client di vRealize Orchestrator.

È inoltre possibile integrare una distribuzione di vRealize Orchestrator esterna in Cloud Assembly. Vedere [Configurazione di un'integrazione di vRealize Orchestrator in Cloud Assembly](#).

Procedure consigliate per la creazione di workflow di vRealize Orchestrator

Una sottoscrizione al workflow si basa su un argomento dell'evento specifico e sui parametri dell'evento di tale argomento. Per assicurarsi che le sottoscrizioni avviino i workflow di vRealize Orchestrator, è necessario configurarle con i parametri di input corretti in modo che funzionino con i dati degli eventi.

Parametri di input dei workflow

Il workflow personalizzato può includere tutti i parametri o un singolo parametro che utilizza tutti i dati nel payload.

Per utilizzare un singolo parametro, configurare un parametro con tipo `Properties` e nome `inputProperties`.

Parametri di output dei workflow

Il workflow personalizzato può includere parametri di output pertinenti a eventi successivi necessari per un tipo di argomento di evento di risposta.

Se un argomento dell'evento prevede una risposta, i parametri di output del workflow devono corrispondere ai parametri dello schema di risposta.

Come monitorare le esecuzioni dei workflow

La finestra **Esecuzioni di workflow** mostra i registri dei workflow attivati dalla sottoscrizione e il relativo stato.

È possibile visualizzare i registri delle esecuzioni di workflow passando a **Estendibilità > Attività > Esecuzioni di workflow**.

Risoluzione dei problemi relativi alle sottoscrizioni al workflow non riuscite

Se la sottoscrizione al workflow non riesce, è possibile eseguire i passaggi di risoluzione dei problemi per correggerla.

Le esecuzioni dei workflow non riuscite possono causare il mancato avvio o completamento della sottoscrizione al workflow. L'errore di esecuzione del workflow può derivare da diversi problemi comuni.

Problema	Causa	Soluzione
La sottoscrizione al workflow di vRealize Orchestrator non è stata avviata o completata correttamente.	È stata configurata la sottoscrizione al workflow per l'esecuzione di un workflow personalizzato quando viene ricevuto il messaggio dell'evento, ma il workflow non viene eseguito o non viene completato correttamente.	<ol style="list-style-type: none"> 1 Verificare che la sottoscrizione al workflow sia salvata correttamente. 2 Verificare che le condizioni della sottoscrizione al workflow siano configurate correttamente. 3 Verificare che vRealize Orchestrator contenga il workflow specificato. 4 Verificare che il workflow sia configurato correttamente all'interno di vRealize Orchestrator.
La sottoscrizione al workflow di vRealize Orchestrator della richiesta di approvazione non è stata eseguita.	L'utente ha configurato una sottoscrizione al workflow di pre-approvazione o post-approvazione per l'esecuzione di un workflow di vRealize Orchestrator. Il workflow non viene eseguito quando una macchina corrispondente ai criteri definiti viene richiesta nel catalogo dei servizi.	<p>Per eseguire correttamente una sottoscrizione al workflow di approvazione, è necessario verificare che tutti i componenti siano configurati correttamente.</p> <ol style="list-style-type: none"> 1 Verificare che il criterio di approvazione sia attivo e correttamente applicato. 2 Verificare che la propria sottoscrizione al workflow sia configurata e salvata correttamente. 3 Controllare nei registri eventi la presenza di messaggi correlati alle approvazioni.
La sottoscrizione al workflow di vRealize Orchestrator della richiesta di approvazione è stata rifiutata.	<p>È stata configurata la sottoscrizione a un workflow di pre-approvazione o post-approvazione che esegue il workflow di vRealize Orchestrator specificato, ma la richiesta è stata rifiutata a livello di approvazione esterna.</p> <p>Una possibile causa è un errore di esecuzione del workflow interno in vRealize Orchestrator. Ad esempio, il workflow non è presente o il server vRealize Orchestrator non è in esecuzione.</p>	<ol style="list-style-type: none"> 1 Controllare nei registri la presenza di messaggi correlati alle approvazioni. 2 Verificare che il server vRealize Orchestrator sia in esecuzione. 3 Verificare che vRealize Orchestrator contenga il workflow specificato.

Ulteriori informazioni sulle sottoscrizioni di estendibilità

È possibile estendere i cicli di vita dell'applicazione utilizzando le azioni di estendibilità o i workflow ospitati in vRealize Orchestrator con le sottoscrizioni di estendibilità.

Quando si verifica un evento di attivazione nell'ambiente, viene avviata la sottoscrizione e il workflow o l'azione di estendibilità specificati vengono eseguiti. È possibile visualizzare gli eventi di sistema nel registro eventi, le esecuzioni del workflow nella finestra Esecuzioni di workflow e le esecuzioni dell'azione nella finestra Esecuzioni di azione. Le sottoscrizioni sono specifiche del progetto, ovvero sono collegate ai modelli cloud e alle distribuzioni tramite il progetto specificato.

Terminologia dell'estendibilità

Quando si utilizzano le sottoscrizioni di estendibilità in Cloud Assembly, è possibile incontrare una terminologia specifica delle sottoscrizioni e del servizio del gestore eventi.

Tabella 6-6. Terminologia dell'estendibilità

Termine	Descrizione
Argomento dell'evento	Descrive una serie di eventi con lo stesso intento logico e la stessa struttura. Ciascun evento è un'istanza di un argomento di evento. È possibile assegnare parametri di blocco a determinati argomenti degli eventi. Per ulteriori informazioni, vedere Argomenti relativi agli eventi di blocco .
Evento	Indica una modifica nello stato del produttore o in qualsiasi entità gestita dal produttore. L'evento rappresenta l'entità che registra informazioni sull'occorrenza dell'evento.
Servizio del gestore eventi	Il servizio di consegna dei messaggi pubblicati da un produttore ai consumatori sottoscrittori.
Payload	I dati dell'evento che contengono tutte le proprietà pertinenti relative all'argomento dell'evento.
Sottoscrizione	Indica che un sottoscrittore è interessato a ricevere la notifica di un evento sottoscrivendo un argomento di evento e definendo i criteri che attivano la notifica. Le sottoscrizioni collegano le azioni di estendibilità o i workflow agli eventi di attivazione utilizzati per automatizzare le parti del ciclo di vita delle applicazioni.
Sottoscrittore	L'utente informato degli eventi pubblicati nel servizio del gestore eventi in base alla definizione della sottoscrizione. Il sottoscrittore può anche essere definito cliente.
Amministratore di sistema	Un utente con privilegi di creazione, lettura, aggiornamento ed eliminazione di sottoscrizioni ai workflow di tenant e sistema che utilizza Cloud Assembly.
Sottoscrizione al workflow	Specifica l'argomento dell'evento e le condizioni che attivano un workflow di vRealize Orchestrator.
Sottoscrizione all'azione	Specifica l'argomento dell'evento e le condizioni che attivano l'esecuzione di un'azione di estendibilità.
Workflow	Un workflow di vRealize Orchestrator integrato all'interno di Cloud Assembly. È possibile collegare questi workflow agli eventi all'interno delle sottoscrizioni.

Tabella 6-6. Terminologia dell'estendibilità (continua)

Termine	Descrizione
Azione di estendibilità	Uno script di codice semplificato che può essere eseguito dopo l'attivazione di un evento in una sottoscrizione. Le azioni di estendibilità sono simili ai workflow, ma sono più leggere. Le azioni di estendibilità possono essere personalizzate da Cloud Assembly.
Esecuzioni di azione	Accessibile tramite la scheda Esecuzioni di azione . L'esecuzione di un'azione è un registro dettagliato delle azioni di estendibilità eseguite in risposta agli eventi di attivazione.

Argomenti relativi agli eventi di blocco

Alcuni argomenti degli eventi supportano gli eventi di blocco. Il comportamento di una sottoscrizione di estendibilità dipende dal fatto che l'argomento supporti o meno questi tipi di evento e da come viene configurata la sottoscrizione.

Le sottoscrizioni di estendibilità di Cloud Assembly possono utilizzare due tipi di argomenti di evento, ovvero gli argomenti relativi agli eventi non di blocco e gli argomenti relativi agli eventi di blocco. Il tipo di argomento dell'evento definisce il comportamento della sottoscrizione di estendibilità.

Argomenti relativi agli eventi non di blocco

Gli argomenti degli eventi non di blocco consentono di creare solo sottoscrizioni non di blocco. Le sottoscrizioni non di blocco vengono attivate in modo asincrono e non è possibile fare affidamento sull'ordine in cui vengono attivate.

Argomenti relativi agli eventi di blocco

Alcuni argomenti degli eventi supportano il blocco. Se una sottoscrizione è contrassegnata come di blocco, tutti i messaggi che soddisfano le condizioni impostate non vengono ricevuti da altre sottoscrizioni con condizioni corrispondenti finché non viene eseguito l'elemento eseguibile della sottoscrizione di blocco.

Le sottoscrizioni di blocco vengono eseguite in ordine di priorità. Il valore di priorità più alto è 0 (zero). Se sono presenti più sottoscrizioni di blocco per lo stesso argomento di evento con lo stesso livello di priorità, le sottoscrizioni vengono eseguite in ordine alfabetico inverso in base al nome della sottoscrizione. Una volta elaborate tutte le sottoscrizioni di blocco, il messaggio viene inviato contemporaneamente a tutte le sottoscrizioni non di blocco. Poiché le sottoscrizioni di blocco vengono eseguite in modo sincrono, il payload dell'evento modificato include l'evento aggiornato quando vengono notificate le sottoscrizioni successive.

È possibile utilizzare gli argomenti relativi agli eventi di blocco per gestire più sottoscrizioni che dipendono l'una dall'altra.

È ad esempio possibile che siano presenti due sottoscrizioni al workflow di provisioning in cui la seconda sottoscrizione dipende dai risultati della prima sottoscrizione. La prima sottoscrizione modifica una proprietà durante il provisioning, mentre la seconda sottoscrizione registra la nuova proprietà, ad esempio il nome di una macchina, in un file system. Alla sottoscrizione `ChangeProperty` viene assegnata la priorità 0, mentre a `RecordProperty` viene assegnata la priorità 1, perché la seconda sottoscrizione utilizza i risultati della prima sottoscrizione. Quando viene effettuato il provisioning di una macchina, viene avviata l'esecuzione della sottoscrizione `ChangeProperty`. Poiché le condizioni della sottoscrizione `RecordProperty` si basano su una condizione di post-provisioning, un evento attiva la sottoscrizione `RecordProperty`. Tuttavia, poiché il workflow di `ChangeProperty` è un workflow di blocco, l'evento viene ricevuto solo dopo che il workflow è stato completato. Quando viene modificato il nome della macchina e viene completata la prima sottoscrizione al workflow, viene eseguita la seconda sottoscrizione al workflow e il nome della macchina viene registrato nel file system.

Elemento eseguibile di ripristino

Per gli argomenti relativi agli eventi di blocco, è possibile aggiungere un elemento eseguibile di ripristino alla sottoscrizione. L'elemento eseguibile di ripristino in una sottoscrizione viene eseguito se l'elemento eseguibile primario non riesce. Ad esempio, è possibile creare una sottoscrizione al workflow in cui l'elemento eseguibile primario sia un workflow che crea record in un sistema CMDB come ServiceNow. Anche se la sottoscrizione al workflow non riesce, è possibile che nel sistema CMDB vengano creati alcuni record. In questo scenario, è possibile utilizzare un elemento eseguibile di ripristino per rimuovere i record lasciati nel sistema CMDB dall'elemento eseguibile non riuscito.

Per i casi d'uso che includono più sottoscrizioni che dipendono l'una dall'altra, è possibile aggiungere una proprietà `ebs.recover.continuation` all'elemento eseguibile di ripristino. Con questa proprietà, è possibile specificare se il servizio di estendibilità deve continuare con la sottoscrizione successiva nella catena, nel caso in cui la sottoscrizione corrente non riesca.

Argomenti degli eventi forniti con Cloud Assembly

Cloud Assembly include argomenti degli eventi predefiniti.

Argomenti degli eventi

Gli argomenti degli eventi sono le categorie che raggruppano eventi simili. Quando vengono assegnati a una sottoscrizione, gli argomenti degli eventi definiscono quali sono gli eventi che attivano la sottoscrizione. I seguenti argomenti degli eventi vengono forniti per impostazione predefinita con Cloud Assembly. Tutti gli argomenti possono essere utilizzati per aggiungere o aggiornare proprietà o tag personalizzati della risorsa. Se l'azione di estendibilità o il workflow di vRealize Orchestrator non riesce, anche l'attività corrispondente non riesce.

Tabella 6-7. Argomenti degli eventi di Cloud Assembly

Argomento dell'evento	Bloccabile	Descrizione
Cloud template configuration	No	Emesso quando si verifica un evento di configurazione del modello cloud, ad esempio la creazione o l'eliminazione di un modello cloud. Questo argomento dell'evento può essere utile per segnalare tali eventi ai sistemi esterni.
Cloud template version configuration	No	Emesso quando si verifica un nuovo evento di controllo delle versioni del modello cloud, ad esempio la creazione, il rilascio, l'annullamento del rilascio o il ripristino di una versione. Questo argomento dell'evento può essere utile con le integrazioni dei sistemi di controllo delle versioni di terze parti.
Compute allocation	Sì	Emesso prima dell'allocazione di <code>resourcenames</code> e <code>hostselections</code> . Entrambe queste proprietà possono essere modificate in questa fase. Emesso una sola volta per un cluster di macchine.
Compute gateway post provisioning	Sì	Emesso dopo il provisioning di una risorsa gateway di elaborazione.
Compute gateway post removal	Sì	Emesso dopo la rimozione di una risorsa gateway di elaborazione.
Compute gateway provisioning	Sì	Emesso prima del provisioning di un gateway di elaborazione.
Compute gateway removal	Sì	Emesso prima della rimozione di un gateway di elaborazione.
Compute initial power on	Sì	Emesso dopo il provisioning di una risorsa a livello di hypervisor, ma prima che la risorsa venga accesa per la prima volta. Attualmente, questo argomento dell'evento è supportato solo per vSphere. Gli eventi vengono inviati per ogni macchina in un cluster. Nota È possibile ignorare l'accensione iniziale della risorsa.
Compute nat post provisioning	Sì	Emesso dopo il provisioning di una risorsa NAT di elaborazione.
Compute nat post removal	Sì	Emesso dopo la rimozione di una risorsa NAT di elaborazione.
Compute nat provisioning	Sì	Emesso prima del provisioning di un NAT di elaborazione.

