

Guida del portale tenant di VMware Cloud Director

Modificato in data 4 APRILE 2021
VMware Cloud Director 10.2

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 © 2017-2021 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

Guida del portale tenant di VMware Cloud Director™ 11

1 Guida introduttiva al portale tenant di VMware Cloud Director 13

- Informazioni su VMware Cloud Director™ 13
- Login nel portale tenant di VMware Cloud Director 15
- Ruoli e diritti per il portale tenant di VMware Cloud Director 15
- Utilizzo del portale tenant di VMware Cloud Director 16
- Utilizzo della ricerca globale di VMware Cloud Director 17
- Utilizzo della ricerca rapida di VMware Cloud Director 18
- Visualizzazione dei task 19
- Interruzione di un'attività in corso 20
- Visualizzazione di eventi 21
- Impostazione delle preferenze utente 21

2 Utilizzo delle macchine virtuali 23

- Architettura di una macchina virtuale 24
- Crittografia della macchina virtuale 25
- Visualizzazione delle macchine virtuali 26
- Creazione di una nuova macchina virtuale standalone 27
- Provisioning rapido delle macchine virtuali 29
- Apertura della console di una macchina virtuale 29
 - Installazione di VMware Remote Console in un client 29
 - Apertura di una console remota della macchina virtuale 30
 - Apertura di una console Web 31
- Esecuzione di operazioni di attivazione nelle macchine virtuali 32
 - Attivazione di una macchina virtuale 32
 - Disattivazione di una macchina virtuale 32
 - Arresto di un sistema operativo guest 33
 - Reimpostazione di una macchina virtuale 33
 - Sospensione di una macchina virtuale 34
 - Annullamento dello stato sospeso di una macchina virtuale 34
 - Attivazione di più macchine virtuali 34
 - Disattivazione di più macchine virtuali 35
 - Rimozione dello stato sospeso di più macchine virtuali 35
 - Reimpostazione di più macchine virtuali 36
- Installazione di VMware Tools in una macchina virtuale 36
- Aggiornamento della versione hardware virtuale di una macchina virtuale 37
- Modifica delle proprietà di una macchina virtuale 38

Modifica delle proprietà generali di una macchina virtuale	38
Modifica delle proprietà dell'hardware di una macchina virtuale	39
Modifica delle proprietà di personalizzazione del sistema operativo guest di una macchina virtuale	42
Modifica delle proprietà avanzate di una macchina virtuale	47
Inserisci file multimediale	49
Espelli file multimediale	50
Copia di una macchina virtuale in una vApp diversa	50
Spostamento di una macchina virtuale in una vApp diversa	51
Affinità e anti-affinità delle macchine virtuali	52
Visualizzazione delle regole di affinità e di anti-affinità	52
Creazione di una regola di affinità	53
Creazione di una regola di anti-affinità	53
Modifica di una regola di affinità o di anti-affinità	54
Eliminazione di una regola di affinità o di anti-affinità	55
Monitoraggio delle macchine virtuali	55
Utilizzo di snapshot	56
Creazione dello snapshot di una macchina virtuale	57
Ripristino dello snapshot di una macchina virtuale	58
Rimozione di una snapshot di una macchina virtuale	58
Rinnovo del lease di una macchina virtuale	59
Eliminazione di una macchina virtuale	59
Gruppi di scalabilità automatica	60
Creazione di un gruppo di scalabilità	60
Aggiunta di una regola di scalabilità automatica	61

3 Gestione delle vApp 63

Visualizzazione delle vApp	64
Creazione di una nuova vApp	64
Creazione di una vApp da pacchetto OVF	67
Aggiunta di una vApp da catalogo	69
Creazione di una vApp da un modello di vApp	71
Importazione di una macchina virtuale da vCenter Server come vApp	73
Esecuzione di operazioni di attivazione nelle vApp	73
Attivazione di una vApp	73
Disattivazione di una vApp	74
Reimpostazione di una vApp	74
Sospensione di una vApp	75
Annullamento dello stato sospeso di una vApp	75
Attivazione di più vApp	76
Disattivazione di più vApp	76
Rimozione dello stato sospeso di più vApp	76

Reimpostazione di più vApp	77
Sospensione di più vApp	77
Apertura di una vApp	78
Modifica proprietà vApp	78
Modifica delle proprietà generali della vApp	78
Modifica dell'ordine di avvio e arresto delle macchine virtuali in una vApp	79
Modifica delle proprietà guest di una vApp	80
Condivisione di una vApp	81
Visualizzazione del diagramma di rete di una vApp	82
Gestione delle reti in una vApp	83
Visualizzazione di reti di vApp	83
Applicazione della priorità in una rete di vApp	84
Aggiunta di una rete a una vApp	85
Configurazione dei servizi di rete per una rete di vApp	86
Eliminazione di una rete di vApp	93
Utilizzo di snapshot	93
Creazione dello snapshot di una vApp	94
Ripristino di una vApp a una snapshot	95
Rimozione dello snapshot di una vApp	95
Creazione di snapshot di più vApp	96
Rimozione degli snapshot di più vApp	96
Ripristino delle snapshot di più vApp	97
Modifica del proprietario di una vApp	97
Spostamento di una vApp in un altro virtual data center	98
Copia di una vApp arrestata in un altro virtual data center	98
Copia di una vApp attivata	99
Aggiunta di una macchina virtuale a una vApp	99
Salvataggio di una vApp come modello di vApp in un catalogo	101
Scaricare una vApp da pacchetto OVF	102
Rinnovo del lease di una vApp	103
Eliminazione di una vApp	104
Eliminazione di più vApp	104
4 Utilizzo dei cluster di Kubernetes	106
Aggiunta di un criterio Kubernetes del VDC dell'organizzazione	107
Modifica del criterio Kubernetes del VDC dell'organizzazione	109
Creazione di un cluster Tanzu Kubernetes	110
Creazione di un cluster Kubernetes nativo	112
Creazione di un cluster VMware Tanzu Kubernetes Grid Integrated Edition	113
Configurazione dell'accesso esterno a un servizio in un cluster Tanzu Kubernetes	114

5 Utilizzo delle reti 117

Gestione delle reti Virtual Data Center dell'organizzazione	120
Visualizzazione delle reti VDC dell'organizzazione disponibili	121
Aggiunta di una rete di virtual data center dell'organizzazione isolata	121
Aggiunta di una rete di virtual data center dell'organizzazione instradata	123
Aggiunta di una rete di virtual data center dell'organizzazione diretta	125
Aggiunta di una rete VDC dell'organizzazione con un commutatore logico NSX-T Data Center importato	126
Modifica delle impostazioni generali di una rete di virtual data center dell'organizzazione	127
Connessione di una rete di virtual data center dell'organizzazione a un gateway edge	127
Disconnessione di una rete VDC dell'organizzazione da un gateway edge	128
Conversione dell'interfaccia di una rete VDC dell'organizzazione instradata	129
Visualizzazione degli indirizzi IP utilizzati per la rete di virtual data center dell'organizzazione	129
Aggiunta di indirizzi IP al pool di IP di una rete di virtual data center dell'organizzazione	130
Modifica o rimozione di intervalli IP utilizzati in una rete di virtual data center dell'organizzazione	131
Modifica delle impostazioni DNS di una rete di virtual data center dell'organizzazione	131
Configurazione delle impostazioni DHCP per una rete di virtual data center dell'organizzazione isolata	132
Aggiunta di un pool DHCP a una rete di virtual data center dell'organizzazione instradata supportata da NSX-T Data Center	133
Modifica o eliminazione di un pool DHCP esistente per una rete di virtual data center dell'organizzazione isolata supportata da NSX Data Center for vSphere	133
Reimpostazione di una rete di virtual data center dell'organizzazione	134
Eliminazione di una rete di virtual data center dell'organizzazione	134
Gestione di reti di gruppi di data center con NSX-T Data Center	135
Gestione dei gruppi di data center con un tipo di provider di rete NSX-T Data Center	136
Utilizzo del firewall distribuito in un gruppo di data center con un tipo di provider di rete NSX-T Data Center	138
Gestione delle reti del gruppo di data center con un tipo di provider di rete NSX-T Data Center	143
Gestione dei punti di uscita dei gruppi di data center con un tipo di provider di rete NSX-T Data Center	149
Gestione di reti di gruppi di data center con NSX Data Center for vSphere	150
Gestione dei gruppi di data center con il tipo di provider di rete di NSX Data Center for vSphere	152
Gestione di reti di gruppi di data center supportate da NSX Data Center for vSphere	166
Gestione dei servizi gateway edge NSX Data Center for vSphere	168
Guida introduttiva alla rete avanzata di VMware Cloud Director con NSX Data Center for vSphere	169
Configurazione del firewall del tenant con NSX Data Center for vSphere	169
Gestione del DHCP del gateway edge NSX Data Center for vSphere	181

Gestione di Network Address Translation in un gateway edge di NSX Data Center for vSphere	186
Configurazione del routing avanzata per i gateway edge di NSX Data Center for vSphere	190
Bilanciamento del carico con NSX Data Center for vSphere	199
Configurazione dell'accesso sicuro tramite VPN in un gateway edge di NSX Data Center for vSphere	213
Gestione del certificato SSL in un gateway edge di NSX Data Center for vSphere	241
Raggruppamento personalizzato di oggetti per i gateway edge di NSX Data Center for vSphere	248
Statistiche e registri per un gateway edge di NSX Data Center for vSphere	251
Abilitazione dell'accesso a un gateway edge di NSX Data Center for vSphere dalla riga di comando SSH	253
Utilizzo dei tag di sicurezza per i gateway edge di NSX Data Center for vSphere	254
Utilizzo dei gruppi di sicurezza per i gateway edge di NSX Data Center for vSphere	258
Gestione dei gateway edge NSX-T Data Center	262
Aggiunta di un set di IP a un gateway edge di NSX-T Data Center	263
Aggiunta di una regola del firewall del gateway edge NSX-T Data Center	263
Aggiunta di una regola SNAT o DNAT a un gateway edge NSX-T	265
Configurazione di un servizio di inoltro DNS su un gateway edge NSX-T	267
Creazione di profili delle porte dell'applicazione personalizzata	268
VPN basata su criteri IPsec per i gateway edge NSX-T Data Center	269
Configurazione dei servizi della rete esterna dedicata	272
Utilizzo del bilanciamento del carico avanzato NSX	278

6 Uso dei dischi denominati e controllo dei criteri di storage 285

Creazione e utilizzo di dischi denominati	285
Creazione di un disco denominato	286
Modifica di un disco denominato	287
Collegamento di un disco denominato a una macchina virtuale	287
Eliminazione di un disco denominato	288
Controllo delle proprietà dei criteri di storage	288

7 Controllo e modifica delle proprietà del virtual data center 289

Controllo delle proprietà del virtual data center	289
Controllo dei metadati del virtual data center	289
Limitazione dell'accesso a un VDC dell'organizzazione per utenti e gruppi specifici dell'organizzazione	290

8 Utilizzo di istanze, endpoint e proxy di vCenter Server dedicati 292

Utilizzo di Chrome Browser Extension for VMware Cloud Director	293
Configurazione del browser con le impostazioni del proxy	293
Accesso all'interfaccia utente di un componente utilizzando un endpoint	294

9 Gestione dei modelli di vApp 296

- Visualizzazione di un modello di vApp 296
- Creazione di un modello di vApp da un file OVF 297
- Importazione di una macchina virtuale da vCenter Server come modello di vApp 298
- Assegnazione di un criterio di posizionamento della macchina virtuale e di un criterio di dimensionamento della macchina virtuale a un modello di vApp 299
- Download di un modello di vApp 300
- Eliminazione di un modello di vApp 300

10 Gestione dei file multimediali 302

- Caricamento di file multimediali 302
- Eliminazione di un file multimediale 303
- Download di un file multimediale 303

11 Gestione dei cataloghi 305

- Visualizzazione dei cataloghi 306
- Creazione di un catalogo 306
- Condividi un catalogo 307
- Eliminazione di un catalogo 308
- Modifica del proprietario di un catalogo 309
- Gestione dei metadati per un catalogo 309
- Pubblicazione di un catalogo 310
- Sottoscrizione a un catalogo esterno 311
- Aggiornamento dell'URL della posizione e della password per un catalogo sottoscritto 311
- Sincronizzazione di un catalogo sottoscritto 312

12 Gestione dei modelli di virtual data center dell'organizzazione 313

- Visualizzazione dei modelli di virtual data center disponibili 313
- Creazione di un'istanza di virtual data center da un modello 314

13 Gestione di utenti, gruppi e ruoli 315

- Gestione degli utenti 315
 - Creazione di un utente 315
 - Importa utenti 317
 - Modifica di un utente 318
 - Disattivazione o attivazione di un account utente 318
 - Eliminazione di un utente 319
 - Sblocco di un account utente bloccato 319
 - Gestione delle quote delle risorse di un utente 320
- Gestione di gruppi 320
 - Importazione di un gruppo 321

Eliminazione di un gruppo	321
Modifica di un gruppo	322
Gestione delle quote delle risorse di un gruppo	322
Ruoli e diritti	323
Ruoli predefiniti e relativi diritti	324
Diritti nei ruoli tenant globali predefiniti	326
Creazione di un ruolo tenant personalizzato	332
Modifica di un ruolo tenant personalizzato	333
Eliminazione di un ruolo	334
14 Configurazione dei provider di identità	335
Consentire all'organizzazione l'uso di un provider di identità SAML	335
Modifica delle impostazioni LDAP dell'organizzazione	337
Configurazione, prova e sincronizzazione di una connessione LDAP	338
15 Gestione dei certificati	341
Importazione di certificati attendibili	341
Importazione dei certificati nella libreria di certificati	342
16 Gestione dell'organizzazione	344
Modifica del nome e della descrizione di un'organizzazione	344
Modifica delle impostazioni e-mail	345
Test delle impostazioni SMTP	346
Modifica delle impostazioni del dominio per le macchine virtuali dell'organizzazione	346
Utilizzo di più siti	347
Configurazione e gestione di distribuzioni multisito	347
Informazioni generali sui lease	348
Modifica dei criteri di lease delle vApp e dei modelli di vApp nell'organizzazione	349
Modifica dei criteri di password e account utente nell'organizzazione	350
Creazione di un dashboard di avvisi	350
17 Utilizzo della Libreria dei servizi	352
Ricerca di un servizio	352
Esecuzione di un servizio	353
18 Gestione delle entità definite	354
Utilizzo delle definizioni entità personalizzata	357
Ricerca di un'entità personalizzata	357
Modifica di una definizione entità personalizzata	357
Aggiunta di una definizione entità personalizzata	358
Istanze entità personalizzata	359

Associazione di un'azione a un'entità personalizzata	359
Annullamento dell'associazione di un'azione a una definizione entità personalizzata	360
Pubblicazione di un'entità personalizzata	361
Eliminazione di un'entità personalizzata	361

Guida del portale tenant di VMware Cloud Director™

La *Guida del portale tenant di VMware Cloud Director™* fornisce informazioni su come utilizzare il portale tenant di VMware Cloud Director. In questa versione, il portale tenant viene utilizzato per amministrare l'organizzazione, nonché creare e configurare macchine virtuali, vApp e reti all'interno di vApp. È inoltre possibile configurare funzionalità avanzate di rete fornite da VMware NSX® for vSphere® all'interno di un ambiente di VMware Cloud Director. Con il portale tenant di VMware Cloud Director, è inoltre possibile creare e gestire cataloghi, vApp e modelli di VDC, nonché creare e gestire reti inter-VDC.

Destinatari della guida

Questa guida è destinata agli utenti che desiderano utilizzare le funzionalità del portale tenant di VMware Cloud Director. Le informazioni sono indirizzate principalmente agli utenti che dispongono del ruolo **Amministratore organizzazione** e utilizzano il portale tenant per amministrare la propria organizzazione, nonché gestire macchine virtuali, vApp, reti e così via.

Glossario di VMware Technical Publications

VMware Technical Publications offre un glossario di termini il cui significato potrebbe essere sconosciuto. Per le definizioni dei termini utilizzati nella documentazione tecnica di VMware, visitare il sito Web all'indirizzo <http://www.vmware.com/support/pubs>.

Termini e condizioni d'uso

VMware concede all'utente l'autorizzazione a modificare questa guida dell'utente del tenant (la "Guida") nella misura necessaria per personalizzarla in modo da riflettere i propri processi operativi e quindi riprodurre e distribuire la Guida modificata ai clienti. Non è possibile addebitare ai clienti una tariffa per l'accesso alla Guida modificata. L'UTENTE RICONOSCE CHE LA GUIDA VIENE FORNITA GRATUITAMENTE "COSÌ COM'È", SENZA ALCUNA GARANZIA E SOLO PER GLI SCOPI SOPRA DESCRITTI. DI CONSEGUENZA, LA RESPONSABILITÀ TOTALE DI VMWARE E DEI SUOI FORNITORI DERIVANTE DA O CONNESSA ALLA FORNITURA DELL'ACCESSO ALLA GUIDA NON POTRÀ SUPERARE I 100 \$. IN NESSUN CASO VMWARE O I SUOI FORNITORI SARANNO RESPONSABILI PER EVENTUALI DANNI INDIRETTI, ACCIDENTALI, PARTICOLARI O CONSEGUENZIALI (INCLUSI, A TITOLO ESEMPLIFICATIVO, DANNI PER PERDITA DI PROFITTI, INTERRUZIONE DELL'ATTIVITÀ O PERDITA DI INFORMAZIONI AZIENDALI), A

PRESCINDERE DALLA CAUSA E PER QUALSIVOGLIA RESPONSABILITÀ, ANCHE SE VMWARE O I SUOI FORNITORI SONO STATI INFORMATI DELLA POSSIBILITÀ DI TALI DANNI. QUESTE LIMITAZIONI VERRANNO APPLICATE ANCHE IN CASO DI MANCATA RIUSCITA DI QUALSIASI RIMEDIO LIMITATO.

Guida introduttiva al portale tenant di VMware Cloud Director

1

Quando si accede al portale tenant, è possibile eseguire diverse attività, dalla creazione di macchine virtuali e vApp, all'impostazione della configurazione dei servizi di rete avanzati e all'esecuzione di flussi di lavoro di vRealize Orchestrator.

Questo capitolo include i seguenti argomenti:

- Informazioni su VMware Cloud Director™
- Login nel portale tenant di VMware Cloud Director
- Ruoli e diritti per il portale tenant di VMware Cloud Director
- Utilizzo del portale tenant di VMware Cloud Director
- Utilizzo della ricerca globale di VMware Cloud Director
- Utilizzo della ricerca rapida di VMware Cloud Director
- Visualizzazione dei task
- Interruzione di un'attività in corso
- Visualizzazione di eventi
- Impostazione delle preferenze utente

Informazioni su VMware Cloud Director™

VMware Cloud Director™ fornisce l'accesso basato su ruolo a un portale tenant basato sul Web, che consente ai membri di un'organizzazione di interagire con le risorse dell'organizzazione stessa per creare e utilizzare vApp e macchine virtuali.

Prima che gli utenti possano accedere all'organizzazione, un **amministratore di sistema** di VMware Cloud Director deve creare l'organizzazione, assegnarle le risorse e fornire l'URL per l'accesso al portale tenant. Ciascuna organizzazione include uno o più **amministratori**, che ne completano la configurazione aggiungendo membri, nonché impostando criteri e preferenze. Dopo aver impostato l'organizzazione, gli utenti non amministratori possono eseguire il login, utilizzare e gestire macchine virtuali e vApp.

Organizzazioni

Un'organizzazione è un'unità di amministrazione di una raccolta di utenti, gruppi e risorse di calcolo. L'autenticazione degli utenti avviene a livello dell'organizzazione mediante la specifica delle credenziali definite da un **amministratore dell'organizzazione** al momento della creazione o dell'importazione dell'utente. Gli **amministratori di sistema** creano le organizzazioni e ne eseguono il provisioning, mentre gli **amministratori dell'organizzazione** gestiscono i cataloghi, i gruppi e gli utenti dell'organizzazione.

Utenti e gruppi

Un'organizzazione può contenere un numero arbitrario di utenti e gruppi. Gli utenti possono essere creati in locale dall'amministratore dell'organizzazione o importati da un servizio di directory. I gruppi devono essere importati dal servizio di directory. Le autorizzazioni all'interno di un'organizzazione sono controllate tramite l'assegnazione dei diritti e dei ruoli a utenti e gruppi.

Virtual data center

Un virtual data center dell'organizzazione fornisce risorse all'organizzazione. I virtual data center forniscono un ambiente in cui è possibile archiviare, distribuire e utilizzare i sistemi virtuali. Forniscono anche lo storage per i supporti CD e DVD virtuali. Un'organizzazione può disporre di più virtual data center.

Reti del virtual data center di un'organizzazione

La rete del virtual data center è contenuta nel virtual data center di un'organizzazione di VMware Cloud Director ed è disponibile per tutte le vApp dell'organizzazione. Una rete di virtual data center dell'organizzazione consente la comunicazione tra tutte le vApp di un'organizzazione. Una rete di virtual data center dell'organizzazione può essere connessa a una rete esterna o isolata e interna all'organizzazione. Solo gli **amministratori di sistema** possono creare reti di virtual data center dell'organizzazione, mentre gli **amministratori dell'organizzazione** possono gestire le reti di virtual data center dell'organizzazione, inclusi i servizi di rete forniti.

Reti di vApp

Una rete di vApp è contenuta in una vApp e consente la comunicazione tra le macchine virtuali della vApp. È possibile connettere una rete di vApp a una rete di virtual data center dell'organizzazione per consentire la comunicazione tra la vApp e le altre vApp dell'organizzazione o esterne all'organizzazione, se la rete di virtual data center dell'organizzazione è connessa a una rete esterna.

Cataloghi

Le organizzazioni utilizzano i cataloghi per l'archiviazione dei modelli di vApp e dei file multimediali. I membri di un'organizzazione che possono accedere a un catalogo possono utilizzare i file multimediali e i modelli di vApp del catalogo per creare le proprie vApp. Gli **amministratori dell'organizzazione** possono copiare elementi da cataloghi pubblici nel catalogo dell'organizzazione.

Istanze di vCenter Server dedicate (SDDC) e proxy

Un data center definito dal software (SDDC) incapsula un intero ambiente vCenter Server. Un'istanza di vCenter Server dedicata può includere uno o più proxy che forniscono l'accesso a componenti diversi dell'ambiente sottostante. L'**amministratore di sistema** può pubblicare una o più istanze di vCenter Server dedicate nell'organizzazione. È possibile utilizzare i proxy contenenti per accedere all'interfaccia utente o all'API dei componenti con proxy.

Login nel portale tenant di VMware Cloud Director

È possibile accedere al portale tenant di VMware Cloud Director utilizzando un URL specifico dell'organizzazione.

Se non si conosce l'URL del portale tenant dell'organizzazione, contattare l'**amministratore dell'organizzazione**. Per ulteriori informazioni sui browser e sulle configurazioni supportati, vedere *Note di rilascio di VMware Cloud Director*.

Procedura

- 1 In un browser Web, accedere all'URL del portale tenant dell'organizzazione.

Ad esempio, *<https://cloud.example.com/tenant/myOrg>*.

- 2 Immettere il nome utente e la password e fare clic su **Esegui login**.

Ruoli e diritti per il portale tenant di VMware Cloud Director

VMware Cloud Director include un set preconfigurato di ruoli utente e dei relativi diritti. I ruoli che possono accedere al portale tenant di VMware Cloud Director sono quelli creati per impostazione predefinita in qualsiasi organizzazione o altri ruoli che vengono creati dall'amministratore dell'organizzazione.

Gli utenti a cui vengono assegnati i seguenti ruoli dell'organizzazione possono accedere al portale tenant. Gli elementi che possono visualizzare e le azioni che possono eseguire dipendono dai diritti associati a un determinato ruolo.

- **Amministratore organizzazione**
- **Autore catalogo**
- **Autore vApp**
- **Utente vApp**

■ Solo accesso console

Per informazioni sui ruoli predefiniti e sui relativi diritti, vedere [Ruoli predefiniti e relativi diritti](#).

Utilizzo del portale tenant di VMware Cloud Director

Se si dispone di più virtual data center, quando si accede al portale tenant di VMware Cloud Director, si viene reindirizzati alla schermata del dashboard **Data center**. Se si dispone di un solo virtual data center, quando si accede al portale tenant di VMware Cloud Director, si viene reindirizzati direttamente al data center.

La schermata del dashboard **Data center** fa parte della funzionalità multisito di VMware Cloud Director, che consente ai tenant di visualizzare l'ambiente del cloud distribuito geograficamente come una singola entità. Per ulteriori informazioni sulla funzionalità multisito, vedere [Utilizzo di più siti](#).

Il dashboard fornisce una vista unificata dei virtual data center di VMware Cloud Director e dei siti non solo in una singola organizzazione. In un ambiente con più celle e più organizzazioni, è possibile visualizzare anche i virtual data center di tutte le altre organizzazioni associate.

Nota A seconda dei diritti di cui dispongono, gli utenti tenant possono visualizzare tutti i siti membri di un'organizzazione o solo un sottoinsieme di siti.

Le informazioni relative all'organizzazione vengono visualizzate nella parte superiore della barra multifunzione di riepilogo.

Se si accede come **amministratore dell'organizzazione**, è possibile visualizzare:

- Il numero di siti, organizzazioni e virtual data center
- Il numero totale di vApp e macchine virtuali in esecuzione
- Le risorse hardware utilizzate, come CPU, memoria e storage.

I virtual data center vengono visualizzati in una vista a schede. Ciascuna scheda contiene informazioni sull'organizzazione a cui appartiene il virtual center, il numero di vApp, il numero totale di macchine virtuali e il numero di macchine virtuali in esecuzione. Nella scheda vengono inoltre visualizzate la CPU, la memoria e la capacità di storage disponibili per il data center, nonché le metriche in tempo reale relative alle allocazioni e alle prenotazioni correnti delle risorse.

Nella barra di navigazione superiore, è possibile passare a varie voci di menu.

Voce del menu	Descrizione
Data center	Consente di passare alle risorse Virtual data center , Gruppi di data center e Data center di vSphere dedicati nell'organizzazione.
Virtual data center	Consente di passare alla schermata Virtual data center in cui sono visualizzati i virtual data center dell'organizzazione.
Data center di vSphere dedicati	Consente di passare alla schermata in cui sono visualizzati i data center di vSphere dedicati che il provider di servizi ha pubblicato nell'organizzazione.
Applicazioni	Consente di passare alle risorse Applicazioni virtuali e Macchine virtuali nell'organizzazione.

Voce del menu	Descrizione
Librerie	Consente di passare a una vista unificata di modelli di vApp, cataloghi, multimedia e altri tipi di file. È possibile utilizzare tali modelli e file per distribuire macchine virtuali o vApp.
Rete	Consente di accedere alle reti, ai gateway edge e ai gruppi di data center dell'organizzazione.
Amministrazione	Consente di passare alle schermate di configurazione Controllo accessi e Provider di identità , nonché alle impostazioni generali, e-mail, personalizzazione guest, metadati, multisito e criteri per l'organizzazione.
Monitora	Consente di passare alle schermate Attività ed Eventi . Nella schermata Attività vengono visualizzate le attività segnalate da VMware Cloud Director. La schermata Eventi visualizza gli eventi segnalati da VMware Cloud Director.