Tabella 6-7. Argomenti degli eventi di Cloud Assembly (continua)

Argomento dell'evento	Bloccabile	Descrizione
Compute nat removal	Sì	Emesso prima della rimozione di un NAT di elaborazione.
Compute post provision	Sì	Emesso dopo il provisioning di una risorsa. Gli eventi vengono inviati per ogni macchina in un cluster.
Compute post removal	Sì	Emesso dopo la rimozione di una risorsa di elaborazione. Gli eventi vengono inviati per ogni macchina in un cluster.
Compute provision	Sì	Emesso prima che venga eseguito il provisioning della risorsa a livello dell'hypervisor. Gli eventi vengono inviati per ogni macchina in un cluster. Nota È possibile modificare l'indirizzo IP allocato.
Compute removal	Sì	Emesso prima della rimozione della risorsa. Gli eventi vengono inviati per ogni macchina in un cluster.
Compute reservation	Sì	Emesso al momento della prenotazione. Emesso una sola volta per un cluster di macchine. Nota È possibile modificare l'ordine di posizionamento.
Custom resource post provision	Sì	Emesso per gli eventi di post-provisioning attivati da operazioni di risorse personalizzate.
Custom resource pre provision	Sì	Emesso per eventi di pre-provisioning attivati da operazioni di risorse personalizzate.
Deployment action completed	Sì	Emesso dopo il completamento di un'azione di distribuzione.
Deployment action requested	Sì	Emesso prima del completamento di un'azione di distribuzione.
Deployment completed	Sì	Emesso dopo la distribuzione di una richiesta di modello cloud o di catalogo.
Deployment onboarded	No	Emesso quando è stato eseguito l'onboarding di una nuova distribuzione.
Deployment requested	Sì	Emesso prima della distribuzione di una richiesta di modello cloud o di catalogo.

Tabella 6-7. Argomenti degli eventi di Cloud Assembly (continua)

Argomento dell'evento	Bloccabile	Descrizione
Deployment resource action completed	Sì	Emesso dopo la distribuzione di un'azione risorsa.
Deployment resource action requested	Sì	Emesso prima della distribuzione di un'azione risorsa.
Deployment resource completed	Sì	Emesso dopo il provisioning di una risorsa di distribuzione.
Deployment resource requested	Sì	Emesso prima del provisioning di una risorsa di distribuzione.
Disk allocation	Sì	Emesso per la preallocazione delle risorse del disco.
Disk attach	Sì	<p>Emesso prima che un disco sia collegato a una macchina. <code>Disk attach</code> è un evento di lettura e scrittura. Le proprietà del disco supportate per il writeback sono:</p> <ul style="list-style-type: none"> ■ <code>diskFullPaths</code> ■ <code>diskDatastoreNames</code> ■ <code>diskParentDirs</code> <p>Per gli aggiornamenti sono necessarie tutte e tre le proprietà del disco specifiche di vSphere. Tutte le altre proprietà sono di sola lettura.</p> <p>Nota Il writeback è facoltativo per i First Class Disk di vSphere.</p>
Disk detach	Sì	Emesso dopo lo scollegamento di un disco da una macchina. <code>Disk detach</code> è un evento di sola lettura.
Disk post removal	Sì	Emesso dopo l'eliminazione di una risorsa del disco.
Disk post resize	Sì	Emesso dopo il ridimensionamento di una risorsa del disco.
Kubernetes cluster allocation	Sì	Emesso per la preallocazione di risorse per un cluster Kubernetes.
Kubernetes cluster post provision	Sì	Emesso dopo il provisioning di un cluster Kubernetes.
Kubernetes cluster post removal	Sì	Emesso dopo l'eliminazione di un cluster Kubernetes.
Kubernetes cluster provision	Sì	Emesso prima del provisioning di un cluster Kubernetes.
Kubernetes cluster removal	Sì	Emesso prima dell'avvio del processo di eliminazione di un cluster Kubernetes.

Tabella 6-7. Argomenti degli eventi di Cloud Assembly (continua)

Argomento dell'evento	Bloccabile	Descrizione
Kubernetes namespace allocation	Sì	Emesso durante la preallocazione per le risorse dello spazio dei nomi Kubernetes.
Kubernetes namespace post provision	Sì	Emesso dopo il provisioning di una risorsa dello spazio dei nomi Kubernetes.
Kubernetes namespace post removal	Sì	Emesso dopo la rimozione di una risorsa dello spazio dei nomi Kubernetes.
Kubernetes namespace provision	Sì	Emesso prima del provisioning di uno spazio dei nomi Kubernetes.
Kubernetes namespace removal	Sì	Emesso prima della rimozione di una risorsa cluster dello spazio dei nomi.
Kubernetes supervisor namespace allocation	Sì	Emesso durante la preallocazione per le risorse dello spazio dei nomi supervisore Kubernetes.
Kubernetes supervisor namespace post provision	Sì	Emesso dopo il provisioning di uno spazio dei nomi supervisore.
Kubernetes supervisor namespace post removal	Sì	Emesso dopo la rimozione di una risorsa dello spazio dei nomi supervisore.
Kubernetes supervisor namespace provision	Sì	Emesso prima del provisioning di uno spazio dei nomi supervisore.
Kubernetes supervisor namespace removal	Sì	Emesso prima della rimozione di una risorsa dello spazio dei nomi supervisore.
Load balancer post provision	Sì	Emesso dopo il provisioning di un bilanciamento del carico.
Load balancer post removal	Sì	Emesso dopo la rimozione di un bilanciamento del carico.
Load balancer provision	Sì	Emesso prima del provisioning di un bilanciamento del carico.
Load balancer removal	Sì	Emesso prima della rimozione di un bilanciamento del carico.
Network Configure	Sì	Emesso quando la rete viene configurata durante l'allocazione della risorsa di elaborazione.
Network post provisioning	Sì	Emesso dopo il provisioning di una risorsa di rete.

Nota L'argomento Configurazione rete supporta più indirizzi IP/NIC.

Tabella 6-7. Argomenti degli eventi di Cloud Assembly (continua)

Argomento dell'evento	Bloccabile	Descrizione
Network post removal	Sì	Emesso dopo la rimozione di una risorsa di rete.
Network provisioning	Sì	Emesso prima del provisioning di una risorsa di rete.
Network removal	Sì	Emesso prima della rimozione di una risorsa di rete.
Project Lifecycle Event Topic	No	Emesso al momento della creazione, dell'aggiornamento o dell'eliminazione di un progetto.
Provisioning request	Sì	Emesso prima della rimozione di un gruppo di sicurezza.
Security group post provision	Sì	Emesso dopo il provisioning di un gruppo di sicurezza.
Security group post removal	Sì	Emesso dopo la rimozione di un gruppo di sicurezza.
Security group provisioning	Sì	Emesso prima del provisioning di un gruppo di sicurezza.
Security group removal	Sì	Emesso prima della rimozione di un gruppo di sicurezza.

Parametri degli eventi

Dopo aver aggiunto un argomento dell'evento, è possibile visualizzare i parametri di tale argomento dell'evento. Questi parametri di evento definiscono la struttura del payload dell'evento o `inputProperties`. Alcuni parametri di evento non possono essere modificati e sono contrassegnati come di sola lettura. È possibile identificare questi parametri di sola lettura facendo clic sull'icona delle informazioni a destra del parametro.

Registro degli eventi di estendibilità

La pagina degli eventi di estendibilità mostra l'elenco di tutti gli eventi che si sono verificati all'interno dell'ambiente.

È possibile visualizzare i registri degli eventi di estendibilità passando a **Estendibilità > Eventi**. È inoltre possibile filtrare l'elenco degli eventi in base a una o più proprietà. Per visualizzare ulteriori dettagli di un singolo evento, selezionare l'ID dell'evento.

ID	Timestamp	Event Topic	User Name	Target ID	Description
cbaf56ce-a324-f5ae-5dd1-66d1e59f1a6	04/28/20, 1:10 PM	N/A	N/A	endpoints	CREATE
ef621f51-2906-dce2-14ab-68c17132d756	03/25/20, 4:22 PM	N/A	N/A	endpoints	CREATE
468e8e55-cf27-e77e-0179-1b5b736717b3	03/25/20, 10:12 AM	N/A	N/A	endpoints	CREATE
d9482883-d1ae-5899-fb06-852c202cc178	03/20/20, 2:41 PM	N/A	N/A	endpoints	CREATE
38584d40-a663-631f-7098-3747aa528d12	01/30/20, 5:35 PM	N/A	N/A	endpoints	CREATE

Creazione di una sottoscrizione di estendibilità

Utilizzando un'integrazione o le azioni di estendibilità di vRealize Orchestrator con Cloud Assembly, è possibile creare sottoscrizioni per estendere le applicazioni.

Le sottoscrizioni di estendibilità consentono di estendere le applicazioni attivando workflow o azioni durante eventi specifici del ciclo di vita. È inoltre possibile applicare filtri alle proprie sottoscrizioni per impostare condizioni booleane per l'evento specificato. Ad esempio, l'evento e il workflow o l'azione vengono attivati solo se l'espressione booleana è `'true'`. Ciò è utile per gli scenari in cui si desidera controllare quando vengono attivati gli eventi, le azioni o i workflow.

Prerequisiti

- Verificare di disporre del ruolo utente di amministratore del cloud.
- Se si utilizzano i workflow di vRealize Orchestrator:
 - La libreria del client vRealize Orchestrator incorporato o la libreria di qualsiasi istanza di vRealize Orchestrator esterna integrata.
- Se si utilizzano le azioni di estendibilità:
 - Script di azioni di estendibilità esistenti. Per ulteriori informazioni, vedere [Come creare le azioni di estendibilità](#).

Procedura

- 1 Selezionare **Estendibilità > Sottoscrizioni**.
- 2 Fare clic su **Nuova sottoscrizione**.
- 3 Inserire i dettagli della sottoscrizione.
- 4 Impostare il campo **Ambito organizzazione** per la sottoscrizione.

Nota Per ulteriori informazioni sulla creazione di sottoscrizioni di estendibilità per i provider e i tenant dell'organizzazione, vedere [Creazione di sottoscrizioni di estendibilità per provider o tenant](#).

- 5 Selezionare un **Argomento dell'evento**.

6 (Facoltativo) Impostare le condizioni per l'argomento dell'evento.

Nota È possibile creare condizioni utilizzando un'espressione con sintassi JavaScript. Questa espressione può includere operatori booleani, ad esempio "&&" (AND), "||" (OR), "^" (XOR) e "!" (NOT). È inoltre possibile utilizzare gli operatori aritmetici, come "==" (equal to), "!=" (not equal to), ">=" (greater than or equal), "<=" (less than or equal), ">" (greater than) e "<" (lesser than). Le espressioni booleane più complesse possono essere composte da espressioni più semplici. Per accedere al payload dell'evento in base ai parametri dell'argomento specificato, utilizzare `'event.data'` o qualsiasi proprietà dell'intestazione dell'evento: `sourceType`, `sourceIdentity`, `timeStamp`, `eventType`, `eventTopicId`, `correlationType`, `correlationId`, `description`, `targetType`, `targetId`, `userName` e `orgId`.

7 In **Azione/Workflow** selezionare un elemento eseguibile per la sottoscrizione dell'estendibilità.

8 (Facoltativo) Se applicabile, configurare il comportamento di blocco per l'argomento dell'evento.

9 (Facoltativo) Per definire l'ambito del progetto della sottoscrizione di estendibilità, deselezionare **Qualsiasi progetto** e fare clic su **Aggiungi progetti**.

Nota Se l'ambito dell'organizzazione della sottoscrizione è impostato su **Qualsiasi organizzazione tenant**, l'ambito del progetto è sempre impostato su **Qualsiasi progetto** e non può essere modificato. È possibile modificare l'ambito del progetto solo se l'ambito dell'organizzazione è impostato sull'organizzazione del provider.

10 Per salvare la sottoscrizione, fare clic su **Salva**.

Risultati

La sottoscrizione viene creata. Quando un evento, classificato in base all'argomento dell'evento selezionato, si verifica, vengono avviati il workflow o l'azione di estendibilità di vRealize Orchestrator collegati e vengono informati tutti i sottoscrittori.

Operazioni successive

Dopo aver creato la sottoscrizione, è possibile creare o distribuire un modello cloud per collegare e utilizzare la sottoscrizione. È inoltre possibile controllare lo stato dell'esecuzione del workflow o dell'estendibilità nella scheda **Estendibilità** in Cloud Assembly. Per le sottoscrizioni che contengono workflow vRealize Orchestrator, è anche possibile monitorare le esecuzioni e lo stato del workflow dal client vRealize Orchestrator.

Utilizzo delle sottoscrizioni di estendibilità per gestire la scadenza delle distribuzioni

È possibile gestire le distribuzioni scadute e le relative risorse utilizzando l'azione `Expire` insieme agli argomenti degli eventi esistenti.

Dopo la scadenza del lease di distribuzione nell'ambiente in uso, è possibile utilizzare gli argomenti dell'evento di estendibilità per eseguire attività, ad esempio l'interruzione del backup o il monitoraggio di una risorsa di distribuzione. Per eseguire queste operazioni giorno 2, l'API di vRealize Automation utilizza un'azione `Expire` a livello di sistema. Questa azione viene attivata automaticamente dal sistema ogni volta che un lease di distribuzione nell'organizzazione scade. L'attivazione dell'azione `Expire` precede l'evento di spegnimento di tutte le risorse associate a tale distribuzione.

Nota Nelle versioni precedenti del prodotto, l'evento di spegnimento veniva attivato a livello di distribuzione dopo la scadenza del lease. Ora l'evento di spegnimento viene attivato a livello di risorsa per ogni risorsa di distribuzione accesa.

L'azione `Expire` è inclusa nel payload degli argomenti dell'evento esistenti, ad esempio **Azione di distribuzione richiesta** e **Azione di distribuzione completata**, e utilizza il parametro `deploymentid` per eseguire attività precedenti alla scadenza e successive alla scadenza associate alle risorse di distribuzione.

Nota L'azione `Expire` viene attivata circa 10-15 minuti dopo la scadenza del lease di distribuzione. Il sistema non attiva gli eventi di scadenza del lease prima della scadenza effettiva del lease. L'azione `Expire` è un'azione a livello di sistema e gli utenti non possono attivare manualmente gli eventi associati a tale azione.

Per il caso d'uso corrente, si utilizza l'argomento dell'evento **Azione di distribuzione richiesta** insieme all'azione `Expire` per eseguire il backup di una macchina virtuale nella distribuzione come modello. In questo caso, il backup viene eseguito utilizzando un workflow di vRealize Orchestrator, ma è possibile eseguire la stessa attività anche utilizzando un'azione di estendibilità come elemento eseguibile della sottoscrizione.

Procedura

- 1 Passare a **Estendibilità > Sottoscrizioni** e fare clic su **Nuova sottoscrizione**.
- 2 Immettere un nome per la sottoscrizione.
- 3 In **Stato** verificare che la sottoscrizione sia abilitata.
- 4 In **Argomento dell'evento** selezionare l'argomento dell'evento **Azione di distribuzione richiesta**.
- 5 Attivare l'opzione **Condizione** e aggiungere un filtro per l'azione di scadenza:

```
event.data.actionName == 'Expire'
```

Nota L'argomento dell'evento **Azione di distribuzione richiesta** può essere attivato da operazioni giorno 2 di distribuzione diverse, ad esempio la modifica della durata del lease della distribuzione. L'aggiunta del filtro dell'azione di scadenza del lease garantisce che la sottoscrizione venga attivata solo per gli eventi di scadenza.