È possibile personalizzare il portale tenant di VMware Cloud Director utilizzando **Branding Cloud Director OpenAPI**. Per informazioni sull'uso di Cloud Director OpenAPI, vedere il documento *Guida introduttiva a Cloud Director OpenAPI* all'indirizzo <https://code.vmware.com>.

Utilizzo della ricerca globale di VMware Cloud Director

È possibile utilizzare la ricerca globale di VMware Cloud Director per eseguire una ricerca in base a un nome o parte di esso tra i nomi degli oggetti presenti nell'ambiente. È inoltre possibile cercare una macchina virtuale in base al suo indirizzo IP, se l'indirizzo IP della macchina virtuale è statico.

L'elenco degli oggetti preimpostati è:

- Data center
- Modelli di vApp
- vApp
- Macchine virtuali
- Reti di vApp
- Cataloghi

Se una macchina virtuale utilizza un indirizzo IP assegnato da DHCP, la ricerca non ne restituisce l'indirizzo IP. Se si desidera cercare una macchina virtuale con un indirizzo IP assegnato da DHCP, è necessario effettuare la ricerca in base al nome.

Per impostazione predefinita, è possibile eseguire la ricerca solo negli oggetti presenti nel sito locale. Se si dispone di un ambiente multisito, è possibile eseguire la ricerca tra più siti.

Procedura

- 1 Nell'angolo superiore destro del portale tenant di VMware Cloud Director, fare clic sull'icona **Cerca**.
- 2 (Facoltativo) Bloccare il pannello di ricerca facendo clic sull'icona **Blocca**.

- 3 Nella casella di testo **Cerca**, immettere un simbolo, una parte di un nome o un indirizzo IP in base a cui cercare i nomi o gli indirizzi IP statici degli oggetti corrispondenti delle macchine virtuali.
- 4 Se si utilizza un ambiente multisito, selezionare i siti in cui si desidera eseguire la ricerca.
- 5 Premere **Invio**.

Risultati

Vengono visualizzati i primi cinque risultati corrispondenti per tipo di oggetto. I risultati vengono ordinati alfabeticamente.

Operazioni successive

- Per visualizzare altri risultati, se presenti, fare clic su **Carica altre** sotto ciascun tipo di oggetto.
- Per visualizzare ulteriori informazioni su un oggetto specifico dai risultati della ricerca, posizionare il puntatore del mouse sull'oggetto.
- Per gestire un oggetto specifico, ad esempio per visualizzarne o modificarne le impostazioni, fare clic sull'oggetto. I dettagli relativi all'oggetto vengono visualizzati sulla sinistra.

Utilizzo della ricerca rapida di VMware Cloud Director

È possibile utilizzare la ricerca rapida di VMware Cloud Director per trovare schermate, entità e azioni. I risultati dipendono dalla posizione nell'interfaccia utente.

I risultati variano in base al contesto, indipendentemente dal fatto che sia stata selezionata un'entità e in base alle azioni disponibili per una determinata entità. I risultati della ricerca sono raggruppati in sezioni.

- Navigazione globale: i risultati di questa sezione non sono correlati a un'entità specifica, ad esempio gateway edge, LDAP, attività, certificati attendibili, macchine virtuali e così via. Questi risultati si ottengono indipendentemente dalla posizione in cui ci si trova nell'interfaccia utente.
- Navigazione contestuale: i risultati di questa sezione dipendono dall'entità selezionata nell'interfaccia utente. Ad esempio, le viste specifiche di una vApp, come le macchine virtuali, il diagramma della rete e così via. Se si seleziona un'entità come una vApp, la ricerca mostra sia i risultati di navigazione globali che quelli contestuali e tutte le azioni che potrebbero essere applicabili all'entità.
- Azioni contestuali: i risultati di questa sezione dipendono dall'entità selezionata nell'interfaccia utente. In base alla posizione nell'interfaccia utente e all'entità selezionata, utilizzando i risultati della ricerca rapida è possibile eseguire un'azione correlata all'entità. Ad esempio, la ricerca dalla vista dei dettagli di una macchina virtuale mostra i risultati delle viste globali, delle viste contestuali e delle azioni che è possibile eseguire nella macchina virtuale selezionata.

- Ricerca entità per nome: se si visualizza un elenco di entità, i risultati della ricerca possono includere anche i nomi di entità dello stesso tipo di quelle nell'elenco. Ad esempio, se si visualizza un elenco di macchine virtuali, i risultati della ricerca includono le corrispondenze di navigazione globale e i nomi corrispondenti delle macchine virtuali. Se nell'elenco si visualizzano più pagine di entità, la ricerca verifica l'elenco completo delle entità e potrebbe mostrare un nome che non è visibile nella pagina corrente.

Procedura

- 1 Aprire la finestra **Ricerca rapida**.
 - Sulla barra di navigazione superiore, fare clic sul menu **Guida** e selezionare **Ricerca rapida**.
 - Premere CTRL+. o CMD+., in base al sistema operativo in uso.
- 2 Immettere i criteri di ricerca.
- 3 Sfogliare i risultati e selezionare un'opzione oppure eseguire un'azione facendo clic o premendo Invio.

È possibile utilizzare i tasti freccia su e giù per sfogliare i risultati della ricerca.


Visualizzazione dei task

Nel portale tenant, è possibile visualizzare l'elenco dei task recenti, nonché i dettagli e lo stato. È inoltre possibile visualizzare l'elenco di tutti i task.

Per impostazione predefinita, il pannello **Task recenti** viene visualizzato nella parte inferiore del portale tenant e contiene un elenco dei task eseguiti di recente. Quando si avvia un'operazione, ad esempio per creare una macchina virtuale, il task viene visualizzato nel pannello. Se si riduce a icona il pannello **Task recenti**, è comunque possibile vedere il numero di task recenti eseguiti correttamente o non riusciti. È sempre possibile aprire nuovamente il pannello **Task recenti** facendo clic sulle doppie frecce.

La vista task include tutti i task e indica quando sono stati eseguiti e se sono stati completati correttamente. Questa vista è il primo passo per la risoluzione dei problemi nel proprio ambiente. La vista task contiene operazioni di lunga durata, come la creazione di macchine virtuali o vApp.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Monitor** e su **Attività**.
Viene visualizzato l'elenco di tutti i task, insieme all'ora in cui sono stati eseguiti e al loro stato.
- 2 Fare clic sull'icona dell'editor () per modificare i dettagli che si desidera vengano visualizzati sui task.
- 3 (Facoltativo) Per visualizzare i dettagli di un task, fare clic sul nome del task.
I dettagli includono informazioni come il motivo dell'errore, quando il task non è riuscito e così via.

Dettaglio	Descrizione
Operazione	Nome dell'operazione eseguita.
ID processo	ID dell'attività.
Tipo	L'oggetto in cui è stata eseguita l'attività. Ad esempio, se si crea una macchina virtuale, il tipo è <code>vm</code> .
Organizzazione	Nome dell'organizzazione.
Stato	Stato del task, come Riuscito, In esecuzione o Non riuscito.
Iniziatore	L'utente che ha avviato l'operazione.
Ora di inizio	Data e ora di inizio dell'operazione.
Ora di completamento	Data e ora in cui l'operazione è riuscita o non è riuscita.
Spazio dei nomi del servizio	Nome del servizio, ad esempio <code>com.vmware.cloud</code> .
Dettagli	Motivo dell'errore dell'attività. Ad esempio, se si tenta di creare una snapshot di una macchina virtuale e l'operazione non riesce perché lo storage non è sufficiente, i dettagli dell'attività sono del seguente tipo: L'operazione richiesta causerà il superamento della quota di storage del VDC: 8.693 MB di criterio di storage "*" disponibili su 41.472 MB richiesti.

Interruzione di un'attività in corso

Se si avvia accidentalmente un'operazione prima di applicare o rivedere tutte le impostazioni necessarie, è possibile interrompere il task in corso.

Per impostazione predefinita, il pannello **Task recenti** viene visualizzato nella parte inferiore del portale. Quando si avvia un'operazione, ad esempio per creare una macchina virtuale, il task viene visualizzato nel pannello.

Prerequisiti

Il pannello **Task recenti** deve essere aperto.

Procedura

- 1 Avviare un'operazione di lunga durata.

Le operazioni di lunga durata sono, ad esempio, la creazione di una macchina virtuale o una vApp, le operazioni di attivazione eseguite nelle macchine virtuali o nelle vApp e così via.

- 2 Nel pannello **Task recenti**, fare clic sull'icona **Annulla**.
- 3 Nella finestra di dialogo **Annulla task**, confermare l'annullamento dell'attività facendo clic su **OK**.

Risultati

L'operazione viene interrotta.

Visualizzazione di eventi


Dal portale è possibile visualizzare l'elenco di tutti gli eventi, nonché i dettagli e lo stato.

La vista eventi è un modo per visualizzare lo stato degli eventi nel portale. La vista indica quando si sono verificati gli eventi e se sono stati completati correttamente. La vista eventi contiene gli eventi che si verificano una volta sola, come gli accessi degli utenti e la creazione o l'eliminazione di oggetti.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Monitor** e su **Eventi**.

Viene visualizzato l'elenco di tutti gli eventi, insieme all'ora in cui si sono verificati e al loro stato.

- 2 Fare clic sull'icona dell'editor () per modificare i dettagli che si desidera vengano visualizzati sugli eventi.

- 3 (Facoltativo) Fare clic su un evento per visualizzarne i dettagli.

Dettaglio	Descrizione
Evento	Nome dell'evento. Ad esempio, se si modifica una vApp in modo da includervi macchine virtuali, l'evento che avvia l'intera operazione è <i>Task 'Modify vApp' start</i> .
ID evento	ID dell'attività.
Tipo	L'oggetto in cui è stata eseguita l'attività. Ad esempio, se si crea una macchina virtuale, il tipo è <i>vm</i> .
Destinazione	Oggetto di destinazione dell'evento. Ad esempio, quando si modifica una vApp in modo da includervi macchine virtuali, la destinazione dell'evento <i>Task 'Modify vApp' start</i> è <i>vdcUpdateVapp</i> .
Stato	Stato dell'evento, ad esempio Eseguito correttamente o Non riuscito.
Spazio dei nomi del servizio	Nome del servizio, ad esempio <i>com.vmware.cloud</i> .
Organizzazione	Nome dell'organizzazione.
Proprietario	Utente che ha attivato l'evento.
Ora di occorrenza	Data e ora dell'evento.

Impostazione delle preferenze utente

È possibile impostare determinate preferenze relative agli avvisi di sistema e alla visualizzazione che diventeranno effettive ogni volta che si esegue il login al sistema.

Per ulteriori informazioni sui lease, vedere [Informazioni generali sui lease](#).

Procedura

- 1 Nella barra di navigazione superiore, fare clic sul nome utente e selezionare **Preferenze utente**.
- 2 Selezionare la pagina da visualizzare quando si esegue il login.
 - a Selezionare il pulsante di opzione accanto a **Pagina iniziale** e fare clic su **Modifica**.
 - b Selezionare un'opzione dal menu a discesa e fare clic su **Salva**.
- 3 Configurare una notifica tramite e-mail per le scadenze dei lease di runtime.
 - a Selezionare il pulsante di opzione accanto a **Ora avviso lease di distribuzione** e fare clic su **Modifica**.
 - b Immettere un valore in secondi e fare clic su **Salva**.
- 4 Configurare una notifica tramite e-mail per le scadenze dei lease di storage.
 - a Selezionare il pulsante di opzione accanto a **Ora avviso lease di storage** e fare clic su **Modifica**.
 - b Immettere un valore in secondi e fare clic su **Salva**.

Utilizzo delle macchine virtuali

2

Una macchina virtuale è un computer software che, allo stesso modo di un computer fisico, esegue un sistema operativo e delle applicazioni. La macchina virtuale è costituita da una serie di file di configurazione e specifiche ed è supportata dalle risorse fisiche di un host. Ogni macchina virtuale dispone di dispositivi virtuali che forniscono le stesse funzionalità dell'hardware fisico, ma con maggiore portabilità, sicurezza e semplicità di gestione.

Oltre alle operazioni che possono essere eseguite in una macchina fisica, le macchine virtuali di VMware Cloud Director supportano operazioni dell'infrastruttura virtuale, come la creazione di una snapshot dello stato della macchina virtuale e lo spostamento di una macchina virtuale da un host all'altro.

A partire da VMware Cloud Director 9.5, le macchine virtuali supportano la connettività IPv6. È possibile assegnare indirizzi IPv6 a macchine virtuali connesse a reti IPv6.

Importante Tutti i passaggi per l'utilizzo delle macchine virtuali sono documentati nella vista a schede, supponendo che si disponga di più virtual data center. Le stesse procedure possono essere completate anche dalla vista griglia, ma i passaggi possono variare leggermente.

Questo capitolo include i seguenti argomenti:

- [Architettura di una macchina virtuale](#)
- [Crittografia della macchina virtuale](#)
- [Visualizzazione delle macchine virtuali](#)
- [Creazione di una nuova macchina virtuale standalone](#)
- [Provisioning rapido delle macchine virtuali](#)
- [Apertura della console di una macchina virtuale](#)
- [Esecuzione di operazioni di attivazione nelle macchine virtuali](#)
- [Installazione di VMware Tools in una macchina virtuale](#)
- [Aggiornamento della versione hardware virtuale di una macchina virtuale](#)
- [Modifica delle proprietà di una macchina virtuale](#)
- [Inserisci file multimediale](#)
- [Espelli file multimediale](#)

- [Copia di una macchina virtuale in una vApp diversa](#)
- [Spostamento di una macchina virtuale in una vApp diversa](#)
- [Affinità e anti-affinità delle macchine virtuali](#)
- [Monitoraggio delle macchine virtuali](#)
- [Utilizzo di snapshot](#)
- [Rinnovo del lease di una macchina virtuale](#)
- [Eliminazione di una macchina virtuale](#)
- [Gruppi di scalabilità automatica](#)

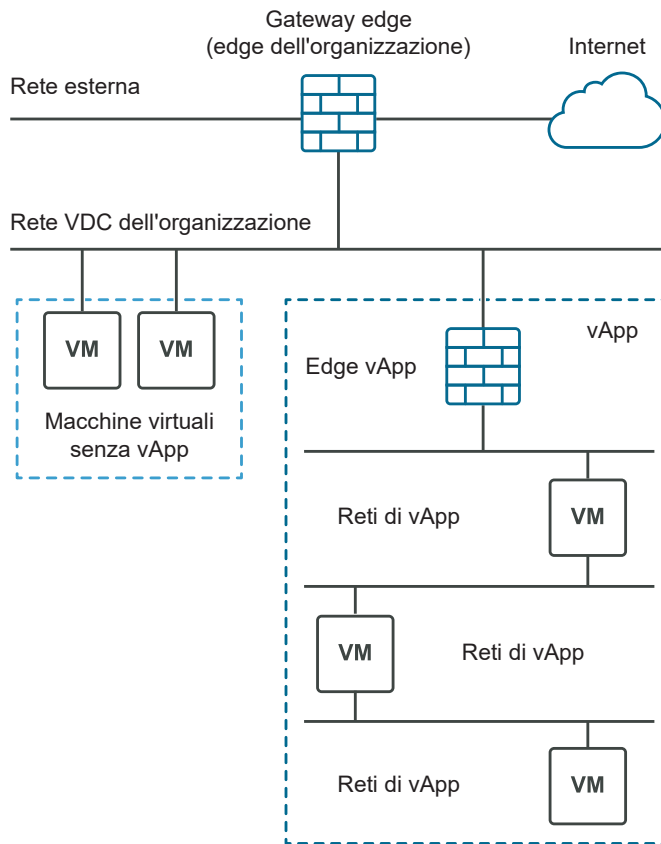
Architettura di una macchina virtuale

Una macchina virtuale può esistere come macchina autonoma o trovarsi all'interno di una vApp.

Una macchina virtuale è un computer software che, allo stesso modo di un computer fisico, esegue un sistema operativo e delle applicazioni. La macchina virtuale è costituita da una serie di file di configurazione e specifiche ed è supportata dalle risorse fisiche di un host. Ogni macchina virtuale dispone di dispositivi virtuali che forniscono le stesse funzionalità dell'hardware fisico, ma con maggiore portabilità, sicurezza e semplicità di gestione. Le macchine virtuali possono essere autonome o trovarsi all'interno di una vApp. Una vApp è un oggetto composto, costituito da una o più macchine virtuali nonché da una o più reti.

Nella figura seguente vengono illustrate le diverse opzioni disponibili durante la creazione di una macchina virtuale. È possibile creare una macchina virtuale autonoma o una macchina virtuale all'interno di una vApp. La macchina virtuale autonoma è collegata direttamente al virtual data center dell'organizzazione. È anche possibile creare una macchina virtuale all'interno di una vApp. Creando una macchina virtuale all'interno di una vApp, è possibile raggruppare più macchine virtuali e le loro reti associate. Le vApp consentono di creare applicazioni complesse e salvarle in un catalogo per poterle utilizzare in futuro.

Figura 2-1. Le macchine virtuali possono essere autonome o trovarsi all'interno di una vApp



Crittografia della macchina virtuale

A partire da VMware Cloud Director 10.1, è possibile migliorare la sicurezza dei dati utilizzando la crittografia della macchina virtuale. È possibile crittografare macchine virtuali e dischi associandoli a criteri di storage che dispongono della funzionalità di crittografia della macchina virtuale.

La crittografia protegge non solo la macchina virtuale, ma anche i dischi della macchina virtuale e gli altri file. È possibile visualizzare le funzionalità dei criteri di storage e lo stato di crittografia delle macchine virtuali e dei dischi nell'API e nell'interfaccia utente. Nelle macchine virtuali e nei dischi crittografati è possibile eseguire tutte le operazioni supportate nella rispettiva versione di vCenter Server.

Se il VDC dell'organizzazione dispone di un criterio di storage con crittografia delle macchine virtuali abilitata, è possibile crittografare macchine virtuali e dischi. Vedere l'argomento [Abilitazione della crittografia della macchina virtuale nei criteri di storage di un virtual data center dell'organizzazione](#) in *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*. Per crittografare una macchina virtuale o un disco, associarlo a un criterio di storage abilitato per la crittografia della macchina virtuale. Per le macchine virtuali, vedere [Creazione](#)

di una nuova macchina virtuale standalone o [Modifica delle proprietà generali di una macchina virtuale](#). Per i dischi denominati, vedere [Creazione di un disco denominato](#) o [Modifica di un disco denominato](#). Per decrittografare una macchina virtuale o un disco, associare la macchina virtuale o il disco a un criterio di storage in cui non è abilitata la crittografia.

Limitazioni della crittografia della macchina virtuale

Le seguenti azioni non sono supportate in VMware Cloud Director.

- Crittografare o decrittografare una macchina virtuale accesa o i relativi dischi.
- Esportare un OVF di una macchina virtuale crittografata.
- Crittografare e decrittografare i dischi di una macchina virtuale con uno snapshot se i dischi fanno parte dello snapshot.
- Decrittografare una macchina virtuale quando il relativo disco è in un criterio crittografato.
- Aggiungere un disco crittografato a una macchina virtuale non crittografata.
- Crittografare un disco esistente in una macchina virtuale non crittografata.
- Aggiungere un disco denominato crittografato a una macchina virtuale non crittografata.
- Creare un clone collegato crittografato.
- Crittografare la macchina virtuale o i relativi dischi di un clone collegato.
- Creare un'istanza, spostare o clonare le macchine virtuali nelle istanze di vCenter Server quando la macchina virtuale di origine è crittografata.

Nota In un VDC dell'organizzazione con provisioning rapido, se la macchina virtuale di origine o di destinazione è crittografata e si desidera creare un clone, VMware Cloud Director crea sempre un clone completo.

Identificazione della funzionalità di storage della crittografia di una macchina virtuale

Per impostazione predefinita, gli **amministratori di sistema** e gli **amministratori dell'organizzazione** dispongono dei diritti necessari per visualizzare le funzionalità di storage del VDC dell'organizzazione e per determinare se le macchine virtuali e i dischi sono crittografati. Chi dispone del ruolo **Autore vApp** può visualizzare lo stato di crittografia di una macchina virtuale e i relativi dischi nella pagina **Dettagli** della macchina virtuale. Per ulteriori informazioni su questi ruoli e diritti, vedere [Ruoli predefiniti e relativi diritti](#).



Visualizzazione delle macchine virtuali

È possibile visualizzare macchine virtuali standalone o incluse in una vApp. Le macchine virtuali possono essere visualizzate in una vista griglia o a schede.

Procedura


1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.

2 Scegliere una delle seguenti opzioni.

- Per visualizzare le macchine virtuali in una vista griglia, fare clic su .
- Per visualizzare le macchine virtuali in una vista a schede, fare clic su .

L'elenco delle macchine virtuali viene visualizzato in una vista griglia o come elenco di schede.

3 (Facoltativo) Ordinare l'elenco di macchine virtuali dal menu a discesa **Ordinamento**.

4 (Facoltativo) Nella vista griglia, fare clic su  a sinistra di una macchina virtuale per visualizzare le azioni disponibili per la macchina virtuale selezionata.

Ad esempio, è possibile spegnere una macchina virtuale.

5 Per accedere all'interfaccia del sistema operativo guest della macchina virtuale, fare clic sull'icona del desktop nell'angolo superiore destro della vista a schede.


6 Per visualizzare e modificare i dettagli di una macchina virtuale, fare clic su **Dettagli**.

Creazione di una nuova macchina virtuale standalone

È possibile creare una nuova macchina virtuale standalone.

Procedura

1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.

2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.

3 Fare clic su **Nuova macchina virtuale**.

4 Immettere il nome e il nome del computer per la macchina virtuale.

Importante Il nome del computer può contenere solo caratteri alfanumerici e trattini. Non può essere costituito solo da cifre e non può contenere spazi.

5 (Facoltativo) Immettere una descrizione significativa.

6 Selezionare se si desidera che la macchina virtuale venga accesa subito dopo la creazione.

7 Selezionare la modalità di distribuzione della macchina virtuale.

Opzione	Azione
Nuova	<p>È possibile distribuire una nuova macchina virtuale con impostazioni personalizzabili.</p> <ul style="list-style-type: none"> a Selezionare una famiglia di sistemi operativi e il sistema operativo. b (Facoltativo) Selezionare un'immagine di avvio. c (Facoltativo) Selezionare un criterio di posizionamento della macchina virtuale e un criterio di dimensionamento della macchina virtuale. <p>I menu a discesa dei criteri di posizionamento della macchina virtuale e di dimensionamento della macchina virtuale sono visibili solo se il provider di servizi ha pubblicato tali criteri nel VDC dell'organizzazione.</p> <ul style="list-style-type: none"> d (Facoltativo) Selezionare la dimensione della macchina virtuale dalle opzioni di dimensionamento predefinite o fare clic su Opzioni di dimensionamento personalizzate per specificare manualmente il numero di CPU virtuali e di core per socket, nonché le impostazioni della memoria. <p>Se si seleziona un criterio di dimensionamento della macchina virtuale che definisce la dimensione della macchina virtuale, questa opzione non è visibile.</p> <p>Le dimensioni predefinite della macchina virtuale sono: Piccola, Media e Grande.</p> <ul style="list-style-type: none"> e Specificare le impostazioni di storage per la macchina virtuale, ad esempio il criterio di storage e la dimensione in GB. f Specificare le impostazioni di rete per la macchina virtuale, ad esempio rete, modalità IP, indirizzo IP e NIC primario.
Da modello	<p>È possibile distribuire la macchina virtuale da un modello selezionato nel catalogo dei modelli.</p> <ul style="list-style-type: none"> a Selezionare un modello di macchina virtuale nell'elenco dei modelli disponibili. b (Facoltativo) Selezionare un criterio di posizionamento della macchina virtuale e un criterio di dimensionamento della macchina virtuale. <p>I menu a discesa dei criteri di posizionamento della macchina virtuale e di dimensionamento della macchina virtuale sono visibili solo se il provider di servizi ha pubblicato tali criteri nel VDC dell'organizzazione. Se il modello selezionato dispone di criteri assegnati, potrebbe essere limitato ai criteri del modello predefiniti.</p> <ul style="list-style-type: none"> c (Facoltativo) Scegliere di utilizzare un criterio di storage personalizzato e selezionare il criterio di storage dal menu a discesa Criterio di storage personalizzato da utilizzare. d Leggere e accettare l'accordo di licenza con l'utente finale, se presente.

8 Fare clic su **OK** per salvare le impostazioni della macchina virtuale e avviare il processo di creazione.

Nel catalogo è ora presente la scheda della macchina virtuale. Finché la macchina virtuale non viene creata, il suo stato è **Occupato**.

Provisioning rapido delle macchine virtuali

Il provisioning rapido consente di risparmiare tempo grazie all'utilizzo di cloni collegati per le operazioni di provisioning delle macchine virtuali.

Un clone collegato è un duplicato di una macchina virtuale che utilizza lo stesso disco virtuale dell'originale, con una catena di dischi delta per tenere traccia delle differenze tra l'originale e il clone. Se si disattiva il provisioning rapido, tutte le operazioni di provisioning restituiscono cloni completi.

Un clone collegato non può esistere in un data center o in un archivio dati di vCenter Server diverso da quello della macchina virtuale originale.

Quando si esegue il provisioning rapido di una macchina virtuale, VMware Cloud Director crea una macchina virtuale shadow per supportare la creazione di cloni collegati nei data center e negli archivi dati di vCenter Server per le macchine virtuali associate a un modello di vApp specifico.

Una macchina virtuale shadow è una copia esatta della macchina virtuale originale e viene creata nel data center e nell'archivio dati in cui viene creato il clone collegato.

Importante Il consolidamento sul posto di una macchina virtuale con provisioning rapido non è supportato nei contenitori di archiviazione che utilizzano snapshot nativi. Poiché i volumi virtuali e gli archivi dati abilitati per VAAI utilizzano snapshot nativi, le macchine virtuali con provisioning rapido distribuite in uno di questi contenitori di archiviazione non possono essere consolidate. Per consolidare una macchina virtuale con provisioning rapido distribuita in un volume virtuale o in un archivio dati abilitato per VAAI, è necessario trasferire la macchina virtuale in un contenitore di archiviazione diverso.

Apertura della console di una macchina virtuale

L'accesso alla console di una macchina virtuale consente di visualizzare informazioni sulla macchina virtuale, utilizzare il sistema operativo guest ed eseguire operazioni relative al sistema operativo guest.

Prerequisiti

La macchina virtuale è attivata.

Installazione di VMware Remote Console in un client

VMware Remote Console offre un'interazione utente-guest integrata in tutte le macchine virtuali di cui vengono eseguiti il provisioning e la gestione mediante VMware Cloud Director. Questa sezione illustra le attività necessarie per installare VMware Remote Console in Windows, Apple OS X e Linux.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Utente vApp** predefinito o un set di diritti equivalente.