6 In **Azione/Workflow**, aggiungere il workflow vRealize Orchestrator.

Lo schema di questo workflow di esempio include un'attività gestibile tramite script e un elemento del workflow che include il workflow **Clona macchina virtuale, nessuna personalizzazione** preconfigurato con vRealize Orchestrator. L'elemento dell'attività gestibile tramite script include il seguente script di esempio:

```
System.log("Lease expiry action triggered to clone a VM...")

System.log("Deployment Id is: " + inputProperties.deploymentId);
inputHeaders = new Properties();
deploymentId = inputProperties.deploymentId;
pathUriVariable = "/deployment/api/deployments/" + deploymentId + "/resources";
var restClient = vRAHost.createRestClient();
var request = restClient.createRequest("GET", pathUriVariable, null);
var keys = inputHeaders.keys;
for(var key in keys){
    request.setHeader(keys[key], inputHeaders.get(keys[key]));
}
var response = restClient.execute(request);
System.log("Content as string: " + response.contentAsString);
var content = response.contentAsString;
var obj = JSON.parse(content);

var object = new Properties(obj);
var contentJson = object.content;
for (var i = 0; i < contentJson.length; i++) {
    var resources = contentJson[i];

    var resourceProperties = resources.properties;
    System.log("Resource name is: " + resourceProperties.resourceName)
    resourceName = resourceProperties.resourceName;
}

var query = "xpath:name='" + resourceName + "'";
var vms=Server.findAllForType("VC:VirtualMachine", query);
vcVM=vms[0];

System.log("VM input is: " + vcVM);
dataStoreOutput = datastore
template= true;
name="test-vm-name"
```

7 Decidere se impostare la sottoscrizione come bloccante o non bloccante.

Nota Se si rende la sottoscrizione bloccante, l'evento di spegnimento per le risorse di distribuzione viene attivato solo dopo che l'esecuzione dell'elemento eseguibile, in questo caso il workflow di scadenza del lease, viene completata correttamente. Se si rende la sottoscrizione non bloccante, l'evento di spegnimento viene attivato per le risorse di distribuzione indipendentemente dallo stato dell'esecuzione del workflow.

8 Per completare la modifica della sottoscrizione, fare clic su **Salva**.

Operazioni successive

Dopo che la sottoscrizione di estendibilità viene attivata dall'evento di scadenza del lease e l'esecuzione del workflow viene eseguita correttamente, passare a vSphere Web Client e verificare che la macchina virtuale sia stata convertita in un modello.

Risoluzione dei problemi relativi a una sottoscrizione di estendibilità

Risolvere gli errori della sottoscrizione di estendibilità.

Quando la sottoscrizione non riesce, è in genere dovuto a errori con il workflow o con lo script dell'azione di estendibilità.

Visualizzazione di parametri e payload dell'argomento

È possibile utilizzare uno script dei parametri dell'argomento della sottoscrizione dump per visualizzare i parametri e il payload specifici della macchina virtuale in qualsiasi fase dell'evento specificato.

In primo luogo, questo script è utile per il debug e la verifica degli input disponibili per il workflow di vRealize Orchestrator. Per visualizzare tutti i parametri della macchina virtuale, utilizzare il seguente script con il workflow:

```
function dumpProperties(props, lvl) {
    var keys = props.keys;
    var prefix = ""
    for (var i=0; i<lvl; i++){
        prefix = prefix + " ";
    }
    for (k in keys){
        var key = keys[k];
        var value = props.get(keys[k])
        if ("Properties" == System.getObjectType(value)){
            System.log(prefix + key + "[")
            dumpProperties(value, (lvl+2));
            System.log(prefix+ "]")
        } else{
            System.log( prefix + key + ":" + value)
        }
    }
}

dumpProperties(inputProperties, 0)

customProps = inputProperties.get("customProperties")
```

Cronologia delle versioni della sottoscrizione

Se la sottoscrizione non riesce, è possibile visualizzare la cronologia delle versioni.

Visualizzazione della cronologia delle versioni della sottoscrizione

Nella scheda **Cronologia versioni** dell'editor di sottoscrizioni è possibile visualizzare la cronologia delle modifiche della sottoscrizione con l'utente che ha eseguito la modifica e la data. È inoltre possibile confrontare diverse versioni di sottoscrizione facendo clic su **Confronta con**. Se la sottoscrizione non riesce o è in esecuzione in modo errato, la cronologia delle versioni può aiutare a identificare la causa.

Gestione di distribuzioni e risorse in Cloud Assembly

7

In qualità di amministratori del cloud o sviluppatori di modelli cloud è possibile utilizzare la scheda Risorse per gestire le risorse cloud. Le risorse possono essere quelle distribuite, ma possono anche essere quelle rilevate per gli account cloud, le risorse individuate di cui è stato eseguito l'onboarding o altre risorse disponibili per la gestione utilizzando Cloud Assembly

Questo capitolo include i seguenti argomenti:

- [Gestione delle distribuzioni di Cloud Assembly](#)
- [Gestione delle risorse in Cloud Assembly](#)

Gestione delle distribuzioni di Cloud Assembly

Gli amministratori del cloud e gli sviluppatori di modelli cloud di Cloud Assembly possono utilizzare la scheda Distribuzioni per gestire le distribuzioni e le risorse associate. È possibile risolvere i problemi correlati a processi di provisioning non riusciti, apportare modifiche alle risorse ed eliminare definitivamente le distribuzioni inutilizzate.

Le distribuzioni includono modelli cloud distribuiti e risorse di cui è stato eseguito l'onboarding. È inoltre possibile che le risorse create utilizzando l'API IaaS vengano visualizzate come distribuzioni.

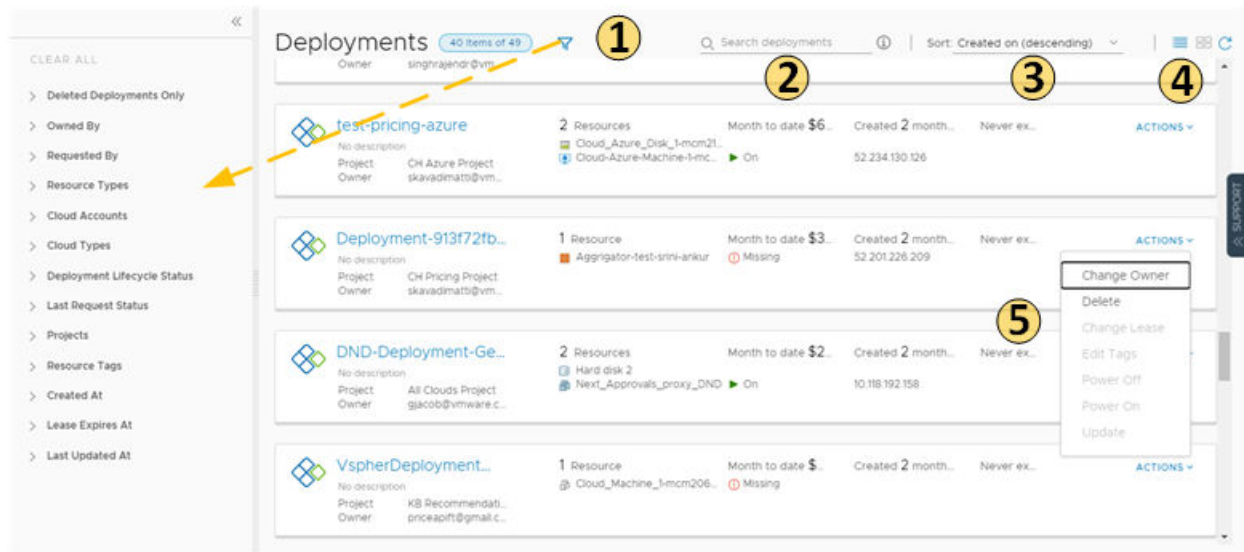
Se si gestisce un numero ridotto di distribuzioni, dalle schede delle distribuzioni è possibile accedere a una vista grafica per la loro gestione. Se si gestisce un numero di distribuzioni elevato, l'elenco delle distribuzioni e l'elenco delle risorse offrono una vista di gestione più robusta.

Per visualizzare le distribuzioni, selezionare **Risorse > Distribuzioni**.

Utilizzo delle schede delle distribuzioni e dell'elenco di distribuzioni

È possibile individuare e gestire le distribuzioni utilizzando l'elenco di schede. È possibile filtrare o cercare distribuzioni specifiche e quindi eseguire azioni su tali distribuzioni.

Figura 7-1. Vista scheda pagina Distribuzioni



1 Filtrare le richieste in base ad attributi.

Ad esempio, è possibile filtrare in base al proprietario, ai progetti, alla data di scadenza del lease o ad altre opzioni di filtraggio. Oppure è possibile trovare tutte le distribuzioni per due progetti con un tag specifico. Quando si crea il filtro per i progetti e l'esempio di tag, i risultati sono conformi ai seguenti criteri: (Project1 OR Project2) AND Tag1.

I valori visualizzati nel riquadro dei filtri dipendono dalle distribuzioni correnti che si è autorizzati a visualizzare o gestire.

La maggior parte dei filtri e il loro utilizzo sono di facile comprensione. Di seguito sono disponibili ulteriori informazioni su alcuni di questi filtri.

- 2 Cercare le distribuzioni in base alle parole chiave o al richiedente.
- 3 Ordinare l'elenco in base all'ora o al nome.
- 4 Passare dalla vista scheda delle distribuzioni alla vista elenco delle distribuzioni e viceversa.
- 5 Eseguire azioni a livello di distribuzione sulla distribuzione, tra cui l'eliminazione delle distribuzioni inutilizzate per recuperare le risorse.

È inoltre possibile visualizzare i costi, le date di scadenza e lo stato delle distribuzioni.

Nella sezione in alto a destra nella pagina, a destra della casella di testo Ordina, è possibile passare dalla vista scheda alla vista elenco e viceversa. È possibile utilizzare la vista elenco per gestire un numero elevato di distribuzioni in meno pagine.

Figura 7-2. Vista elenco della pagina Distribuzioni

Deployments 40 items of 208 🔍 Search deployments ⓘ Sort: Created on (descending) ⌵ ☰ 88 ↻

	Actions	Address	Owner	Project	Status	Expires on	Price
▼	⚙ shared-ip-ranges-d...		bratanov@vmware.com	bratanov-ipa...		Never	
	⚙ nikola-ipam-test-0...	192.168.0.6			▶ On		
	⚙ net.90						
>	⚙ shared-ip-ranges-d...		bratanov@vmware.com	bratanov-ipa...		Never	
>	⚙ test-depl		bratanov@vmware.com	bratanov-ipa...	❗ Create — Failed	Never	
>	⚙ test2222		tdimitrova@vmware.com	vraikov		Never	
>	⚙ afd54234		vraikov@vmware.com	vraikov		Never	
>	⚙ 4erasd		vraikov@vmware.com	vraikov		Never	
>	⚙ grigor test 2412412		gganekov@vmware.com	vp-project		Never	

Utilizzo dei filtri delle distribuzioni selezionati

La tabella seguente non rappresenta un elenco definitivo delle opzioni di filtro. La maggior parte di queste sono autoesplicative. Tuttavia, alcuni filtri richiedono ulteriori approfondimenti.

Tabella 7-1. Informazioni sul filtro selezionato

Nome del filtro	Descrizione
Solo risorse ottimizzabili	Se vRealize Operations Manager è stato integrato e si utilizza l'integrazione per identificare le risorse recuperabili, è possibile attivare il filtro per limitare l'elenco delle distribuzioni idonee.
Stato ciclo di vita distribuzione	<p>I filtri Stato ciclo di vita distribuzione e Stato ultima richiesta possono essere utilizzati singolarmente o in combinazione, in particolare se si gestisce un numero elevato di distribuzioni. Alcuni esempi sono inclusi alla fine della sezione Stato ultima richiesta riportata di seguito.</p> <p>Stato ciclo di vita distribuzione consente di filtrare lo stato corrente della distribuzione in base alle operazioni di gestione.</p> <p>Questo filtro non è disponibile per le distribuzioni eliminate.</p> <p>I valori visualizzati nel riquadro dei filtri dipendono dallo stato corrente delle distribuzioni elencate. Potrebbero non essere visualizzati tutti i valori possibili. L'elenco seguente include tutti i valori possibili. Le azioni del giorno 2 sono incluse nello stato Aggiornamento.</p> <ul style="list-style-type: none"> ■ Creazione - Riuscita ■ Creazione - In corso ■ Creazione - Non riuscita ■ Aggiornamento - Riuscito ■ Aggiornamento - In corso ■ Aggiornamento - Non riuscito ■ Eliminazione - In corso ■ Eliminazione - Non riuscita
Filtri di Stato ultima richiesta	<p>Stato ultima richiesta consente di filtrare l'ultima operazione o azione eseguita nella distribuzione.</p> <p>Questo filtro non è disponibile per le distribuzioni eliminate.</p> <p>I valori visualizzati nel riquadro dei filtri dipendono dalle ultime operazioni eseguite nelle distribuzioni elencate. Potrebbero non essere visualizzati tutti i valori possibili. L'elenco seguente contiene tutti i valori possibili.</p> <ul style="list-style-type: none"> ■ In sospeso. La prima fase di una richiesta in cui l'azione viene inviata ma il processo di distribuzione non è ancora stato avviato. ■ Non riuscita. Si è verificato un errore della richiesta durante una fase qualsiasi del processo di distribuzione. ■ Annullata. La richiesta è stata annullata da un utente mentre il processo di distribuzione era in fase di elaborazione e non era ancora stato completato. ■ Riuscita. La richiesta ha creato, aggiornato o eliminato una distribuzione.

Tabella 7-1. Informazioni sul filtro selezionato (continua)

Nome del filtro	Descrizione
	<ul style="list-style-type: none"> ■ In corso. Il processo di distribuzione è attualmente in esecuzione. Gli stati di distribuzione aggiuntivi, ad esempio Inizializzazione e Completamento visualizzati nella scheda Cronologia della distribuzione non vengono forniti come filtri, ma è possibile utilizzare il filtro In corso per individuare le distribuzioni che hanno tali stati. ■ Approvazione in sospeso. La richiesta ha attivato uno o più criteri di approvazione. Il processo è in attesa di una risposta alla richiesta di approvazione. ■ Approvazione rifiutata. La richiesta è stata rifiutata dagli approvatori nei criteri di approvazione attivati. La richiesta non continua. <p>Gli esempi seguenti illustrano come utilizzare i filtri di Stato ciclo di vita distribuzione e Stato ultima richiesta singolarmente o insieme.</p> <ul style="list-style-type: none"> ■ Per trovare tutte le richieste di eliminazione non riuscite, selezionare Eliminazione - Non riuscita nel filtro Stato ciclo di vita distribuzione. ■ Per trovare tutte le richieste in attesa di approvazione, selezionare Approvazione in sospeso nel filtro Stato ultima richiesta. ■ Per trovare le richieste di eliminazione in cui la richiesta di approvazione è ancora in sospeso, selezionare Eliminazione - In corso nel filtro Stato ciclo di vita distribuzione e Approvazione in sospeso nel filtro Stato ultima richiesta.