Procedura

- 1 Scaricare il programma di installazione.
 - Passare alla pagina di download di VMware Remote Console e selezionare il collegamento appropriato per la piattaforma in uso.
www.vmware.com/go/download-vmrc
 - Nella schermata del dashboard **Virtual data center** nel VMware Cloud Director Tenant Portal, fare clic sulla scheda del virtual data center che si desidera esplorare. Selezionare una macchina virtuale e dal menu **Azioni** scegliere **Scarica VMRC**.
- 2 Eseguire l'installazione appropriata per la piattaforma in uso.
 - Se si utilizza Windows, fare doppio clic sul programma di installazione `.msi` e seguire le istruzioni visualizzate.
 - Se si utilizza Linux, accedere con privilegi **root**, eseguire il programma di installazione `.bundle` e seguire le istruzioni visualizzate.
 - Se si utilizza Mac OS, fare doppio clic sul pacchetto `.dmg` per aprirlo, quindi fare doppio clic sull'icona di VMware Remote Console al suo interno per copiarlo nella cartella Applicazioni.

Risultati

Dopo l'installazione, è possibile aprire VMware Remote Console facendo clic sugli URI (Uniform Resource Identifier) che iniziano con lo schema `vmrc://`. Anche VMware Workstation, Player e Fusion sono in grado di gestire lo schema URI `vmrc://`.


Apertura di una console remota della macchina virtuale

È possibile aprire la console di una macchina virtuale utilizzando VMware Remote Console tramite il portale tenant di VMware Cloud Director.

Prerequisiti

- Verificare che VMware Remote Console sia installata nel sistema locale.
- Accertarsi che la macchina virtuale selezionata sia attivata.
- Questa operazione richiede i diritti inclusi nel ruolo **Utente vApp** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.

- 3 Dal menu **Azioni** della macchina virtuale, selezionare **Avvia VM Remote Console**.

Nota Se VMware Remote Console non è installata, viene visualizzata una finestra a comparsa in cui viene richiesto di installare VMware Remote Console o di utilizzare la console Web.

Risultati

La console della macchina virtuale viene aperta come una console remota virtuale esterna.

Nota Quando ci si connette a una macchina virtuale VMware Cloud Director utilizzando VMware Remote Console, è possibile interagire solo con la console (premendo i tasti `Ctrl+Alt+Del`). Non è possibile eseguire operazioni sui dispositivi, operazioni di attivazione o gestire le impostazioni.


Apertura di una console Web

È possibile connettersi alla console di una macchina virtuale anche se VMware Remote Console non è installata nel sistema locale.

Prerequisiti

- Verificare che la macchina virtuale sia attivata.
- Questa operazione richiede i diritti inclusi nel ruolo **Utente vApp** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale, selezionare **Avvia console Web**.

Risultati

La console della macchina virtuale viene aperta in una nuova scheda del browser tramite VMware HTML Console SDK.

Operazioni successive

Fare clic in un punto qualsiasi all'interno della finestra della console per iniziare a utilizzare il mouse, la tastiera e altri dispositivi di input nella console.

Nota Per ulteriori informazioni sulle tastiere internazionali supportate, fare riferimento alla documentazione di VMware HTML Console SDK all'indirizzo <https://www.vmware.com/support/developer/html-console/>.

Esecuzione di operazioni di attivazione nelle macchine virtuali

È possibile eseguire operazioni di attivazione nelle macchine virtuali, ad esempio l'attivazione, la disattivazione, la sospensione o la reimpostazione di una macchina virtuale oppure l'arresto del sistema operativo guest di una macchina virtuale.

Attivazione di una macchina virtuale


Attivare una macchina virtuale equivale ad attivare una macchina fisica.

Non è possibile attivare una macchina virtuale in cui è abilitata la personalizzazione del sistema operativo guest, a meno che non sia installata al suo interno una versione corrente di VMware Tools.

Prerequisiti

La macchina virtuale è disattivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale che si desidera avviare, selezionare **Attiva**.

Risultati

Per una macchina virtuale attivata, lo stato Attivata viene visualizzato in verde.


Disattivazione di una macchina virtuale

Disattivare una macchina virtuale equivale a disattivare una macchina fisica.

Prerequisiti

La macchina virtuale è attivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale che si desidera disattivare, selezionare **Disattiva**.

Risultati

Per una macchina virtuale disattivata, lo stato Disattivata viene visualizzato in rosso.


Arresto di un sistema operativo guest

Arrestare il sistema operativo guest di una macchina virtuale equivale a spegnere una macchina fisica.

Prerequisiti

La macchina virtuale e il sistema operativo guest devono essere attivati.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale, selezionare **Spegni sistema operativo guest**.

Risultati

Il sistema operativo guest viene arrestato.


Reimpostazione di una macchina virtuale

La reimpostazione di una macchina virtuale cancella lo stato (memoria, cache e così via) della macchina virtuale, che però continua a funzionare. Questa operazione equivale alla pressione del pulsante di reimpostazione in una macchina fisica. Avvia infatti un hard reset del sistema operativo senza modificare lo stato di attivazione della macchina virtuale.

Prerequisiti

La macchina virtuale è attivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale da reimpostare, selezionare **Reimposta**.

Risultati

Lo stato della macchina virtuale viene cancellato.

Sospensione di una macchina virtuale


La sospensione di una macchina virtuale ne preserva lo stato corrente scrivendo la memoria sul disco.

La funzionalità di sospensione e ripresa è utile quando si desidera salvare lo stato corrente della macchina virtuale e continuare a lavorare partendo dallo stesso stato in un momento successivo.

Prerequisiti

La macchina virtuale è attivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale da sospendere, selezionare **Sospendi**.

Risultati

La macchina virtuale viene sospesa, ma il suo stato viene mantenuto.


Annullamento dello stato sospeso di una macchina virtuale

Se una macchina virtuale è nello stato di sospensione e non è più necessario riprendere a utilizzarla, è possibile ignorare tale stato. Se si ignora lo stato sospeso, la memoria salvata viene rimossa e per la macchina viene ripristinato lo stato disattivato.

Prerequisiti

Una macchina virtuale in stato sospeso.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale, selezionare **Ignora stato sospeso**.

Risultati

Lo stato viene ignorato e la macchina virtuale viene disattivata.

Attivazione di più macchine virtuali

È possibile attivare più macchine virtuali contemporaneamente.

Non è possibile attivare una macchina virtuale in cui è abilitata la personalizzazione del sistema operativo guest, a meno che non sia installata al suo interno una versione corrente di VMware Tools.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le macchine virtuali che si desidera attivare.
- 4 Dal menu **Azioni**, selezionare **Attiva**.
- 5 Fare clic su **OK** per confermare.

Disattivazione di più macchine virtuali

È possibile disattivare più macchine virtuali contemporaneamente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le macchine virtuali che si desidera disattivare.
- 4 Dal menu **Azioni**, selezionare **Disattiva**.
- 5 Fare clic su **OK** per confermare.

Rimozione dello stato sospeso di più macchine virtuali

Se più macchine virtuali si trovano in stato sospeso e non è più necessario riprenderne l'uso, è possibile rimuovere lo stato sospeso delle macchine virtuali contemporaneamente. Se si rimuove lo stato sospeso, la memoria salvata viene rimossa e le macchine virtuali vengono disattivate.

Prerequisiti

Verificare che le macchine virtuali siano in stato sospeso.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le macchine virtuali per cui si desidera ignorare lo stato sospeso.
- 4 Dal menu **Azioni**, scegliere **Ignora stato sospeso**.
- 5 Fare clic su **OK** per confermare.

Reimpostazione di più macchine virtuali

La reimpostazione di più macchine virtuali contemporaneamente ne cancella lo stato (memoria, cache e così via), mentre la loro esecuzione continua.

Questa operazione equivale alla pressione del pulsante di reimpostazione in una macchina fisica. Avvia infatti un hard reset del sistema operativo senza modificare lo stato di attivazione della macchina virtuale.

Prerequisiti

Verificare che le macchine virtuali siano attivate.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le macchine virtuali che si desidera reimpostare.
- 4 Nel menu **Azioni**, selezionare **Reimposta**.
- 5 Fare clic su **OK** per confermare.

Installazione di VMware Tools in una macchina virtuale

VMware Cloud Director dipende da VMware Tools per la personalizzazione del sistema operativo guest.


VMware Tools migliora la gestione e le prestazioni della macchina virtuale sostituendo i driver generici del sistema operativo con i driver VMware ottimizzati per l'hardware virtuale. VMware Tools viene installato nel sistema operativo guest. Anche se il sistema operativo guest può essere eseguito senza VMware Tools, si perdono praticità e funzionalità importanti.

Prerequisiti

- Verificare che la macchina virtuale sia attivata.
- Se nella macchina virtuale appena creata non è presente un sistema operativo guest, è necessario installarne uno prima di installare VMware Tools.
- Prima di installare VMware Tools, è necessario disattivare la personalizzazione guest.
- Se la versione di VMware Tools è precedente alla 7299 in una macchina virtuale nella vApp, è necessario aggiornarla.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.

- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale in cui si desidera installare VMware Tools, selezionare **Installa VMware Tools**.

VMware Tools viene installato nel sistema operativo guest di destinazione. Se si verifica un errore durante l'installazione, viene visualizzato un messaggio. È inoltre possibile visualizzare l'avanzamento dell'operazione di installazione nella finestra **Task**.
- 4 Per aprire la console Web della macchina virtuale, dal menu **Azioni**, selezionare **Avvia console Web**.
- 5 Per configurare VMware Tools per il sistema operativo specifico in uso, seguire le istruzioni disponibili nell'[articolo 1014294 della Knowledge Base di VMware](#).

Risultati

VMware Tools è installato e configurato nel sistema operativo guest.

Aggiornamento della versione hardware virtuale di una macchina virtuale

È possibile aggiornare la versione hardware virtuale di una macchina virtuale. Le versioni hardware virtuali successive supportano più funzionalità.

Non è possibile eseguire il downgrade della versione hardware delle macchine virtuali in una vApp.

VMware Cloud Director supporta le versioni dell'hardware in base alle risorse vSphere di supporto. La versione dell'hardware supportata dipende dalla versione dell'hardware virtuale supportata più recente nel VDC del provider di supporto. Un **amministratore dell'organizzazione** o un **amministratore di sistema** può impostare la versione dell'hardware su una versione precedente rispetto a quella più recente supportata dall'hardware sottostante. Il portale tenant di VMware Cloud Director imposta in modo dinamico l'elenco delle versioni dell'hardware virtuale selezionabili in base all'hardware di supporto del VDC dell'organizzazione o del provider.


Per informazioni sulle funzionalità hardware disponibili con le impostazioni di compatibilità della macchina virtuale, vedere la *guida all'amministrazione della macchina virtuale vSphere*.

Per informazioni sui prodotti VMware e sulla relativa versione dell'hardware virtuale, vedere <https://kb.vmware.com/s/article/1003746>.

Prerequisiti

- Arrestare la macchina virtuale o la vApp che contiene la macchina virtuale.
- Verificare che nella macchina virtuale sia installata la versione più recente di VMware Tools.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale da aggiornare, selezionare **Aggiorna versione hardware virtuale**.
- 4 Fare clic su **OK**.

Risultati

La macchina virtuale viene aggiornata alla versione più recente.

Modifica delle proprietà di una macchina virtuale

È possibile modificare le proprietà di una macchina virtuale, inclusi il nome e la descrizione, le impostazioni di hardware e rete, le impostazioni del sistema operativo guest e così via.


Modifica delle proprietà generali di una macchina virtuale

È possibile rivedere e modificare il nome, la descrizione e altre proprietà generali di una macchina virtuale.

Prerequisiti

La modifica di proprietà come il sistema operativo richiede lo spegnimento della macchina.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Nella scheda della macchina virtuale che si desidera modificare, fare clic su **Dettagli**.

- 4 L'elenco delle proprietà che è possibile visualizzare o modificare in **Generale** viene espanso per impostazione predefinita.


Opzione	Azione
Nome macchina virtuale	Modificare il nome della macchina virtuale. È possibile modificare questa proprietà mentre la macchina virtuale è accesa.
Nome computer	Modificare il nome del computer o dell'host impostato nel sistema operativo guest che identifica la macchina virtuale in una rete. Il campo può contenere un massimo di 15 caratteri, a causa delle limitazioni sui nomi dei computer del sistema operativo Windows. È possibile modificare questa proprietà mentre la macchina virtuale è accesa.
Descrizione	Modificare la descrizione facoltativa della macchina virtuale. È possibile modificare questa proprietà mentre la macchina virtuale è accesa.
Famiglia sistema operativo	Selezionare una famiglia di sistemi operativi dal menu a discesa. È possibile modificare questa proprietà mentre la macchina virtuale è spenta. Inoltre, non è possibile modificare questa proprietà se nella macchina virtuale è già presente un sistema operativo.
Sistema operativo	Selezionare un sistema operativo dal menu a discesa. È possibile modificare questa proprietà mentre la macchina virtuale è spenta. Inoltre, non è possibile modificare questa proprietà se nella macchina virtuale è già presente un sistema operativo.
Ritardo avvio	Specificare il tempo in millisecondi per il ritardo dell'operazione di avvio. L'intervallo di tempo tra l'attivazione della macchina virtuale e l'uscita dal BIOS seguita dall'avvio del software del sistema operativo guest può essere breve. È possibile modificare il ritardo di avvio per fare in modo che questo intervallo sia più lungo.
Criterio di storage	Selezionare un criterio di storage per la macchina virtuale da usare dal menu a discesa. È possibile modificare questa proprietà mentre la macchina virtuale è accesa.
Virtual data center	Mostra il nome del virtual data center a cui appartiene la macchina virtuale.
VMware Tools	Mostra se nella macchina virtuale è installato VMware Tools.
Versione hardware virtuale	Mostra la versione dell'hardware virtuale della macchina virtuale.
Aggiorna a:	Per eseguire l'aggiornamento, selezionare una versione dal menu a discesa.
Sincronizza ora	Selezionare questa casella di controllo per abilitare la sincronizzazione dell'ora tra il sistema operativo della macchina virtuale e il virtual data center in cui è in esecuzione.
Inserire la configurazione BIOS	Selezionare questa opzione per forzare l'accesso alla schermata di configurazione del BIOS al successivo avvio della macchina virtuale. È possibile modificare questa proprietà mentre la macchina virtuale è spenta.