Come monitorare le distribuzioni in Cloud Assembly

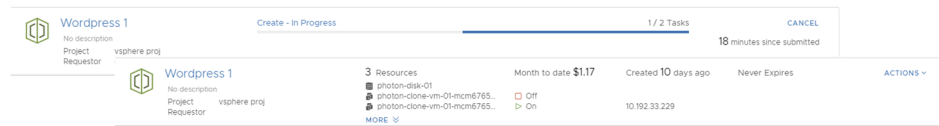
Dopo aver distribuito un modello cloud di Cloud Assembly, è possibile monitorare la richiesta per assicurarsi che le risorse siano sottoposte a provisioning e in esecuzione. A partire dalla scheda di distribuzione, è possibile verificare il provisioning delle risorse. Successivamente, è possibile esaminare i dettagli della distribuzione. Infine, è possibile visualizzare e filtrare le distribuzioni eliminate fino a 90 giorni dopo l'eliminazione.

Procedura

- 1 Selezionare **Risorse > Distribuzioni** e individuare la distribuzione utilizzando il filtro e la ricerca, se necessario.

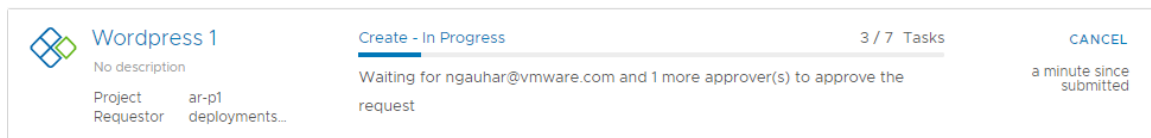
2 Rivedere lo stato della scheda.

Se la distribuzione è in corso, la barra di avanzamento indica il numero di attività rimanenti. Se la distribuzione è stata completata correttamente, la scheda mostra i dettagli di base relativi



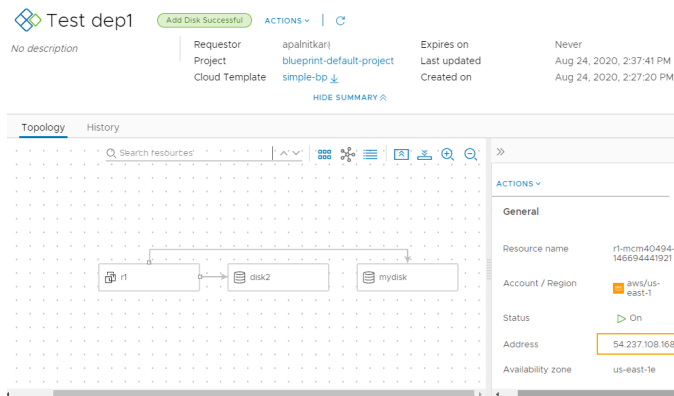
alla distribuzione.

Se per la richiesta viene attivato un criterio di approvazione, è possibile che la richiesta abbia lo stato "in corso" con il nome di almeno un approvatore. I criteri di approvazione sono definiti in Service Broker dall'amministratore. Gli approvatori sono definiti nel criterio. Gli approvatori approvano le richieste in Service Broker. Possono essere presenti anche le approvazioni per le azioni del giorno 2.



3 Per determinare dove sono state distribuite le risorse, fare clic sul nome della distribuzione ed esaminare i dettagli nella pagina Topologia.

Sarà probabilmente necessario l'indirizzo IP del componente primario. Quando si fa clic su un componente, vengono visualizzate informazioni specifiche del componente. In questo esempio viene evidenziato l'indirizzo IP.



La disponibilità del collegamento esterno dipende dal provider di cloud. Quando sono disponibili, è necessario disporre delle credenziali relative a tale provider per accedere al componente.

Operazioni successive

- È possibile apportare modifiche alla distribuzione. Vedere [Come gestire il ciclo di vita di una distribuzione di Cloud Assembly completata](#).
- Se la distribuzione non riesce, vedere [Che cosa è possibile fare se una distribuzione Cloud Assembly non riesce](#).

Che cosa è possibile fare se una distribuzione Cloud Assembly non riesce

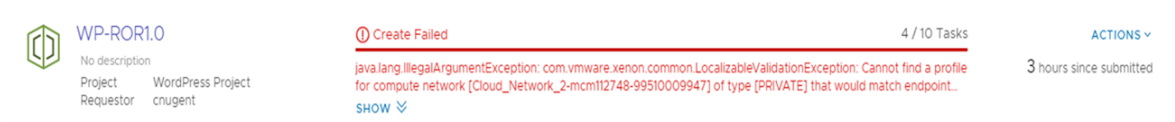
La richiesta di distribuzione potrebbe non riuscire per numerosi motivi. Potrebbe essere dovuto al traffico di rete, a una mancanza di risorse nel provider cloud di destinazione o a una specifica di distribuzione errata. Oppure, è possibile che la distribuzione sia stata completata, ma la distribuzione non sembra funzionare. È possibile utilizzare Cloud Assembly per esaminare la distribuzione ed eventuali messaggi di errore, e determinare se il problema è rappresentato dall'ambiente, dalla specifica di carico di lavoro richiesto o da qualcos'altro.

È possibile utilizzare questo workflow per iniziare l'indagine. Il processo potrebbe indicare che l'errore è dovuto a un problema ambientale temporaneo. La ridistribuzione della richiesta dopo la verifica del miglioramento delle condizioni risolve questo tipo di problema. In altri casi, è possibile che l'indagine richieda di esaminare in dettaglio altre aree.

In qualità di membro di un progetto, è possibile rivedere i dettagli della richiesta in Cloud Assembly.

Procedura

- 1 Per determinare se una richiesta non è andata a buon fine, selezionare **Risorse > Distribuzioni** e individuare la scheda della distribuzione.



Le distribuzioni non riuscite sono indicate sulla scheda.

- a Esaminare il messaggio di errore.
- b Per ulteriori informazioni, fare clic sul nome della distribuzione per visualizzarne i dettagli.

2 Nella pagina dei dettagli della distribuzione, fare clic sulla scheda **Cronologia**.

WP - ROR2 Create Failed ACTIONS ⌵ ⌵

No description

Requestor: fritz
Project: Tiger Team
Cloud Template: WordPress Template [⌵](#)

Expires on: Never
Last updated: Sep 9, 2020, 12:06:42 PM
Created on: Sep 9, 2020, 12:06:38 PM

[HIDE SUMMARY](#)

Topology **History**

Sep 9, 2020, 12:06:42 PM ! CREATE fritz 2.a

Create Failed Requested by: fritz [Provisioning diagram](#) 2.c

Events Request details

Timestamp	Status	Resource type	Resource name	Details 2.b
Sep 9, 2020, ...	REQUEST_FAILED			Could not find any profile to match network 'WP-Network-Private' of type 'EXISTING' with constraints '[type:isolated-net, env:dev]'.
Sep 9, 2020, ...	COMPLETION_FINISHED			
Sep 9, 2020, ...	COMPLETION_IN_PROGRE...			
Sep 9, 2020, ...	ALLOCATE_FAILED	Cloud.Network	WP-Network-Private	Could not find any profile to match...

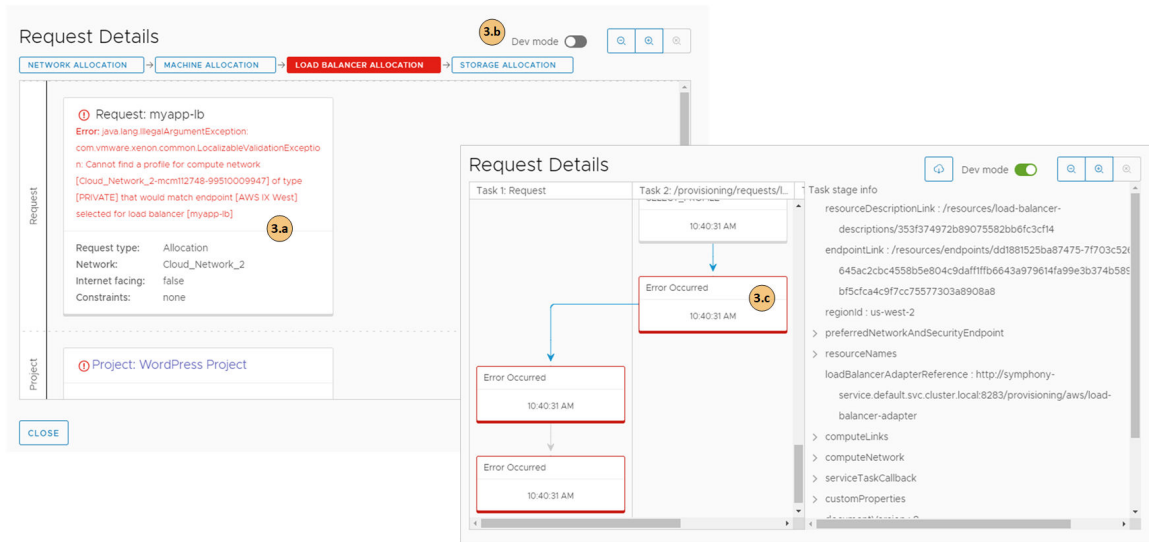
8 Events

- Esaminare l'albero degli eventi per vedere in che punto non è riuscito il processo di provisioning. Questo albero è utile quando si modifica una distribuzione, ma la modifica non riesce.

L'albero mostra anche quando si eseguono le azioni di distribuzione. È possibile utilizzare l'albero per risolvere i problemi relativi alle modifiche non riuscite.
 - In **Dettagli** è presente una versione più dettagliata del messaggio di errore.
 - Se l'elemento richiesto è un modello cloud di Cloud Assembly, il collegamento a destra del messaggio apre Cloud Assembly in modo da poter visualizzare i **Dettagli richiesta**.
- 3** In **Dettagli richiesta** è disponibile il workflow di provisioning per i componenti non riusciti che consente di cercare il problema.

La cronologia delle richieste viene conservata per 48 ore.

Visualizzazione e filtro della cronologia delle distribuzioni eliminate fino a 90 giorni dopo l'eliminazione

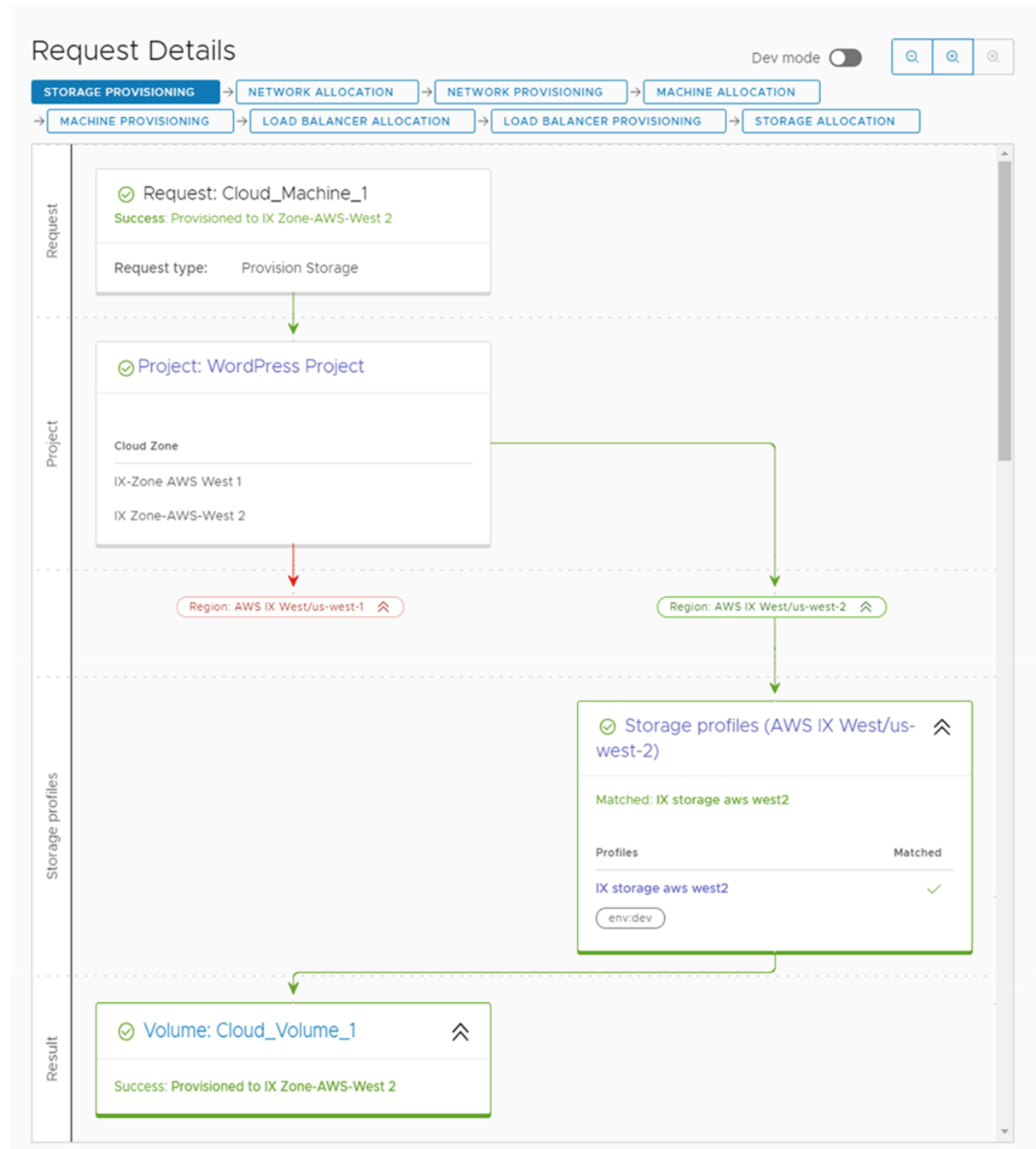


- a Esaminare il messaggio di errore.
 - b È possibile attivare la **Modalità sviluppo** per passare da un workflow di provisioning semplice a un diagramma di flusso più dettagliato.
 - c Fare clic sulla scheda per esaminare lo script di distribuzione.
- 4 Risolvere gli errori e ridistribuire il modello cloud.

Gli errori potrebbero trovarsi nella costruzione del modello o essere correlati al modo in cui l'infrastruttura è configurata.

Operazioni successive

Quando gli errori vengono risolti e il modello cloud viene distribuito, è possibile visualizzare informazioni simili al seguente esempio in Dettagli richiesta. Per visualizzare i dettagli della richiesta, selezionare **Infrastruttura > Attività > Richieste**.



Come gestire il ciclo di vita di una distribuzione di Cloud Assembly completata

Dopo il provisioning e l'esecuzione di una distribuzione, è possibile eseguire varie azioni per gestire la distribuzione. La gestione del ciclo di vita può includere l'attivazione o la disattivazione, il ridimensionamento e l'eliminazione di una distribuzione. È inoltre possibile eseguire varie azioni sui singoli componenti per gestirli.

Procedura

- 1 Selezionare **Risorse > Distribuzioni** e individuare la distribuzione.
- 2 Per accedere ai dettagli della distribuzione, fare clic sul nome della distribuzione.

I dettagli della distribuzione vengono utilizzati per capire in che modo le risorse vengono distribuite e quali modifiche sono state apportate. È inoltre possibile visualizzare informazioni sui prezzi, lo stato corrente della distribuzione e le eventuali risorse che devono essere modificate.