- 5 Una volta completate le modifiche, fare clic su **Salva**.

Modifica delle proprietà dell'hardware di una macchina virtuale

È possibile rivedere e modificare le proprietà dell'hardware di una macchina virtuale.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Nella scheda della macchina virtuale che si desidera modificare, fare clic su **Dettagli**.
- 4 Fare clic su **Hardware** per espandere l'elenco delle proprietà dell'hardware che è possibile visualizzare e modificare.

Opzione	Descrizione
Numero di CPU virtuali	Modificare il numero di CPU. Il numero massimo di CPU virtuali che è possibile assegnare a una macchina virtuale dipende dal numero di CPU logiche nell'host e dal tipo di sistema operativo guest installato nella macchina virtuale.
Core per socket	Modificare il numero di core per socket. È possibile configurare la modalità di assegnazione delle CPU virtuali in termini di core e core per socket. Stabilire il numero di core della CPU desiderati nella macchina virtuale, quindi selezionare il numero di core per ciascun socket, a seconda che si desideri una CPU single-core, dual-core, tri-core e così via.
Esponi virtualizzazione CPU assistita mediante hardware al sistema operativo guest	È possibile esporre la virtualizzazione CPU completa al sistema operativo guest in modo che le applicazioni che richiedono la virtualizzazione dell'hardware possano essere eseguite nelle macchine virtuali senza conversione binaria o paravirtualizzazione.
Memoria totale	Modificare le impostazioni delle risorse di memoria per una macchina virtuale. Le dimensioni della memoria della macchina virtuale devono essere un multiplo di 4 MB. Questa impostazione determina la quantità di memoria dell'host ESXi allocata per la macchina virtuale. Le dimensioni della memoria dell'hardware virtuale determinano la quantità di memoria disponibile per le applicazioni eseguite nella macchina virtuale. Una macchina virtuale non può utilizzare ulteriori risorse di memoria rispetto alle dimensioni della memoria dell'hardware virtuale configurato.
Aggiunta a caldo della memoria	Se si abilita l'aggiunta a caldo della memoria, è possibile aggiungere risorse di memoria a una macchina virtuale mentre la macchina è accesa. Questa funzionalità è supportata solo su determinati sistemi operativi guest e sulle versioni dell'hardware della macchina virtuale successive alla 7.
Aggiunta a caldo della CPU virtuale	Se si abilita l'aggiunta a caldo di CPU virtuali, è possibile aggiungere CPU virtuali alla macchina virtuale mentre è accesa. È possibile aggiungere solo multipli del numero di core per socket. Questa funzione è supportata solo su determinati sistemi operativi guest e versioni hardware di macchine virtuali.

Opzione	Descrizione
Numero di socket	Mostra il numero di socket. Il numero di socket è determinato dal numero di CPU virtuali disponibili. Il numero cambia quando si aggiorna il numero di CPU virtuali.
Multimedia rimovibile	Visualizza i supporti rimovibili disponibili, ad esempio unità floppy e CD/DVD collegati.

5 In **Dischi rigidi**, fare clic su **Aggiungi** per aggiungere un disco rigido.

Opzione	Descrizione
Dimensioni	<p>Specificare la dimensione del disco rigido in MB. È possibile aumentare le dimensioni del disco rigido in un secondo momento.</p> <p>Nota È possibile aumentare le dimensioni di un disco rigido esistente se la macchina virtuale non è un clone collegato e non dispone di snapshot.</p>
Criterio	<p>Per impostazione predefinita viene utilizzato il criterio di storage per la macchina virtuale.</p> <p>Per impostazione predefinita, tutti i dischi rigidi collegati a una macchina virtuale utilizzano il criterio di storage specificato per la macchina virtuale. È possibile sovrascrivere le impostazioni predefinite per ciascun disco quando si crea una macchina virtuale o se ne modificano le proprietà. La colonna Dimensione per ciascun disco rigido include un menu a discesa che elenca tutti i criteri di storage disponibili per la macchina virtuale.</p>
IOPS	<p>Selezionare un IOPS specifico per il disco.</p> <p>Utilizzare questa opzione per limitare le operazioni di I/O per disco al secondo.</p>
Tipo di bus	<p>Selezionare il tipo di bus.</p> <p>Le opzioni sono Paravirtual (SCSI), LSI Logic parallelo (SCSI), LSI Logic SAS (SCSI), IDE e SATA. Per ulteriori informazioni sui tipi di controller di storage e sulla compatibilità, vedere <i>Guida all'amministrazione della macchine virtuali di vSphere</i>.</p>
Numero bus	Immettere il numero di bus.
Numero unità	Immettere il numero di unità logiche per l'unità disco rigido.

6 In NIC, fare clic su **Aggiungi** per aggiungere una nuova scheda NIC.

È possibile aggiungere fino a 10 NIC. Per informazioni sul numero di NIC supportate in base alla versione dell'hardware della macchina virtuale, vedere: <http://kb.vmware.com/s/article/2051652>. VMware Cloud Director supporta la modifica delle NIC di una macchina virtuale mentre la macchina virtuale è in esecuzione. Per informazioni sui tipi di schede di rete supportati, vedere <http://kb.vmware.com/kb/1001805>.

Opzione	Descrizione
NIC primaria	Viene visualizzato un contrassegno quando si seleziona la scheda NIC primaria. Selezionare una scheda NIC primaria. L'impostazione della NIC primaria determina il gateway predefinito e unico per la macchina virtuale. La macchina virtuale può utilizzare qualsiasi NIC per connettersi alle macchine virtuale e fisiche direttamente connesse alla stessa rete della NIC, ma può utilizzare soltanto la NIC primaria per connettersi alle macchine sulle reti che richiedono una connessione al gateway.
NIC	Numero della scheda NIC.
Connessa	Selezionare la casella di controllo per collegare una scheda NIC.
Rete	Selezionare una rete nel menu a discesa.
Modalità IP	Selezionare una modalità IP. Attenzione Se è stata selezionata una rete a cui connettere la scheda NIC, non impostare la modalità IP su Nessuno . <ul style="list-style-type: none"> ■ Statico - Pool IP Estrae un indirizzo IP statico dal pool di indirizzi IP della rete. ■ Statico - Manuale Consente di specificare manualmente un indirizzo IP specifico. Se si seleziona questa opzione, è necessario digitare un indirizzo IP nella colonna Indirizzo IP. ■ DHCP Estrae un indirizzo IP da un server DHCP.
Indirizzo MAC	Nel menu a discesa, selezionare se mantenere o reimpostare l'indirizzo MAC.

7 Fare clic su **Salva**.

Modifica delle proprietà di personalizzazione del sistema operativo guest di una macchina virtuale


La personalizzazione del sistema operativo guest su VMware Cloud Director è facoltativa per tutte le piattaforme. È necessaria per le macchine virtuali che devono essere aggiunte a un dominio Windows.

Alcune delle informazioni richieste in questo menu si applicano solo alle piattaforme Windows. Il riquadro Personalizzazione sistema operativo guest contiene le informazioni necessarie per aggiungere la macchina virtuale a un dominio Windows. Un **Amministratore organizzazione** può specificare valori predefiniti per un dominio a cui possono essere aggiunti i guest Windows presenti nell'organizzazione. Non tutte le macchine virtuali Windows devono essere aggiunte a un dominio, ma nella maggior parte delle installazioni aziendali una macchina virtuale che non fa parte di un dominio non può accedere a molte delle risorse di rete disponibili.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Autore vApp** predefinito o un set di diritti equivalente.
- Per la personalizzazione del guest, è necessario che nella macchina virtuale sia in esecuzione VMware Tools.
- Prima di poter personalizzare un sistema operativo guest Windows, è necessario che l'**amministratore di sistema** installi i file di Microsoft Sysprep appropriati nel gruppo di server di VMware Cloud Director. Vedere *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.
- Per personalizzare sistemi operativi guest Linux è necessario che sul guest sia installato Perl.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Nella scheda della macchina virtuale che si desidera modificare, fare clic su **Dettagli**.
- 4 Fare clic su **Personalizzazione sistema operativo guest e Proprietà** per espandere l'elenco delle impostazioni del sistema operativo guest.

Opzione	Descrizione
Abilita personalizzazione guest	Selezionare questa opzione per abilitare la personalizzazione del guest.
Modifica SID	Selezionare questa opzione per modificare l'ID di sicurezza Windows (SID). Questa opzione è specifica per le macchine virtuali che eseguono un sistema operativo guest Windows. Il SID viene utilizzato in alcuni sistemi operativi Windows per identificare univocamente sistemi e utenti. Se non si seleziona questa opzione, la nuova macchina virtuale avrà lo stesso SID della macchina virtuale o del modello su cui è basata. SID duplicati non causano problemi quando i computer fanno parte di un dominio e sono utilizzati solo account utente del dominio. Tuttavia, se i computer fanno parte di un gruppo di lavoro o se vengono utilizzati account utente locali, eventuali SID duplicati possono compromettere i controlli di accesso ai file. Per ulteriori informazioni, consultare la documentazione del sistema operativo Microsoft Windows.

Opzione	Descrizione
Consenti password amministratore locale	<p>Selezionare questa opzione per consentire l'impostazione di una password di amministratore nel sistema operativo guest.</p> <ul style="list-style-type: none"> a Specificare una password per l'amministratore locale. <p>Se si lascia vuota la casella di testo Specifica password, la password viene generata automaticamente.</p> <ul style="list-style-type: none"> b Specificare il numero di accessi automatici consentiti. <p>Se si immette il valore zero, l'accesso automatico come amministratore viene disattivato.</p>
Richiedi all'amministratore di cambiare la password al primo login	<p>Selezionare questa opzione per richiedere all'amministratore di cambiare la password del sistema operativo guest al primo login. Questa opzione è consigliata per motivi di sicurezza.</p>
Genera automaticamente password	<p>Selezionare questa opzione per consentire la generazione automatica della password.</p>
Abilita la macchina virtuale per l'aggiunta a un dominio	<p>È possibile selezionare questa opzione per aggiungere la macchina virtuale a un dominio Windows. È possibile utilizzare il dominio dell'organizzazione oppure sostituirlo e specificare le proprietà del dominio.</p> <ul style="list-style-type: none"> a Immettere il nome del dominio. b Immettere il nome utente e la password. c Immettere l'unità organizzativa dell'account.
Script	<p>È possibile utilizzare uno script di personalizzazione per modificare il sistema operativo guest della macchina virtuale. Quando si aggiunge uno script di personalizzazione a una macchina virtuale, lo script viene richiamato solo durante la personalizzazione iniziale e quando si forza una nuova personalizzazione. Se si imposta il parametro della riga di comando <code>precustomization</code>, lo script viene richiamato prima dell'inizio della personalizzazione del guest. Se si imposta il parametro della riga di comando <code>postcustomization</code>, lo script viene richiamato al termine della personalizzazione del guest.</p> <ul style="list-style-type: none"> ■ Fare clic sul pulsante Carica sotto la casella di testo dello script per passare a uno script di personalizzazione nella macchina locale. ■ Digitare lo script di personalizzazione direttamente nella casella di testo File script. <p>Uno script di personalizzazione immesso direttamente nella casella di testo File script non può contenere più di 1500 caratteri. Per ulteriori informazioni, vedere l'articolo della Knowledge Base di VMware https://kb.vmware.com/kb/1026614.</p>

5 Una volta completate le modifiche, fare clic su **Salva**.

Informazioni generali sulla personalizzazione del sistema operativo guest

Quando si personalizza il sistema operativo guest, è necessario conoscere la funzione di alcune impostazioni e opzioni.

Casella di controllo **Abilita personalizzazione guest**

Questa casella di controllo si trova nella scheda **Personalizzazione sistema operativo guest** nella pagina **Proprietà** della macchina virtuale. L'obiettivo della personalizzazione guest è di effettuare la configurazione in base alle opzioni selezionate nella pagina **Proprietà**. Se questa casella di controllo è selezionata, la personalizzazione e la nuova personalizzazione del sistema operativo guest vengono eseguite quando è necessario.

Questo processo è obbligatorio per consentire il funzionamento di tutte le funzionalità di personalizzazione del sistema operativo guest, ad esempio il nome del computer, le impostazioni di rete, l'impostazione e la scadenza delle password di amministratore e dell'utente root, la modifica del SID per i sistemi operativi Windows e così via. Questa opzione deve essere selezionata affinché **Attiva e forza nuova personalizzazione** funzioni.

Se la casella di controllo è selezionata e i parametri di configurazione della macchina virtuale in VMware Cloud Director non sono sincronizzati con le impostazioni nel sistema operativo guest, la scheda **Profilo** nella pagina **Proprietà** della macchina virtuale indica che le impostazioni non sono sincronizzate con il sistema operativo guest e che la macchina virtuale richiede una personalizzazione del guest.

Comportamento della personalizzazione del sistema operativo guest per vApp e macchine virtuali

Le caselle di controllo sono deselezionate.

- **Abilita personalizzazione guest**
- Nei sistemi operativi guest Windows, **Modifica SID**
- **Reimpostazione password**

Se si desidera eseguire la personalizzazione (o sono state apportate modifiche alle impostazioni di rete che devono essere riflesse nel sistema operativo guest), è possibile selezionare la casella di controllo **Abilita personalizzazione guest** e impostare le opzioni nella scheda **Personalizzazione sistema operativo guest** della pagina **Proprietà** della macchina virtuale. Quando si utilizzano macchine virtuali di modelli di vApp per creare una vApp e quindi si aggiunge una macchina virtuale, i modelli di vApp rappresentano gli elementi costitutivi. Quando si aggiungono macchine virtuali di un catalogo in una nuova vApp, le macchine virtuali vengono abilitate per la personalizzazione del sistema operativo guest per impostazione predefinita. Quando si salva un modello di vApp di un catalogo come vApp, le macchine virtuali vengono abilitate per la personalizzazione del sistema operativo guest solo se la casella di controllo **Abilita personalizzazione guest** è selezionata.