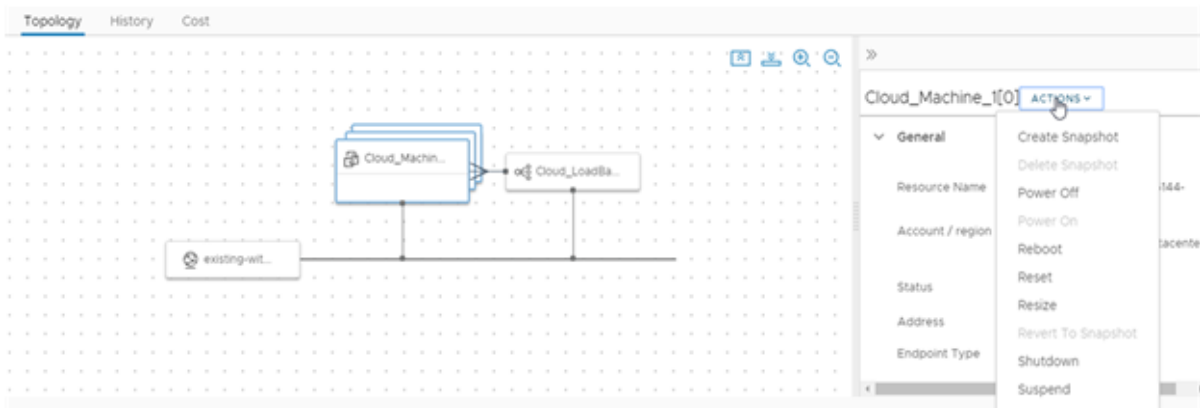
The image displays a sequence of overlapping screenshots from the vRealize Automation Cloud Assembly user interface, illustrating different functional areas:

- Topology View:** Shows a hierarchical view of cloud resources, including Cloud_vSphere_Machine_1[0] and Cloud_vSphere_Machine_1[1], with options to view attached volumes and actions.
- History View:** Displays a 'Create' event log with columns for Timestamp, Status, Resource type, Resource name, and Details. It shows successful provisioning events for Cloud_vSphere_Machine_1.
- Price View:** Provides a 'Price analysis' section with tabs for Overall and Details. It includes a bar chart showing price trends over time, with a price of \$0.38 per month.
- Monitor View:** Offers a detailed view of resource usage for specific VMs. It includes a table for CPU, Memory, and Storage usage, and a line graph showing CPU usage over time.
- Alerts View:** Displays a list of alerts, including 'Definition_Deployment_VM' and 'AlertDefinition_Deployment_has_cost', with filters for severity and status.
- Optimize View:** Shows a summary of 'Underutilized VMs' and a table detailing VM status, allocated CPU, memory, and storage.

- **Scheda Topologia.** È possibile utilizzare la scheda Topologia per comprendere la struttura e le risorse della distribuzione.
- **Scheda Cronologia.** La scheda Cronologia include tutti gli eventi di provisioning e tutti gli eventi correlati alle azioni eseguite dopo la distribuzione dell'elemento richiesto. Se si verificano problemi relativi al processo di provisioning, gli eventi della scheda Cronologia consentiranno di correggere gli errori.

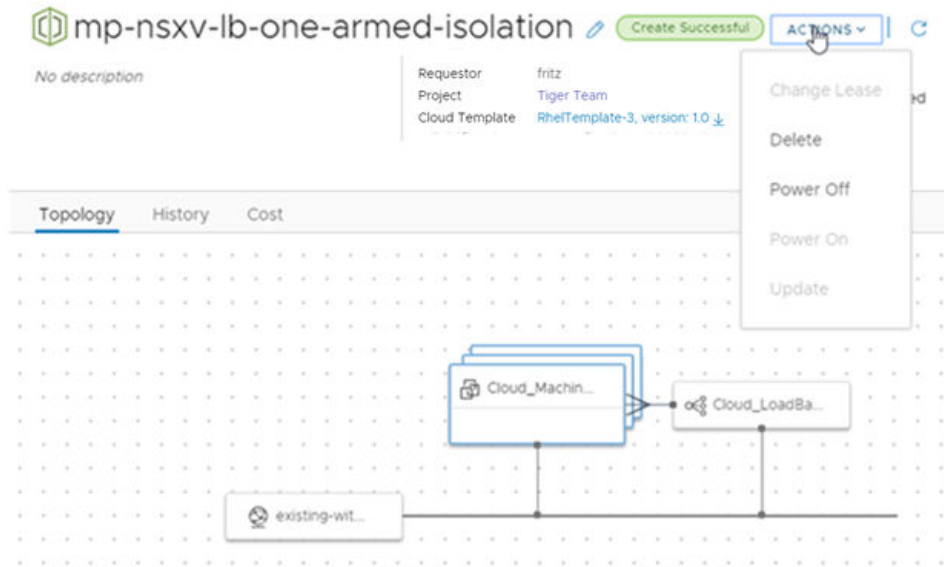
- Scheda **Prezzi**. È possibile utilizzare la scheda Prezzi per comprendere il costo della distribuzione in uso per l'organizzazione. Le informazioni sui prezzi si basano sulle integrazioni di vRealize Operations Manager o CloudHealth.
 - Scheda **Monitora**. La scheda Monitora fornisce informazioni sull'integrità della distribuzione in base ai dati provenienti da vRealize Operations Manager.
 - Scheda **Avvisi**. La scheda Avvisi fornisce avvisi attivi sulle risorse di distribuzione. È possibile ignorare l'avviso o aggiungere note di riferimento. Gli avvisi si basano sui dati recuperati da vRealize Operations Manager.
 - Scheda **Ottimizza**. La scheda Ottimizza fornisce informazioni sull'utilizzo della distribuzione e offre suggerimenti per recuperare o modificare in altro modo le risorse per ottimizzare il consumo di risorse. Le informazioni sull'ottimizzazione si basano sui dati provenienti da vRealize Operations Manager.
- 3 Se si determina che una distribuzione è troppo costosa nella configurazione corrente e si desidera ridimensionare un componente, selezionare il componente nella pagina Topologia, quindi selezionare **Azioni > Ridimensiona** nella pagina del componente.

Le azioni disponibili dipendono dal componente, dall'account cloud e dalle autorizzazioni di cui si dispone.



- 4 Come parte del ciclo di vita dello sviluppo, una delle distribuzioni non è più necessaria. Per rimuovere la distribuzione e recuperare le risorse, selezionare **Azioni > Elimina**.

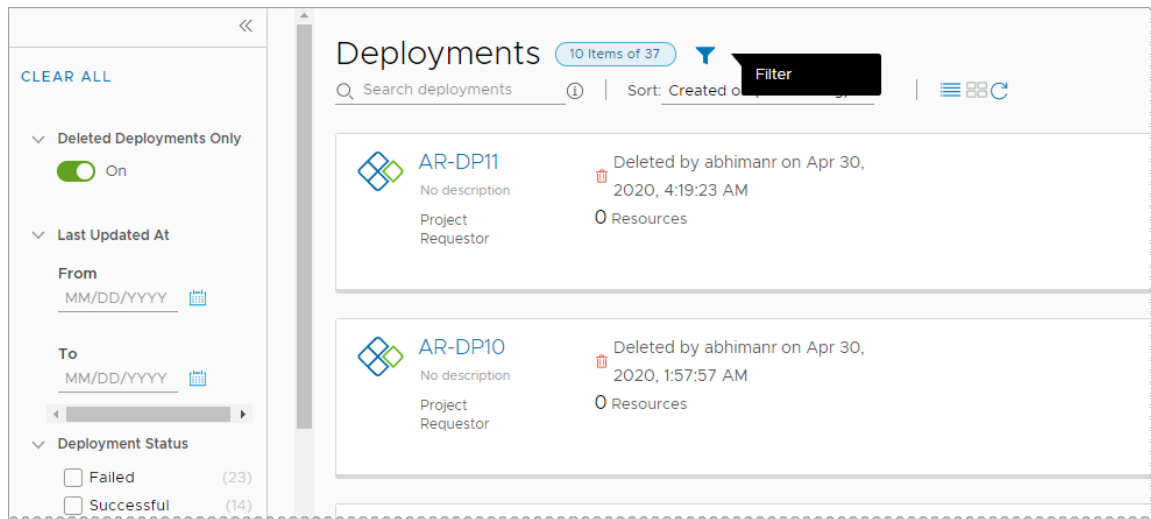
Le azioni disponibili dipendono dallo stato della distribuzione.



- Per visualizzare le distribuzioni eliminate, fare clic sul filtro nella pagina **Distribuzioni** e quindi attivare l'interruttore **Solo distribuzioni eliminate**.

L'elenco delle distribuzioni è ora limitato a quelle eliminate. È possibile che si desideri rivedere la cronologia di una distribuzione specifica. Ad esempio per recuperare il nome di una macchina eliminata.

Le distribuzioni eliminate sono elencate per 90 giorni.



Operazioni successive

Per ulteriori informazioni sulle possibili azioni, vedere [Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly](#).

Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly

Dopo aver distribuito i modelli cloud, è possibile eseguire azioni in Cloud Assembly per gestire le risorse. Le azioni disponibili dipendono dal tipo di risorsa e dal fatto che le azioni siano supportate in un account cloud o una piattaforma specifici.

Le azioni disponibili dipendono anche da ciò che l'amministratore ha autorizzato a eseguire.

In qualità di amministratore o amministratore del progetto, è possibile impostare i criteri delle azioni giorno 2 in Service Broker. Vedere [Come autorizzare i consumatori per i criteri di azione giorno 2 di Service Broker](#)

Potrebbero essere visualizzate anche azioni non incluse nell'elenco. Si tratta probabilmente di azioni personalizzate aggiunte dall'amministratore. Ad esempio, un'[Come creare un'azione risorsa di Cloud Assembly in una macchina virtuale vMotion](#).

Tabella 7-2. Elenco di azioni possibili

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Aggiungi disco	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordine 	<p>Aggiungere altri dischi alle macchine virtuali esistenti.</p> <p>Se si aggiunge un disco a una macchina Azure, il disco persistente o il disco non persistente viene distribuito nel gruppo di risorse che include la macchina.</p> <p>Quando si aggiunge un disco a una macchina Azure, è anche possibile crittografare il nuovo disco utilizzando il set di crittografia del disco di Azure nel profilo di storage.</p> <p>Non è possibile aggiungere un disco a una macchina Azure con un disco non gestito.</p> <p>Quando si aggiunge un disco alle macchine vSphere, è possibile selezionare il controller SCSI, il cui ordine è stato impostato nel modello cloud e distribuito. È inoltre possibile specificare il numero di unità per il nuovo disco. Non è possibile specificare un numero di unità senza un controller selezionato. Se non si seleziona un controller o non si specifica un numero di unità, il nuovo disco viene distribuito al primo controller disponibile e gli viene assegnato il numero di unità successivo disponibile in tale controller.</p> <p>Se si aggiunge un disco a una macchina vSphere per un progetto con limiti di storage definiti, il disco aggiunto non deve superare i limiti di storage.</p> <p>Se si utilizza VMware Storage DRS (SDRS) e il cluster di datastore è configurato nel profilo di storage, è possibile aggiungere dischi in SDRS nelle macchine vSphere.</p>
Applica configurazione Salt	Macchine	<ul style="list-style-type: none"> ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordine 	<p>Installare un minion Salt o aggiornare la configurazione Salt su una macchina virtuale.</p> <p>L'opzione Applica configurazione Salt è disponibile se è stata configurata l'integrazione di SaltStack Config.</p> <hr/> <p>Nota Prima di usare questo metodo per installare il minion Salt, esiste un'opzione più robusta quando si include il minion nel modello cloud. Il metodo del modello include un tipo di risorsa SaltStack Config nella distribuzione. Per ulteriori informazioni, vedere Aggiunta della risorsa SaltStack Config a modelli.</p> <hr/> <p>Per applicare una configurazione, è necessario selezionare un metodo di autenticazione. L'opzione Accesso remoto con credenziali esistenti utilizza le credenziali di accesso remoto incluse nella distribuzione. Se dopo la distribuzione sono state modificate le credenziali della macchina, è possibile che l'azione non riesca. Se si conoscono le nuove credenziali, utilizzare il metodo di autenticazione Password.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
				<p>Le opzioni Password e Chiave privata utilizzano il nome utente e la password o la chiave per convalidare le credenziali e quindi connettersi alla macchina virtuale mediante il protocollo SSH.</p> <p>Se non si specifica un valore per ID master e ID minion, Salt crea tali valori automaticamente.</p>
Annulla	<ul style="list-style-type: none"> ■ Distribuzioni ■ Vari tipi di risorse nelle distribuzioni 	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordinamento 	<p>Annulla una distribuzione o un'azione del giorno 2 in una distribuzione o una risorsa durante l'elaborazione della richiesta.</p> <p>È possibile annullare la richiesta nella scheda della distribuzione o nei dettagli della distribuzione. Dopo l'annullamento, la richiesta viene visualizzata come richiesta non riuscita nella pagina Distribuzioni. Utilizzare l'azione Elimina per rilasciare tutte le risorse distribuite e ripulire l'elenco di distribuzione.</p> <p>L'annullamento di una richiesta che si ritiene sia stata in esecuzione troppo a lungo è un metodo per gestire il tempo di distribuzione. Tuttavia, è più efficiente impostare il valore di Timeout richiesta nei progetti. Il timeout predefinito è di due ore. È possibile impostare un valore di tempo più lungo se la distribuzione del carico di lavoro per un progetto richiede più tempo.</p>
Modifica lease	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordinamento 	<p>Modificare la data e l'ora di scadenza del lease.</p> <p>Quando un lease scade, la distribuzione viene eliminata e le risorse vengono recuperate.</p> <p>I criteri di lease sono impostati in Service Broker.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Cambia proprietario	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordinamento 	<p>Modifica del proprietario della distribuzione per l'utente selezionato. L'utente selezionato in qualità di singolo utente o membro di un gruppo deve essere un amministratore o membro dello stesso progetto che ha distribuito la richiesta.</p> <p>Quando un progettista di modelli cloud distribuisce un modello, il progettista è sia il richiedente sia il proprietario. Tuttavia, un richiedente può rendere proprietario un altro membro del progetto.</p> <p>È possibile utilizzare criteri per controllare ciò che un proprietario può fare con una distribuzione, assegnandogli autorizzazioni più o meno restrittive.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Modifica del progetto	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ NSX-T ■ NSX-V ■ VMware Cloud Director ■ VMware Cloud Foundation ■ VMware Cloud on AWS ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	<p>L'azione di modifica del progetto consente di spostare una distribuzione da un progetto a un altro.</p> <p>L'azione di modifica del progetto è disponibile per le distribuzioni con risorse distribuite e le distribuzioni con risorse sottoposte a onboarding. Questa azione non è supportata per le distribuzioni che contengono sia risorse sottoposte a onboarding sia risorse distribuite. L'azione non è disponibile per le distribuzioni migrate.</p> <p>Le risorse supportate includono i seguenti tipi di risorse e vincoli:</p> <ul style="list-style-type: none"> ■ Le distribuzioni con risorse distribuite possono contenere macchine virtuali, dischi, bilanciamenti del carico, reti, gruppi di sicurezza, gruppi di Azure, NAT e gateway. ■ Le distribuzioni con risorse sottoposte a onboarding possono contenere macchine virtuali, dischi e reti. ■ Se si aggiunge un tipo di risorsa non supportato a un tipo di distribuzione o all'altro, con risorse distribuite o con risorse sottoposte a onboarding, non è possibile eseguire l'azione di modifica del progetto. Ad esempio, se si aggiunge una configurazione Terraform a una distribuzione, l'azione di modifica del progetto non è disponibile. <p>Ruoli, considerazioni e vincoli per le distribuzioni con risorse distribuite:</p> <ul style="list-style-type: none"> ■ Per modificare il progetto di una distribuzione con risorse distribuite, l'utente che avvia la modifica deve disporre del ruolo seguente: <ul style="list-style-type: none"> ■ Amministratore del cloud. ■ È possibile modificare il progetto solo quando il progetto di destinazione contiene tutte le zone cloud in cui sono distribuite le macchine e i dischi della distribuzione. La distribuzione spostata è quindi soggetta ai limiti configurati per il progetto di destinazione, inclusi il numero delle istanze, la memoria, la CPU e lo storage. Dopo lo spostamento, l'utilizzo corrente viene rilasciato dal progetto di origine. ■ Dopo aver spostato una distribuzione nel progetto di destinazione, è soggetta ai criteri del progetto di destinazione. Ad esempio, lease, azioni giorno 2, quota della risorsa e altri criteri.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
				<p>Per spostare una distribuzione, il lease della distribuzione definito dal criterio di lease del progetto di destinazione non può scadere nelle 24 ore successive.</p> <p>Ruoli, considerazioni e vincoli per le distribuzioni con risorse sottoposte a onboarding:</p> <ul style="list-style-type: none"> ■ Per spostare una distribuzione con risorse sottoposte a onboarding, l'utente che avvia lo spostamento deve disporre di almeno uno dei seguenti ruoli: <ul style="list-style-type: none"> ■ Amministratore del cloud. ■ Autorizzazione Gestisci distribuzioni. Questa autorizzazione può essere definita come un ruolo personalizzato. ■ Amministratore del progetto di destinazione. ■ Il membro del progetto di destinazione e le distribuzioni vengono condivise tra tutti gli utenti nel progetto di destinazione. ■ Anche se è possibile spostare le risorse sottoposte a onboarding in un progetto che non contiene le stesse zone cloud, se il progetto di destinazione non dispone delle stesse zone cloud, tutte le azioni giorno 2 future che coinvolgono le risorse dell'account cloud o delle regioni che vengono eseguite potrebbero non funzionare. <p>Considerazioni generali:</p> <ul style="list-style-type: none"> ■ Se si è un amministratore che sposta la distribuzione, è possibile che si sposti la distribuzione in un progetto in cui il proprietario non è un membro e pertanto perde l'accesso. È possibile aggiungere il proprietario al progetto di destinazione o spostare la distribuzione in un progetto di cui è membro.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Modifica gruppi di sicurezza	Macchine	■ VMware vSphere	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	<p>È possibile associare e dissociare i gruppi di sicurezza a reti di macchine in una distribuzione. L'azione di modifica si applica ai gruppi di sicurezza esistenti e su richiesta per NSX-V e NSX-T. Questa azione è disponibile solo per le singole macchine e non per i cluster di macchine.</p> <p>Per associare un gruppo di sicurezza alla rete di macchine, è necessario che il gruppo di sicurezza sia presente nella distribuzione.</p> <p>La dissociazione di un gruppo di sicurezza da tutte le reti di tutte le macchine in una distribuzione non rimuove il gruppo di sicurezza dalla distribuzione.</p> <p>Queste modifiche non influiscono sui gruppi di sicurezza applicati come parte dei profili di rete.</p> <p>Questa azione modifica la configurazione del gruppo di sicurezza della macchina senza ricreare la macchina. Si tratta di una modifica non distruttiva.</p> <ul style="list-style-type: none"> ■ Per modificare la configurazione del gruppo di sicurezza della macchina, selezionare la macchina nel riquadro della topologia, quindi fare clic sul menu Azione nel riquadro destro e selezionare Modifica gruppi di sicurezza. A questo punto è possibile aggiungere o rimuovere l'associazione dei gruppi di sicurezza alle reti di macchine.
Connetti a console remota	Macchine	■ VMware vSphere	<ul style="list-style-type: none"> ■ Distribuita ■ Rilevata ■ Di cui è stato eseguito l'onboarding 	<p>Aprire una sessione remota nella macchina selezionata.</p> <p>Rivedere i seguenti requisiti per stabilire la connessione correttamente.</p> <ul style="list-style-type: none"> ■ In qualità di consumatore della distribuzione, verificare che la macchina sottoposta a provisioning sia accesa.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Creazione dello snapshot del disco	Macchine e dischi	<ul style="list-style-type: none"> Microsoft Azure 	<ul style="list-style-type: none"> Distribuita Dal cui stato è eseguito l'ordinamento 	<p>Creazione dello snapshot di un disco di una macchina virtuale o di un disco di storage.</p> <ul style="list-style-type: none"> Per le macchine, è possibile creare snapshot per singoli dischi della macchina, inclusi i dischi di avvio, i dischi immagine e i dischi di storage. Per i dischi di storage, si creano snapshot di dischi gestiti indipendenti, non di dischi non gestiti. <p>Oltre a specificare un nome per lo snapshot, è anche possibile fornire le seguenti informazioni per lo snapshot:</p> <ul style="list-style-type: none"> Snapshot incrementale. Selezionare la casella di controllo per creare uno snapshot delle modifiche dall'ultimo snapshot anziché da uno snapshot completo. Gruppo di risorse. Immettere il nome del gruppo di risorse di destinazione in cui si desidera creare lo snapshot. Per impostazione predefinita, lo snapshot viene creato nello stesso gruppo di risorse utilizzato dal disco principale. ID set di crittografia. Selezionare la chiave di crittografia per lo snapshot. Per impostazione predefinita, lo snapshot viene crittografato con la stessa chiave utilizzata dal disco principale. Tag. Immettere i tag che consentiranno di gestire gli snapshot in Microsoft Azure.
Creazione dello snapshot	Macchine	<ul style="list-style-type: none"> Google Cloud Platform VMware vSphere 	<ul style="list-style-type: none"> Distribuita Dal cui stato è eseguito l'ordinamento 	<p>Creazione di uno snapshot della macchina virtuale.</p> <p>Se sono consentiti solo due snapshot in vSphere e sono già stati creati entrambi, il comando diventa disponibile solo dopo l'eliminazione di uno snapshot.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Elimina i	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	<p>Eliminazione di una distribuzione.</p> <p>Tutte le risorse vengono eliminate e recuperate. Se l'eliminazione non riesce, è possibile eseguire l'azione di eliminazione in una distribuzione una seconda volta. Durante il secondo tentativo, è possibile selezionare Ignora errori di eliminazione. Se si seleziona questa opzione, la distribuzione viene eliminata, ma le risorse potrebbero non essere recuperate. È necessario controllare i sistemi in cui è stato eseguito il provisioning della distribuzione per assicurarsi che tutte le risorse vengano rimosse. In caso contrario, è necessario eliminare manualmente le risorse rimanenti in tali sistemi.</p>
	Gateway NSX	<ul style="list-style-type: none"> ■ NSX 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	Eliminare le regole di inoltro della porta NAT da un gateway di NSX-T o NSX-V.
	Macchine e bilanciamenti del carico	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere ■ VMware NSX 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	Rimuovere una macchina o un bilanciamento del carico da una distribuzione. Questa azione potrebbe comportare una distribuzione non utilizzabile.

Tabella 7-2. Elenco di azioni possibili (continua)

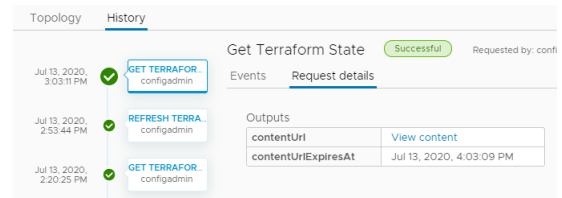
Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
	Gruppi di sicurezza	<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'onboarding 	<p>Se il gruppo di sicurezza non è associato ad alcuna macchina nella distribuzione, il processo rimuove il gruppo di sicurezza dalla distribuzione.</p> <ul style="list-style-type: none"> ■ Se il gruppo di sicurezza è su richiesta, viene eliminato nell'endpoint. ■ Se il gruppo di sicurezza è condiviso, l'azione non riesce.
	Cluster di Tanzu Kubernetes	<ul style="list-style-type: none"> ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'onboarding 	Rimuovere un cluster Tanzu Kubernetes da una distribuzione.
Eliminazione dello snapshot del disco	Macchine e dischi	<ul style="list-style-type: none"> ■ Microsoft Azure 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'onboarding 	<p>Eliminare uno snapshot del disco della macchina virtuale Azure o di un disco gestito.</p> <p>Questa azione è disponibile quando è presente almeno uno snapshot.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Elimina snapshot	Macchine	<ul style="list-style-type: none"> ■ VMware vSphere ■ Google Cloud Platform 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originale 	Eliminazione di uno snapshot della macchina virtuale.
Disabilita diagnostica all'avvio	Macchine	<ul style="list-style-type: none"> ■ Microsoft Azure 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originale 	<p>Disattivare la funzionalità di debug della macchina virtuale Azure.</p> <p>L'opzione Disabilita è disponibile solo se la funzionalità è attivata.</p>
Modifica tag	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originale 	Aggiungere o modificare i tag di risorsa applicati alle singole risorse di distribuzione.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Abilita diagnostica all'avvio	Macchine	<ul style="list-style-type: none"> Microsoft Azure 	<ul style="list-style-type: none"> Distribuita Dal cui stato è eseguito l'onboarding 	<p>Attivare la funzionalità di debug della macchina virtuale Azure per diagnosticare gli errori di avvio delle macchine virtuali. Le informazioni di diagnostica all'avvio sono disponibili nella console di Azure.</p> <p>L'opzione Abilita è disponibile solo se la funzionalità non è al momento attivata.</p>
Ottieni stato Terraform	Configurazione Terraform	<ul style="list-style-type: none"> Amazon Web Service Google Cloud Platform Microsoft Azure VMware vSphere 	<ul style="list-style-type: none"> Distribuita Dal cui stato è eseguito l'onboarding 	<p>Visualizzare il file dello stato di Terraform.</p> <p>Per visualizzare tutte le modifiche apportate alle macchine Terraform nelle piattaforme cloud su cui sono state distribuite e aggiornare la distribuzione, è innanzitutto necessario eseguire l'azione Aggiorna stato Terraform e quindi eseguire l'azione Ottieni stato Terraform.</p> <p>Quando il file viene visualizzato in una finestra di dialogo. Il file è disponibile per circa 1 ora prima che sia necessario eseguire una nuova azione di aggiornamento. È possibile copiarlo se si intende utilizzarlo in un secondo momento.</p> <p>È inoltre possibile visualizzare il file nella scheda Cronologia della distribuzione. Selezionare l'evento Ottieni stato Terraform nella scheda Eventi, quindi fare clic su Dettagli richiesta. Se il file non è scaduto, fare clic su Visualizza contenuto. Se il file è scaduto, eseguire nuovamente le azioni Aggiorna e Ottieni.</p>



È possibile eseguire altre azioni del giorno 2 relative alle risorse di Terraform incorporate nella configurazione. Le azioni disponibili dipendono dal tipo di risorsa, dalla piattaforma cloud su cui sono distribuite e dal fatto che l'utente abbia o meno il permesso di eseguire le azioni in base a un criterio del giorno 2.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Spegni	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Rilevata ■ Di cui è stato eseguito l'onboarding 	Spegnere la distribuzione dopo il primo tentativo di shutdown dei sistemi operativi guest. Se lo spegnimento temporaneo non riesce, viene ancora eseguito uno spegnimento a freddo.
	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	Spegnere la macchina dopo il primo tentativo di spegnimento dei sistemi operativi guest. Se lo spegnimento temporaneo non riesce, viene ancora eseguito uno spegnimento a freddo.
Accendi	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	Accensione della distribuzione. Se le risorse sono state sospese, il funzionamento normale riprende dal punto in cui erano state sospese.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Rilevata ■ Di cui è stato eseguito l'onboarding 	Accensione della macchina. Se la macchina è stata sospesa, il funzionamento normale riprende dal punto in cui la macchina è stata sospesa.
Riavvia	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	<p>Riavvio del sistema operativo guest su una macchina virtuale.</p> <p>Nel caso di una macchina vSphere, VMware Tools deve essere installato nella macchina per poter eseguire questa azione.</p>
Riconfigura	Bilanciamenti del carico	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware NSX 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	<p>Modificare le dimensioni del bilanciamento del carico e il livello di registrazione.</p> <p>È inoltre possibile aggiungere o rimuovere route e modificare le impostazioni relative a protocollo, porta, configurazione dell'integrità e pool di membri.</p> <p>Per i bilanciamenti del carico NSX, è possibile abilitare o disabilitare il controllo dello stato di integrità e modificare le opzioni di integrità. Per NSX-T, è possibile impostare il controllo su attivo o passivo. NSX-V non supporta controlli dello stato passivi.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Inoltro della porta di NSX Gateway		<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originando 	Aggiungere, modificare o eliminare le regole di inoltro della porta NAT da un gateway di NSX-T o NSX-V.
Gruppi di sicurezza		<ul style="list-style-type: none"> ■ NSX-T ■ NSX-V ■ VMware Cloud ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originando 	<p>Aggiungere, modificare o rimuovere le regole o i vincoli del firewall in base al fatto che il gruppo di sicurezza sia un gruppo di sicurezza su richiesta o esistente.</p> <ul style="list-style-type: none"> ■ Gruppo di sicurezza su richiesta <p>Aggiungere, modificare o rimuovere le regole del firewall per i gruppi di sicurezza su richiesta di NSX-T e VMware Cloud.</p> <ul style="list-style-type: none"> ■ Per aggiungere o rimuovere una regola, selezionare il gruppo di sicurezza nel riquadro della topologia, fare clic sul menu Azione nel riquadro destro e selezionare Riconfigura. A questo punto è possibile aggiungere, modificare o rimuovere le regole. ■ Gruppo di sicurezza esistente <p>Aggiungere, modificare o rimuovere i vincoli per i gruppi di sicurezza esistenti di NSX-V, NSX-T e VMware Cloud.</p> <ul style="list-style-type: none"> ■ Per aggiungere o rimuovere un vincolo, selezionare il gruppo di sicurezza nel riquadro della topologia, fare clic sul menu Azione nel riquadro destro e selezionare Riconfigura. A questo punto è possibile aggiungere, modificare o rimuovere i vincoli.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Aggiorna stato Terraform	Configurazione Terraform	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordinamento 	<p>Recuperare l'iterazione più recente del file dello stato di Terraform.</p> <p>Per recuperare tutte le modifiche apportate alle macchine Terraform nelle piattaforme cloud su cui sono state distribuite e aggiornare la distribuzione, è innanzitutto necessario eseguire l'azione Aggiorna stato Terraform.</p> <p>Per visualizzare il file, eseguire l'azione Ottieni stato Terraform sulla configurazione.</p> <p>Utilizzare la scheda della cronologia della distribuzione per monitorare il processo di aggiornamento.</p>
Rimuovi disco	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordinamento 	<p>Rimuovere i dischi dalle macchine virtuali esistenti.</p> <p>Se si esegue l'azione giorno 2 in una distribuzione distribuita come macchine e dischi vSphere, il conteggio dei dischi viene recuperato poiché si applica ai limiti di storage del progetto. I limiti di storage del progetto non si applicano agli ulteriori dischi aggiunti dopo la distribuzione come azione giorno 2.</p>
Reimposta	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'ordinamento 	<p>Riavvio forzato di una macchina virtuale senza shutdown del sistema operativo guest.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Ridimensiona	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ Google Cloud Platform ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originando 	Aumento o riduzione della CPU e della memoria di una macchina virtuale.
Ridimensiona disco di avvio	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originando 	<p>Aumentare o diminuire le dimensioni del disco di avvio.</p> <p>Se si esegue l'azione giorno 2 in una distribuzione distribuita come macchine e dischi vSphere, l'azione non riesce e viene visualizzato un messaggio simile a "Lo storage richiesto è di dimensioni superiori rispetto al posizionamento di storage disponibile", ciò è probabilmente dovuto ai limiti di storage definiti nei modelli di macchine virtuali e alla libreria dei contenuti di vSphere definiti nel progetto. I limiti di storage del progetto non si applicano agli ulteriori dischi aggiunti dopo la distribuzione come azione giorno 2.</p>
Ridimensiona disco	Disco di storage	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito o l'originando 	<p>Aumento della capacità di un disco di storage.</p> <p>Se si esegue l'azione giorno 2 in una distribuzione distribuita come macchine e dischi vSphere, l'azione non riesce e viene visualizzato un messaggio simile a "Lo storage richiesto è di dimensioni superiori rispetto al posizionamento di storage disponibile", ciò è probabilmente dovuto ai limiti di storage definiti nei modelli di macchine virtuali e alla libreria dei contenuti di vSphere definiti nel progetto. I limiti di storage del progetto non si applicano agli ulteriori dischi aggiunti dopo la distribuzione come azione giorno 2.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
	Macchine	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Google Cloud Platform ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'originando 	Aumento o diminuzione delle dimensioni dei dischi inclusi nel modello di immagine della macchina e di tutti i dischi collegati.
Riavvia	Macchine	<ul style="list-style-type: none"> ■ Microsoft Azure 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'originando 	Shutdown e riavvio di una macchina in esecuzione.
Ripristina snapshot	Macchine	<ul style="list-style-type: none"> ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'originando 	<p>Ripristino di uno snapshot precedente della macchina.</p> <p>Per utilizzare questa azione è necessario disporre di uno snapshot esistente.</p>