Di seguito sono indicate le impostazioni predefinite della personalizzazione del sistema operativo guest.

- La casella di controllo **Abilita personalizzazione guest** corrisponde a quella della macchina virtuale di origine del catalogo.
- Per le macchine virtuali guest Windows, l'opzione **Modifica SID** corrisponde a quella della macchina virtuale di origine del catalogo.

- L'impostazione di reimpostazione della password corrisponde a quella della macchina virtuale di origine del catalogo.

È possibile deselezionare la casella di controllo **Abilita personalizzazione guest**, se necessario, prima di avviare la vApp.

Se a una vApp vengono aggiunte macchine virtuali vuote in cui l'installazione del sistema operativo guest è in sospeso, la casella di controllo **Abilita personalizzazione guest** è deselezionata per impostazione predefinita in quanto queste macchine virtuali non sono pronte per la personalizzazione.

Dopo aver installato il sistema operativo guest e VMware Tools, è possibile disattivare le macchine virtuali, arrestare la vApp e selezionare la casella di controllo **Abilita personalizzazione guest**, quindi avviare la vApp e le macchine virtuali per eseguire la personalizzazione guest.

Se il nome della macchina virtuale e le impostazioni di rete vengono aggiornati su una macchina virtuale che è stata personalizzata, al successivo riavvio la personalizzazione viene ripetuta e di conseguenza la macchina virtuale guest viene risincronizzata con VMware Cloud Director.

Come attivare e forzare la nuova personalizzazione di una macchina virtuale

È possibile attivare una macchina virtuale e forzare una nuova personalizzazione di una macchina virtuale.


Se le impostazioni in una macchina virtuale non sono sincronizzate con VMware Cloud Director o un tentativo di eseguire la personalizzazione di un sistema operativo guest non è riuscito, è possibile forzare la nuova personalizzazione della macchina virtuale.

Assicurarsi che l'applicazione in esecuzione nella macchina virtuale supporti una nuova personalizzazione. Se si modifica un controller di dominio utilizzando Microsoft Sysprep e si modifica anche il SID, è possibile che la macchina virtuale venga danneggiata. Per ridurre il rischio di danneggiare la macchina virtuale, creare una snapshot prima di eseguire la nuova personalizzazione.

Prerequisiti

- È necessario essere un amministratore dell'organizzazione.
- È necessario che la macchina virtuale sia disattivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Attivazione** della macchina virtuale che si desidera attivare e personalizzare, selezionare **Attiva e forza nuova personalizzazione**.

Risultati

La macchina virtuale viene attivata e viene eseguita una nuova personalizzazione.

Modifica delle proprietà avanzate di una macchina virtuale

Nelle impostazioni **Avanzate**, è possibile configurare le impostazioni di allocazione delle risorse (condivisioni, prenotazione e limite) per determinare la quantità di CPU, memoria e risorse di storage fornite per una macchina virtuale.

Utilizzare le impostazioni di allocazione di risorse (condivisioni, prenotazione e limite) per determinare la quantità di CPU, memoria e risorse di storage fornite per una macchina virtuale.

Condivisioni dell'allocazione di risorse

Le condivisioni specificano l'importanza relativa di una macchina virtuale all'interno di un virtual data center. Se una macchina virtuale dispone di una quantità doppia di condivisioni di una risorsa rispetto a un'altra macchina virtuale, può consumare una quantità doppia della risorsa in questione nel caso in cui entrambe le macchine necessitino di risorse. Le condivisioni in genere sono specificate come Alta, Normale o Bassa e queste voci corrispondono a valori della condivisione con un rapporto di 4:2:1 rispettivamente. È inoltre possibile selezionare Personalizzata per assegnare un numero specifico di condivisioni (che esprime un peso proporzionale) a ciascuna macchina virtuale. Quando si assegnano condivisioni a una macchina virtuale, si specifica sempre la priorità per quella macchina virtuale rispetto ad altre macchine virtuali attivate.

Prenotazione dell'allocazione di risorse

Questa opzione specifica l'allocazione minima garantita per una macchina virtuale. VMware Cloud Director consente di attivare una macchina virtuale solo se è disponibile una quantità di risorse non prenotate sufficiente a soddisfare la prenotazione della macchina virtuale. Il virtual data center garantisce questa quantità anche quando le risorse sono molto sovraccariche. La prenotazione viene espressa in unità misurabili (megahertz o megabyte).

Si supponga ad esempio di avere 2 GHz disponibili e di specificare una prenotazione di allocazione delle risorse di 1 GHz per la macchina virtuale 1 e di 1 GHz per la macchina virtuale 2. Ora ogni macchina virtuale può contare su 1 GHz, se necessario. Tuttavia, se la macchina virtuale 1 utilizza solo 500 MHz, la macchina virtuale 2 può utilizzare 1,5 GHz.

Per impostazione predefinita, il valore della prenotazione è 0. È possibile specificare una prenotazione se è necessario garantire che le quantità minime richieste di CPU o memoria siano sempre disponibili per la macchina virtuale.

Limite di allocazione di risorse

Questa opzione specifica un limite superiore per le risorse di CPU e memoria che è possibile allocare a una macchina virtuale. Un virtual data center può allocare a una macchina virtuale una quantità di risorse superiore alla prenotazione, ma non supera mai il limite di allocazione, anche se nel sistema sono presenti risorse inutilizzate. Il limite viene espresso in unità misurabili (megahertz o megabyte).


L'impostazione predefinita è l'assenza di limiti delle risorse di memoria e di CPU. Quando non è impostato un limite della memoria, la quantità di memoria configurata per la macchina virtuale al momento della creazione diventa in molti casi il limite effettivo.

Spesso non è necessario specificare un limite. Se viene specificato, infatti, è possibile che vadano sprecate risorse inattive. Il sistema non consente a una macchina virtuale di utilizzare una quantità di risorse superiore rispetto al limite, anche quando non viene completamente utilizzato e sono disponibili risorse inattive. Specificare un limite solo se è assolutamente necessario.

Prerequisiti

- Un virtual data center del pool di prenotazioni.
- Verificare che il virtual data center fornisca una determinata quantità di memoria per una macchina virtuale.
- Assicurarci che a una determinata macchina virtuale sia sempre allocata una percentuale più elevata di risorse del virtual data center rispetto alle altre macchine virtuali.
- Impostare un limite superiore sulle risorse che sia possibile allocare a una macchina virtuale.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Nella scheda della macchina virtuale che si desidera modificare, fare clic su **Dettagli**.
- 4 Fare clic su **Avanzate** e su **Modifica**.
- 5 Impostare le condivisioni delle allocazioni di risorse per le impostazioni della CPU selezionando un'opzione dal menu a discesa **Priorità**.

Opzione	Descrizione
Bassa	Alloca 500 condivisioni per CPU virtuale.
Normale	Alloca 1000 condivisioni per CPU virtuale.
Alta	Alloca 2000 condivisioni per CPU virtuale.
Ad hoc	Consente di assegnare un numero specifico di condivisioni immettendo il numero di condivisioni (che esprime un peso proporzionale) per ogni macchina virtuale. Quando si assegnano condivisioni a una macchina virtuale, si specifica sempre la priorità per quella macchina virtuale rispetto ad altre macchine virtuali attivate.

- 6 Specificare la prenotazione per le impostazioni della CPU inserendo la prenotazione in MHz e, facoltativamente, il limite per le impostazioni della CPU in MHz.

Opzione	Descrizione
Illimitato	L'opzione della risorsa CPU predefinita.
Massimo	Specificare un limite superiore per le risorse CPU che è possibile allocare a una macchina virtuale in MHz.

- 7 Impostare le condivisioni delle allocazioni di risorse per le impostazioni della memoria selezionando un'opzione dal menu a discesa **Priorità**.

Opzione	Descrizione
Bassa	Alloca 5 condivisioni per megabyte di memoria della macchina virtuale configurata.
Normale	Alloca 10 condivisioni per megabyte di memoria della macchina virtuale configurata.
Alta	Alloca 20 condivisioni per megabyte di memoria della macchina virtuale configurata.
Ad hoc	Consente di assegnare un numero di condivisioni specifico inserendo il numero di condivisioni.

- 8 Specificare la prenotazione per le impostazioni di memoria in MB e, facoltativamente, il limite per le impostazioni della memoria in MB.

Opzione	Descrizione
Illimitato	L'opzione della risorsa di memoria predefinita.
Massimo	Specificare un limite superiore per la prenotazione di memoria che è possibile allocare a una macchina virtuale.

- 9 Fare clic su **Salva**.

Inserisci file multimediale


È possibile inserire file multimediali, ad esempio immagini di CD/DVD da cataloghi, per utilizzarli nel sistema operativo guest di una macchina virtuale. È possibile utilizzare questi file multimediali per installare un sistema operativo nella macchina virtuale, varie applicazioni, driver e così via.

Prerequisiti

Si supponga di avere accesso a un catalogo contenente file multimediali.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.

- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Selezionare la macchina virtuale in cui si desidera aggiungere i file multimediali.
- 4 Dal menu **Azioni**, scegliere **Inserisci file multimediale**.
- 5 Nella finestra **Inserisci CD**, scegliere il file multimediale da inserire nella macchina virtuale.
- 6 Fare clic su **Inserisci**.


Espelli file multimediale

Dopo avere utilizzato un CD o un DVD nella macchina virtuale, è possibile espellere il multimedia.

Prerequisiti

Un multimedia deve essere stato in precedenza inserito nella macchina virtuale.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Selezionare la macchina virtuale da cui si desidera espellere il multimedia.
- 4 Dal menu **Azioni**, scegliere **Espelli file multimediale**.

Risultati

Il file multimediale viene espulso.

Copia di una macchina virtuale in una vApp diversa


È possibile copiare una macchina virtuale in un'altra vApp. Quando si copia una macchina virtuale, la macchina virtuale originale rimane nella vApp di origine.

Quando si copia una macchina virtuale, gli snapshot non vengono inclusi nella copia.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Autore vApp** predefinito o un set di diritti equivalente.
- Disattivare la macchina virtuale.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale da copiare, selezionare **Copia in**.
- 4 Selezionare la vApp di destinazione in cui si desidera copiare la macchina virtuale e fare clic su **Avanti**.
- 5 Configurare le risorse, come il nome della macchina virtuale e il nome del computer e, facoltativamente, i criteri di storage e le schede NIC, quindi fare clic su **Avanti**.

Importante Il nome del computer può contenere solo caratteri alfanumerici e trattini. Non può essere costituito solo da cifre e non può contenere spazi.

- 6 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Spostamento di una macchina virtuale in una vApp diversa

È possibile spostare una macchina virtuale in un'altra vApp. Quando si sposta una macchina virtuale, VMware Cloud Director rimuove la macchina virtuale originale dalla vApp di origine.

Quando si sposta una macchina virtuale in una vApp diversa, gli snapshot creati vengono persi.

Lo spostamento di macchine virtuali tra vApp diverse si basa su VMware vSphere[®] vMotion[®] e su Enhanced vMotion Compatibility (EVC). È possibile spostare una macchina virtuale in una vApp diversa appartenente allo stesso VDC dell'organizzazione oppure a un altro VDC dell'organizzazione all'interno della stessa organizzazione. Il VDC dell'organizzazione può trovarsi nello stesso VDC del provider o in un altro.

Durante il trasferimento di una macchina virtuale in una vApp diversa, è possibile eseguire operazioni di riconfigurazione, come la modifica della rete e del profilo di storage.


Tabella 2-1. Operazioni di riconfigurazione durante i trasferimenti delle macchine virtuali e stati delle macchine virtuali

Riconfigurazione	Stato della macchina virtuale se la vApp di destinazione è nel VDC della stessa organizzazione	Stato della macchina virtuale se la vApp di destinazione è nel VDC di un'altra organizzazione all'interno dello stesso provider di VDC
modifica della rete	disattivata	N/D
rimozione della rete	attivata o disattivata	N/D
modifica del profilo di storage	attivata o disattivata	disattivata

Prerequisiti

- Verificare di disporre del ruolo **Autore vApp** o di un set di diritti equivalente.
- Verificare che le risorse vSphere sottostanti supportino vMotion ed EVC. Per informazioni su requisiti e limitazioni di vMotion ed EVC, vedere *vCenter Server e gestione degli host*.
- Verificare se per modificare la rete della macchina virtuale o il profilo di storage è necessario spegnere la macchina virtuale. Vedere la tabella *Operazioni di riconfigurazione durante gli spostamenti della macchina virtuale e stati della macchina virtuale*.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina che si desidera spostare, selezionare **Sposta in**.
- 4 Selezionare la vApp di destinazione e fare clic su **Avanti**.
- 5 Configurare le risorse, come il nome della macchina virtuale e il nome del computer e, facoltativamente, il criterio di storage e le schede NIC, quindi fare clic su **Avanti**.

Importante Il nome del computer può contenere solo caratteri alfanumerici e trattini. Non può essere costituito solo da cifre e non può contenere spazi.

- 6 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Affinità e anti-affinità delle macchine virtuali

Le regole di affinità e di anti-affinità consentono di distribuire un gruppo di macchine virtuali su diversi host ESXi o di raggrupparle su un host ESXi specifico.