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Esegui attività Puppet	Risorse gestite	■ Puppet Enterprise	■ Distribuita ■ Di cui è stato eseguito l'onboarding	Esecuzione dell'attività selezionata sulle macchine nella distribuzione. Le attività sono definite nell'istanza di Puppet. È necessario essere in grado di identificare l'attività e fornire i parametri di input.
Scalare i nodi di lavoro	Cluster di Tanzu Kubernetes	■ VMware vSphere	■ Distribuita ■ Di cui è stato eseguito l'onboarding	Aumentare o diminuire il numero di macchine virtuali del nodo di lavoro Tanzu Kubernetes nella distribuzione.
Shutdown	Macchine	■ VMware vSphere	■ Distribuita	Shutdown del sistema operativo guest e spegnimento della macchina. Per utilizzare questa azione, è necessario che sulla macchina sia installato VMware Tools.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Sospendi	Macchine	<ul style="list-style-type: none"> ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	Sospensione della macchina in modo che non possa essere utilizzata e non consumi risorse del sistema ad eccezione dello storage che usa.
Aggiorna	Distribuzioni	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	<p>Modifica della distribuzione in base ai parametri di input.</p> <p>Per un esempio, vedere Spostamento di una macchina distribuita in un'altra rete.</p> <p>Se la distribuzione è basata sulle risorse di vSphere e la macchina e i dischi includono l'opzione di conteggio, quando si aumenta il numero potrebbero essere applicati i limiti di storage definiti nel progetto. Se l'azione non riesce e viene visualizzato un messaggio simile a "Lo storage richiesto è di dimensioni superiori rispetto al posizionamento di storage disponibile", ciò è probabilmente dovuto ai limiti di storage definiti nei modelli di macchine virtuali vSphere definiti nel progetto. I limiti di storage del progetto non si applicano agli ulteriori dischi aggiunti dopo la distribuzione come azione giorno 2.</p>
Aggiorna tag	Macchine e dischi	<ul style="list-style-type: none"> ■ Amazon Web Service ■ Microsoft Azure ■ VMware vSphere 	<ul style="list-style-type: none"> ■ Distribuita ■ Di cui è stato eseguito l'onboarding 	Aggiungere, modificare o eliminare un tag applicato a una singola risorsa.

Tabella 7-2. Elenco di azioni possibili (continua)

Azione	Si applica a questi tipi di risorse	Disponibile per questi tipi di cloud	Origine risorsa	Descrizione
Aggiornare la versione Tanzu e Tanzu	Cluster di Tanzu Kubernetes	<ul style="list-style-type: none"> VMware vSphere 	<ul style="list-style-type: none"> Distribuita Dal cui stato eseguito l'onboarding 	Aggiornare la versione Kubernetes corrente a una versione successiva.
Annullamento della registrazione	Macchine	<ul style="list-style-type: none"> Amazon Web Service Google Cloud Platform Microsoft Azure VMware vSphere 	<ul style="list-style-type: none"> Distribuita Dal cui stato eseguito l'onboarding 	<p>L'azione di annullamento della registrazione è disponibile solo per le macchine di distribuzione di cui è stato eseguito l'onboarding.</p> <p>Le macchine di cui viene annullata la registrazione vengono rimosse dalla distribuzione, insieme a tutti i dischi collegati. Rimuovendo le risorse, è possibile eseguire nuovamente il workflow di onboarding per la macchina non registrata. Potrebbe essere necessario eseguire nuovamente l'onboarding della risorsa, questa volta in un nuovo progetto.</p> <p>Se si apportano modifiche alla macchina, ad esempio l'aggiunta di un disco, prima di annullare la registrazione della macchina, l'azione di annullamento della registrazione non riesce.</p>

Gestione delle risorse in Cloud Assembly

L'amministratore del cloud e lo sviluppatore di modelli cloud di Cloud Assembly possono utilizzare la scheda Risorse per gestire le risorse cloud. La scheda Risorse funge da centro risorse in cui è possibile monitorare le risorse tra i cloud, modificarle e persino eliminarle.

È possibile individuare e gestire le risorse utilizzando le diverse visualizzazioni. È possibile filtrare gli elenchi, visualizzare i dettagli delle risorse ed eseguire azioni sui singoli elementi. Le azioni disponibili dipendono dallo stato della risorsa e dai criteri del giorno 2.

Se si è un amministratore di Cloud Assembly, è inoltre possibile visualizzare e gestire le macchine rilevate.

Per visualizzare le risorse, selezionare **Risorse > Risorse**.

Utilizzo degli elenchi di risorse

È possibile utilizzare gli elenchi di risorse per gestire i seguenti tipi di risorse: macchine, volumi di storage, reti, bilanciamenti del carico e gruppi di sicurezza che costituiscono le distribuzioni. Nell'elenco delle risorse è possibile gestirli in gruppi di tipi di risorse anziché in base alle distribuzioni.

- Tutte le risorse

Include tutte le risorse rilevate, distribuite, migrate e di cui è stato eseguito l'onboarding descritte nelle sezioni seguenti.

- Macchine virtuali

Macchine virtuali individuali. Le macchine potrebbero far parte di distribuzioni più grandi.

- Volumi

Volumi di storage rilevati o associati alle distribuzioni.

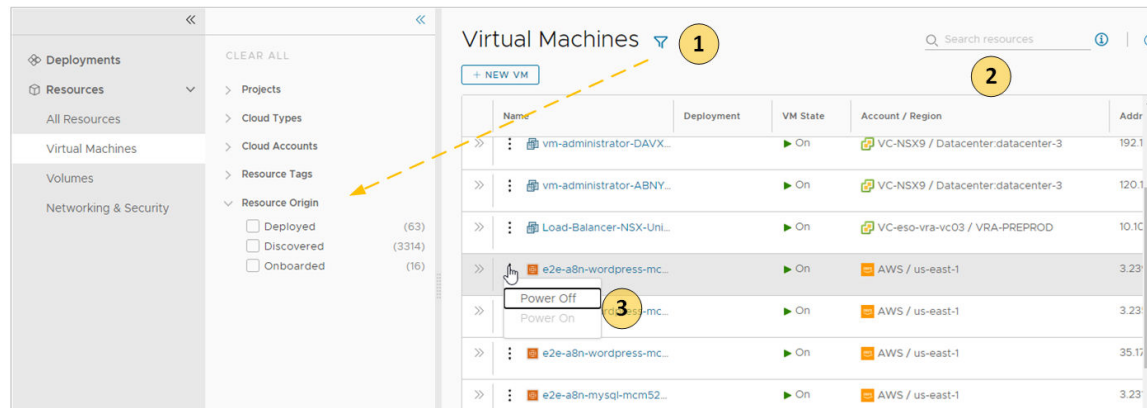
- Rete e sicurezza

Include reti, bilanciamenti del carico e gruppi di sicurezza.

In modo simile alla vista elenco delle distribuzioni, è possibile filtrare l'elenco, selezionare un tipo di risorsa, effettuare ricerche, ordinare ed eseguire azioni.

Se si fa clic sul nome della risorsa, è possibile utilizzare la risorsa nel contesto dei dettagli della risorsa.

Figura 7-3. Elenco delle pagine delle risorse



- 1 Filtrare l'elenco in base agli attributi della risorsa

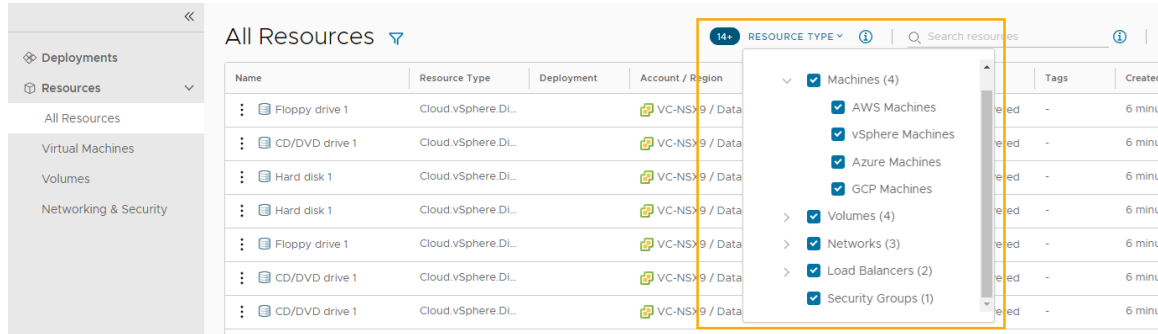
Ad esempio, è possibile filtrare in base al progetto, ai tipi di cloud, all'origine o ad altri attributi.

- 2 Cercare le risorse in base al nome, alle regioni dell'account o ad altri valori.

- 3 Eseguire le azioni gruppo 2 disponibili specifiche per il tipo di risorse e lo stato della risorsa.

Ad esempio, è possibile accendere una macchina rilevata se è spenta. In alternativa, è possibile ridimensionare una macchina di cui è stato eseguito l'onboarding.

Oltre alle opzioni di ricerca e filtro in ogni pagina, la pagina Tutte le risorse include un selettore Tipo di risorsa in cui è possibile creare un filtro per tutte le risorse.



Elenco delle risorse gestite per origine

È possibile utilizzare la scheda Risorse per gestire i seguenti tipi di risorse.

Tabella 7-3. Origini delle risorse

Risorsa gestita	Descrizione
Distribuita	<p>Le distribuzioni gestiscono completamente i carichi di lavoro che sono modelli cloud distribuiti o risorse di cui è stato eseguito l'onboarding. Le risorse del carico di lavoro possono includere macchine, volumi di storage, reti, bilanciamenti del carico e gruppi di sicurezza.</p> <p>È possibile gestire le distribuzioni nella sezione Distribuzioni o nella sezione Risorse.</p>
Rilevata	<p>Le risorse rilevate sono le macchine, i volumi di storage, le reti, i bilanciamenti del carico e i gruppi di sicurezza che il processo di individuazione ha identificato per ogni regione dell'account cloud aggiunta.</p> <p>Solo gli amministratori di Cloud Assembly possono visualizzare e gestire le risorse rilevate nella sezione Risorse.</p>

Tabella 7-3. Origini delle risorse (continua)

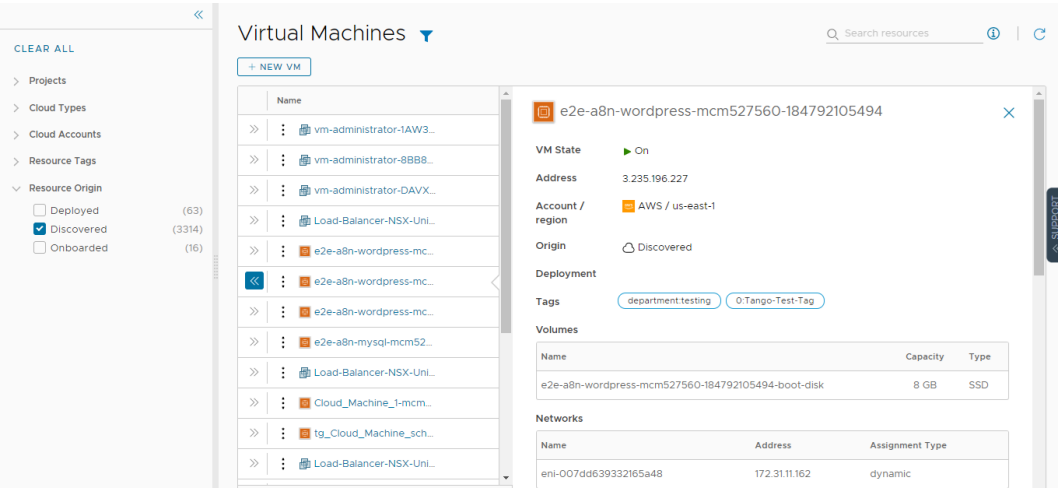
Migrate	<p>Le risorse migrate sono le distribuzioni di 7.x migrate a vRealize Automation. Le risorse migrate possono includere macchine, volumi di storage, reti, bilanciamenti del carico e gruppi di sicurezza. Le risorse migrate vengono gestite come le distribuzioni.</p> <p>È possibile gestire le risorse migrate nella sezione Distribuzioni o nella sezione Risorse.</p>
Di cui è stato eseguito l'onboarding	<p>Le risorse di cui è stato eseguito l'onboarding sono risorse rilevate che vengono sottoposte a una gestione più solida di vRealize Automation. Le risorse di cui è stato eseguito l'onboarding vengono gestite come le distribuzioni.</p> <p>È possibile gestire le risorse di cui è stato eseguito l'onboarding nella sezione Distribuzioni o nella sezione Risorse.</p>

Che cos'è la visualizzazione dettagli risorsa

È possibile utilizzare la visualizzazione dei dettagli della risorsa per esaminare in modo più approfondito la risorsa selezionata. In base alla risorsa, i dettagli possono includere reti, porte e altre informazioni raccolte sulla macchina. La profondità delle informazioni varia in base al tipo di account cloud e all'origine.

Per aprire il riquadro dei dettagli, fare clic sul nome della risorsa o sulle doppie frecce.

Figura 7-4. Riquadro dei dettagli delle risorse



Quali azioni giorno 2 è possibile eseguire sulle risorse?

Le azioni giorno 2 disponibili dipendono dall'origine della risorsa, dall'account cloud, dal tipo di risorsa e dallo stato.

Tabella 7-4. Elenco delle azioni per origine

Origine risorsa	Azioni giorno 2
Distribuita	Le azioni disponibili per l'esecuzione sulle risorse dipendono dal tipo di risorsa, dall'account cloud e dallo stato. Per un elenco dettagliato, vedere Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly .
Rilevata	<p>Le azioni disponibili per le risorse rilevate sono limitate alle macchine virtuali. In base allo stato, è possibile eseguire le seguenti azioni.</p> <ul style="list-style-type: none"> ■ Spegni ■ Accendi <p>Azione aggiuntiva della macchina virtuale vSphere.</p> <ul style="list-style-type: none"> ■ Connetti a console remota
Migrate	Le risorse migrate hanno le stesse opzioni di gestione delle azioni giorno 2 delle distribuzioni. Le azioni disponibili per l'esecuzione sulle risorse migrate dipendono dal tipo di risorsa, dall'account cloud, dallo stato e dai criteri del giorno 2. Per un elenco dettagliato, vedere Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly .
Di cui è stato eseguito l'onboarding	Le risorse di cui è stato eseguito l'onboarding hanno le stesse opzioni di gestione delle azioni giorno 2 delle distribuzioni. Le azioni disponibili per l'esecuzione sulle risorse di cui è stato eseguito l'onboarding dipendono dal tipo di risorsa, dall'account cloud e dallo stato. Per un elenco dettagliato, vedere Quali azioni è possibile eseguire sulle distribuzioni di Cloud Assembly .

Come si utilizzano le singole risorse in Cloud Assembly

In qualità di amministratore del cloud o di membro del progetto con risorse per il progetto, è possibile utilizzare la sezione Risorse della scheda Risorse per gestire le risorse distribuite e di cui è stato eseguito l'onboarding e la migrazione come singole risorse in base al tipo di risorsa.

Questo workflow, incentrato sulla gestione delle macchine virtuali, fornisce una guida per la gestione del ciclo di vita delle risorse di alto livello che è possibile applicare agli altri tipi di risorse.

Individuare le risorse della macchina virtuale.

Le macchine virtuali distribuite, di cui è stato eseguito l'onboarding e la migrazione sono disponibili nella pagina Tutte le risorse e nella pagina Macchine virtuali della scheda Risorse. Questo esempio riguarda le macchine virtuali, ma è possibile applicare lo stesso workflow agli altri tipi di risorse.

- 1 Selezionare **Risorse > Risorse > Macchine virtuali**.
- 2 Individuare la macchina virtuale.

È inoltre possibile utilizzare i filtri o la ricerca per individuare le risorse.

Virtual Machines 🔍 Search resources

[+ NEW VM](#)

Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
vm-administrator-VLDX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-N6CE...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
mcm-20211203215331-0...	Google Cloud Create VM_6f...	On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-

Rivedere i dettagli della macchina virtuale

I dettagli della risorsa forniscono una visualizzazione rapida delle informazioni sulla macchina, tra cui reti, proprietà personalizzate e altre informazioni raccolte.

- 1 Individuare la macchina nell'elenco Macchine virtuali.
- 2 Fare clic sul nome della risorsa o sulle doppie frecce nella colonna a sinistra della tabella.

Il riquadro dei dettagli si apre sul lato destro dell'elenco.

Virtual Machines 🔍 Search resources

[+ NEW VM](#)

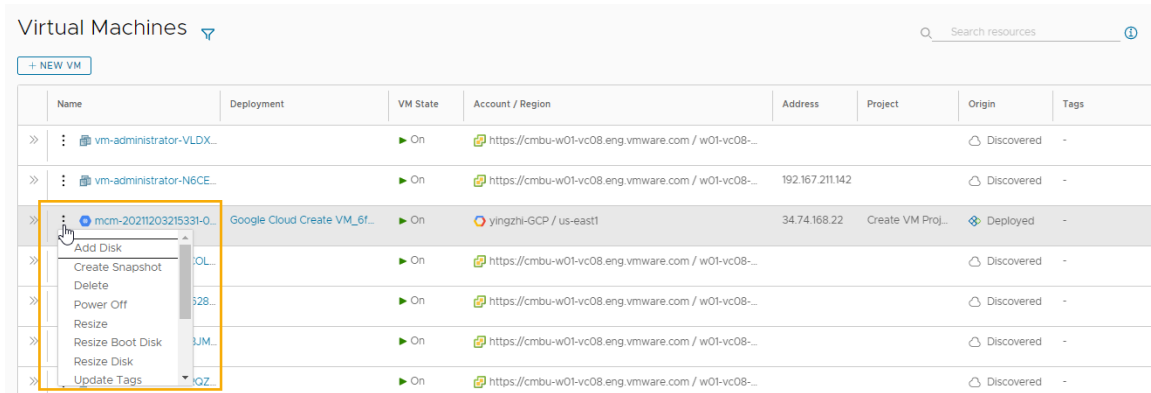
Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
vm-administrator-VLDX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-N6CE...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
mcm-20211203215331-0...	Google Cloud Create VM_6f...	On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-

- 3 Per chiudere il riquadro, fare clic sulle doppie frecce o sul nome della risorsa.

Esecuzione di azioni giorno 2 sulla macchina virtuale

Le azioni giorno 2 consentono di gestire le risorse. Le azioni disponibili dipendono dal tipo di risorsa, dallo stato della risorsa e dai criteri delle azioni del giorno 2 che vengono imposti.

- 1 Individuare la macchina nell'elenco Macchine virtuali.
- 2 Fare clic sui puntini di sospensione verticali per visualizzare le azioni disponibili.
- 3 Fare clic sull'azione.



Name	Deployment	VM State	Account / Region	Address	Project	Origin	Tags
vm-administrator-VLDX...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
vm-administrator-N6CE...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...	192.167.211.142		Discovered	-
mcm-20211203215331-0...	Google Cloud Create VM_6f...	On	yingzhi-GCP / us-east1	34.74.168.22	Create VM Proj...	Deployed	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-
...		On	https://cmbu-w01-vc08.eng.vmware.com / w01-vc08...			Discovered	-

Come si utilizzano le risorse rilevate in Cloud Assembly

L'amministratore di Cloud Assembly utilizza la sezione Risorse della scheda Risorse per gestire le macchine rilevate. Solo gli amministratori vedranno le risorse rilevate nelle varie pagine.

Questo workflow è incentrato sulla gestione delle macchine virtuali rilevate.

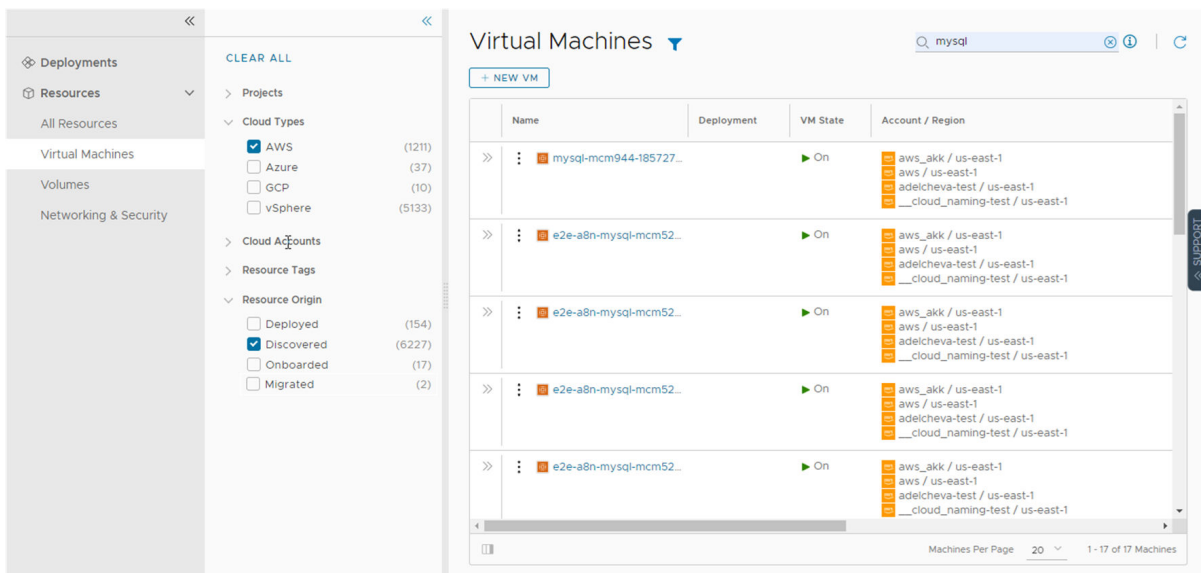
Operazioni preliminari

- Aggiungere un account cloud per le risorse che si desidera individuare. In questo workflow, viene utilizzata come esempio una macchina Amazon Web Services. Per aggiungere un account cloud, vedere [Aggiunta di account cloud a Cloud Assembly](#).

Individuare le macchine virtuali rilevate

Le risorse rilevate vengono raccolte dalla regione dell'account cloud e aggiunte alle risorse nella scheda Risorse. Questo esempio riguarda le macchine virtuali, ma vengono raccolti altri tipi di risorse, incluse le informazioni sullo storage e sulla rete.

1 Selezionare **Risorse > Risorse > Macchine virtuali**.



Name	Deployment	VM State	Account / Region
mysql-mcm944-185727...		On	aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1
e2e-a8n-mysql-mcm52...		On	aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1
e2e-a8n-mysql-mcm52...		On	aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1
e2e-a8n-mysql-mcm52...		On	aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1
e2e-a8n-mysql-mcm52...		On	aws_akk / us-east-1 aws / us-east-1 adelcheva-test / us-east-1 __cloud_naming-test / us-east-1

- 2 Per individuare le macchine virtuali AWS, fare clic sull'icona **Filtro** accanto all'etichetta della pagina

- 3 Nell'elenco dei filtri, espandere **Tipi di cloud** e selezionare **AWS**.

L'elenco è ora limitato alle macchine virtuali AWS. È possibile che vengano distribuiti, individuati e altri tipi di origine.

- 4 Nell'elenco dei filtri, espandere **Origine risorsa** quindi selezionare **Rilevata**.

L'elenco ora è limitato alle macchine virtuali AWS rilevate.

- 5 Per individuare una determinata macchina, è possibile utilizzare l'opzione **Cerca risorse** per eseguire la ricerca in base al nome, all'indirizzo IP, ai tag o ai valori.

In questo esempio, **mysql** è il termine di ricerca.

Controllo dettagli macchina virtuale

I dettagli della risorsa includono tutte le informazioni raccolte per la risorsa. È possibile utilizzare queste informazioni per comprendere la risorsa e tutte le associazioni con altre risorse.

- 1 Individuare la macchina virtuale nell'elenco Macchina virtuale.
- 2 Per visualizzare i dettagli della risorsa, fare clic sul nome della macchina o sulle doppie frecce nella colonna a sinistra.

Il riquadro dei dettagli si apre sul lato destro dell'elenco.

The screenshot displays the 'Virtual Machines' section of the vRealize Automation Cloud Assembly interface. On the left, a list of VMs is shown with names like 'mysql-mcm944-185727...' and 'mysql-mcm1688-17425...'. The VM 'mysql-mcm1688-174252447070' is selected. On the right, a detailed view of this VM is shown, including its state (On), address (44.195.25.253), account/region (aws_akk / us-east-1), origin (discovered), and deployment (cloud_naming-test / us-east-1). It also shows tags (Username:fritz, EventTopic:compute.allocation.pre), volumes (mysql-mcm1688-174252447070-boot-disk, 8 GB, SSD), and networks (eni-0a44e518e9562fddf, 172.31.53.191, dynamic). A search bar at the top right contains the text 'mysql'.

- 3 Rivedere i dettagli, inclusi archivio, reti, proprietà personalizzate e altre informazioni raccolte.
- 4 Per chiudere il riquadro, fare clic sulle doppie frecce o sul nome della risorsa.

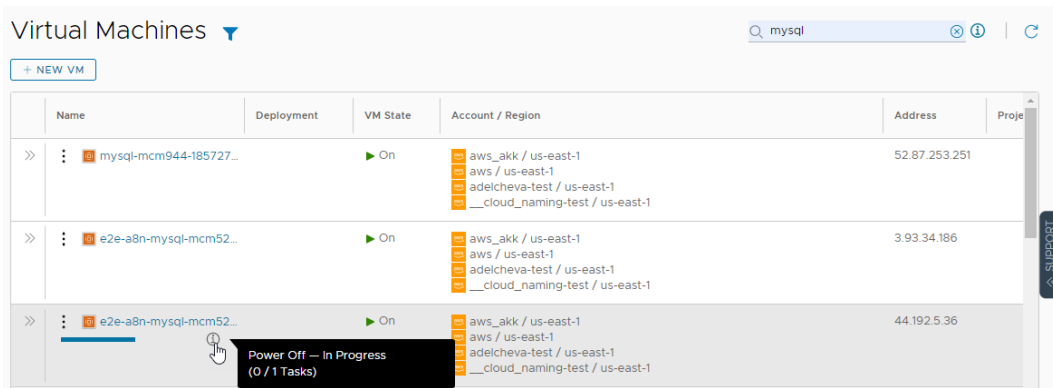
Esecuzione di azioni giorno 2 sulla macchina virtuale

Le azioni giorno 2 consentono di gestire le risorse. Le azioni correnti per le macchine virtuali rilevate includono Accendi e Spegni. Se si gestisce una macchina virtuale vSphere, è anche possibile eseguire Connetti con console remota.

- 1 Individuare la macchina nell'elenco Macchine virtuali.
- 2 Fare clic sui puntini di sospensione verticali per visualizzare le azioni disponibili.

Le azioni possibili per una macchina virtuale AWS sono Spegni e Accendi. L'accensione non è attiva perché la macchina è già accesa.

- 3 Fare clic su **Spegni** e inviare la richiesta.



Al termine del processo, la macchina viene spenta. Ora è possibile riaccenderla.

Quali sono gli altri obiettivi che è possibile raggiungere con la macchina virtuale rilevata

Per portare le risorse rilevate in una gestione completa, è possibile effettuare l'onboarding. Vedere [Che cosa sono i piani di onboarding in Cloud Assembly](#).