Una regola di affinità posiziona un gruppo di macchine virtuali in un host specifico in modo che sia possibile controllare facilmente l'utilizzo di tali macchine. Una regola di anti-affinità posiziona un gruppo di macchine virtuali su diversi host, in modo da evitare che tutte le macchine virtuali restituiscano simultaneamente un errore in caso di problemi con un singolo host.

Se non è possibile soddisfare le regole di affinità o anti-affinità, le macchine virtuali aggiunte alla regola non possono essere attivate.

Visualizzazione delle regole di affinità e di anti-affinità

È possibile visualizzare le regole di affinità e di anti-affinità esistenti e le relative proprietà, ad esempio l'attivazione delle regole e le macchine virtuali da queste interessate.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Regole di affinità** nel pannello sinistro.
- 2 (Facoltativo) Fare clic sull'icona **Editor della griglia** () e selezionare i dettagli delle regole che si desidera vengano visualizzati.

Risultati

Viene visualizzato l'elenco delle regole di affinità e anti-affinità esistenti, le macchine virtuali e lo stato di abilitazione di ciascuna regola.

Creazione di una regola di affinità

Creare una regola di affinità per posizionare un gruppo di macchine virtuali specifico in un singolo host, in modo da poter controllare l'utilizzo di tali macchine virtuali.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Regole di affinità** nel pannello sinistro.
- 2 In **Regole di affinità**, fare clic su **Nuova**.
- 3 Immettere il nome della regola.
- 4 Deselezionare **Abilitato** per creare la regola senza abilitarla.
Per impostazione predefinita, la casella di controllo è selezionata e le regole vengono abilitate dopo essere state create.
- 5 Lasciare selezionata la casella di controllo **Obbligatorio**.
Per impostazione predefinita, ogni regola di affinità è obbligatoria. Ciò indica che se la regola non può essere soddisfatta, le macchine virtuali aggiunte alla regola non vengono attivate.
- 6 Selezionare le macchine virtuali da aggiungere alla regola di affinità.
- 7 Fare clic su **Salva**.

Risultati

VMware Cloud Director posiziona in un unico host le macchine virtuali associate alla regola di affinità.

Creazione di una regola di anti-affinità

Creare una regola di anti-affinità per posizionare un gruppo di macchine virtuali specifico in più host per evitare che tutte le macchine virtuali smettano di funzionare contemporaneamente se si verifica un problema in un singolo host.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Regole di affinità** nel pannello sinistro.
- 2 In **Regole di anti-affinità**, fare clic su **Nuova**.
- 3 Immettere il nome della regola.
- 4 Deselezionare **Abilitato** per creare la regola senza abilitarla.

Per impostazione predefinita, la casella di controllo è selezionata e le regole vengono abilitate dopo essere state create.
- 5 Lasciare selezionata la casella di controllo **Obbligatorio**.

Per impostazione predefinita, ogni regola di anti-affinità è obbligatoria. Ciò indica che se la regola non può essere soddisfatta, le macchine virtuali aggiunte alla regola non vengono attivate.
- 6 Selezionare le macchine virtuali da aggiungere alla regola di anti-affinità.
- 7 Fare clic su **Salva**.

Risultati

VMware Cloud Director posiziona in più host le macchine virtuali associate alla regola di anti-affinità.

Modifica di una regola di affinità o di anti-affinità

È possibile modificare una regola di affinità o anti-affinità per attivare o disattivare la regola, aggiungere o rimuovere macchine virtuali, nonché modificare il nome o la preferenza della regola.

Prerequisiti

Questa operazione richiede il diritto `Organization vDC: VM-VM Affinity Edit` . Il diritto è incluso nei ruoli predefiniti **Autore catalogo**, **Autore vApp** e **Amministratore organizzazione**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Regole di affinità** nel pannello sinistro.
- 2 Fare clic sul pulsante di opzione accanto al nome della regola che si desidera modificare e fare clic su **Modifica**.
- 3 Modificare le proprietà della regola.
 - a Modificare il nome della regola in base alle necessità.
 - b Selezionare se attivare o disattivare la regola.
 - c Lasciare selezionata la casella di controllo **Obbligatorio**.
 - d Aggiungere più macchine virtuali o rimuovere macchine virtuali.

- 4 Fare clic su **Salva**.

Eliminazione di una regola di affinità o di anti-affinità

Se non si desidera più utilizzare una regola di affinità o di anti-affinità, è possibile eliminarla.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Regole di affinità** nel pannello sinistro.
- 2 Fare clic sul pulsante di opzione accanto al nome della regola che si desidera eliminare e fare clic su **Elimina**.
- 3 Per confermare che si desidera eliminare la regola, fare clic su **OK**.

Risultati

VMware Cloud Director elimina la regola di affinità o anti-affinità.

Monitoraggio delle macchine virtuali


Se l'amministratore di VMware Cloud Director ha abilitato la funzionalità per il monitoraggio delle macchine virtuali, è possibile visualizzare il grafico del monitoraggio dal portale tenant.

Utilizzare questa funzionalità per analizzare lo stato di una determinata macchina virtuale nel tempo (giorni, settimane o mesi).

Prerequisiti

Questa funzionalità è disponibile solo se è stata abilitata dall'amministratore di VMware Cloud Director.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Selezionare la macchina virtuale che si desidera monitorare e fare clic su **Dettagli**.
- 4 Fare clic su **Monitoraggio del grafico** per espandere la visualizzazione di monitoraggio.
Verrà visualizzato il grafico del monitoraggio.

5

6 Selezionare un'opzione metrica per il monitoraggio delle macchine virtuali.

L'elenco nel menu a discesa **Metrica** varia in base alle scelte dell'**amministratore di sistema**. Saranno visibili alcune o tutte le opzioni.

Metrica	Descrizione
Disk provisioned latest	Specificata in KB. Scegliere la vista giornaliera, settimanale o mensile.
Disk read average	Specificata come percentuale. Scegliere la vista giornaliera, settimanale o mensile.
Disk write average	Specificata come percentuale. Scegliere la vista giornaliera, settimanale o mensile.
CPU usage average	Specificata come percentuale. Scegliere la vista giornaliera, settimanale o mensile.
Utilizzo CPU medio (MHz)	Specificata in MHz. Scegliere la vista giornaliera, settimanale o mensile.
CPU usage maximum	Specificata come percentuale. Scegliere la vista giornaliera, settimanale o mensile.
Mem usage average	Specificata come percentuale. Scegliere la vista giornaliera, settimanale o mensile.
Disk used latest	Specificata in KB. Scegliere la vista giornaliera, settimanale o mensile.

Ogni volta che si seleziona un valore diverso nell'elenco, viene visualizzato un nuovo grafico.

7 (Facoltativo) Modificare l'intervallo di tempo per la raccolta delle metriche.

8 Fare clic su **Aggiorna**.

9 Per salvare le modifiche, fare clic su **Salva**.

Utilizzo di snapshot

Le snapshot conservano lo stato e i dati di una macchina virtuale al momento della creazione della snapshot. La creazione di una snapshot di una macchina virtuale non influisce sulla macchina virtuale. Viene infatti copiata e memorizzata solo un'immagine della macchina virtuale in un determinato stato. Le snapshot sono utili quando è necessario ripristinare più volte lo stesso stato della macchina virtuale, ma non si desidera creare più macchine virtuali.

Le snapshot sono utili come soluzione a breve termine per il test di software con effetti sconosciuti o potenzialmente dannosi. Ad esempio, è possibile utilizzare una snapshot come punto di ripristino durante un processo lineare o iterativo, come l'installazione di pacchetti di aggiornamento o durante un processo di diramazione, come l'installazione di versioni diverse di un programma.

È consigliabile utilizzare uno snapshot durante l'aggiornamento del sistema operativo di una macchina virtuale. Ad esempio, prima di aggiornare la macchina virtuale, è possibile creare una snapshot per conservare i dati relativi al momento precedente all'aggiornamento. Se l'aggiornamento viene eseguito senza problemi, è possibile scegliere di rimuovere lo snapshot. Questa operazione comporterà il commit delle modifiche apportate durante l'aggiornamento. Tuttavia, se si verifica un problema, è possibile ripristinare la snapshot per tornare allo stato della macchina virtuale salvato prima dell'aggiornamento.

Con VMware Cloud Director è possibile avere una sola snapshot di una macchina virtuale. Ogni volta che si effettua un tentativo di creare una nuova snapshot di una macchina virtuale, la snapshot precedente viene eliminata.

Creazione dello snapshot di una macchina virtuale

È possibile creare lo snapshot di una macchina virtuale. Dopo aver creato lo snapshot, è possibile utilizzarlo per ripristinare la macchina virtuale oppure rimuoverlo.


Prerequisiti

Verificare che la macchina virtuale non sia connessa a un disco denominato.

Nota Gli snapshot non acquisiscono le configurazioni NIC.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.

- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.

- 3 Dal menu **Azioni** della macchina virtuale per cui si desidera creare uno snapshot, selezionare **Crea snapshot**.

Se si crea uno snapshot di una macchina virtuale, viene sostituito lo snapshot eventualmente esistente.

- 4 (Facoltativo) Scegliere se creare lo snapshot della memoria della macchina virtuale.

Quando si acquisisce lo stato della memoria della macchina virtuale, lo snapshot conserva lo stato attivo della macchina virtuale. Lo snapshot della memoria viene creato in un istante preciso, ad esempio per aggiornare software ancora in esecuzione. Se si crea uno snapshot della memoria e l'aggiornamento non viene completato come previsto oppure il software non soddisfa le aspettative, è possibile ripristinare lo stato precedente della macchina virtuale.

Quando si acquisisce lo stato della memoria, i file della macchina virtuale non richiedono la disattivazione. Se non si acquisisce lo stato della memoria, lo snapshot non salva lo stato attivo della macchina virtuale e i dischi sono coerenti con l'arresto anomalo del sistema, a meno che non vengano disattivati.

5 (Facoltativo) Scegliere se disattivare il file system guest.

Per eseguire questa operazione è necessario che nella macchina virtuale sia installato VMware Tools. Quando si disattiva una macchina virtuale, VMware Tools disattiva il file system della macchina virtuale. Un'operazione di disattivazione garantisce che un disco di snapshot rappresenti uno stato coerente dei file system guest. Gli snapshot con disattivazione sono appropriati per backup automatici o periodici. Ad esempio, se non si conosce l'attività della macchina virtuale, ma si desidera ripristinare alcuni backup recenti, è possibile disattivare i file.

Non è possibile disattivare macchine virtuali con dischi di grande capacità.

6 Fare clic su **OK**.

Risultati

Lo snapshot consente di ripristinare la macchina virtuale allo snapshot più recente.


Ripristino dello snapshot di una macchina virtuale

È possibile ripristinare una macchina virtuale allo stato in cui si trovava quando lo snapshot è stato creato.

Prerequisiti

La macchina virtuale dispone di uno snapshot.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale di cui si desidera ripristinare uno snapshot, selezionare **Ripristina snapshot**.
- 4 Fare clic su **OK**.

Risultati

Viene ripristinato lo snapshot salvato della macchina virtuale.

Rimozione di una snapshot di una macchina virtuale


È possibile rimuovere lo snapshot di una macchina virtuale.

Quando si rimuove una snapshot, lo stato della macchina virtuale conservato nella snapshot viene eliminato definitivamente. La rimozione di uno snapshot non influisce sullo stato attuale della macchina virtuale.

Prerequisiti

Una macchina virtuale con uno snapshot archiviato.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale per cui si desidera rimuovere lo snapshot, selezionare **Rimuovi snapshot**.
- 4 Fare clic su **OK**.


Rinnovo del lease di una macchina virtuale

È possibile rinnovare il lease di una macchina virtuale se sta per scadere.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale con il lease in scadenza, selezionare **Rinnova lease**.

Risultati

Il lease viene rinnovato. Nel campo **Lease** viene visualizzata la nuova durata del lease.

Eliminazione di una macchina virtuale


È possibile eliminare una macchina virtuale dall'organizzazione.

Prerequisiti

È necessario che la macchina virtuale sia disattivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.

- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Dal menu **Azioni** della macchina virtuale che si desidera eliminare, selezionare **Elimina**.
- 4 Confermare l'eliminazione.

Risultati

La macchina virtuale viene eliminata.

Gruppi di scalabilità automatica

A partire da VMware Cloud Director 10.2.2, è possibile scalare automaticamente le applicazioni in base all'utilizzo corrente di CPU e memoria.

Per informazioni sulla configurazione della soluzione di scalabilità automatica, vedere [Gruppi di scalabilità automatica](#) nella *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

In base a criteri predefiniti per l'utilizzo di CPU e memoria, VMware Cloud Director può aumentare o ridurre automaticamente il numero di macchine virtuali contenute in un gruppo di scalabilità selezionato. Per bilanciare il carico dei server configurati dall'utente per eseguire la stessa applicazione, è possibile utilizzare VMware NSX Advanced Load Balancer (Avi Networks).

I ruoli **Amministratore di sistema** e **Amministratore organizzazione** dispongono del controllo completo sulle macchine virtuali nei gruppi di scalabilità. Gli altri ruoli tenant globali possono visualizzare le macchine virtuali e accedere alla console Web delle macchine virtuali, ma non possono eliminare, modificare, eseguire operazioni di attivazione e così via.

Se si elimina un gruppo di scalabilità, VMware Cloud Director non elimina alcuna macchina virtuale contenuta nel gruppo di scalabilità.

Creazione di un gruppo di scalabilità

A partire da VMware Cloud Director 10.2.2, il provider di servizi può concedere i diritti per la creazione di gruppi di scalabilità. La quantità di macchine virtuali in un gruppo di scalabilità cambia automaticamente in base alle condizioni definite.

È inoltre possibile accedere ai gruppi di scalabilità da un virtual data center (VDC) dell'organizzazione selezionato.

Procedura

- 1 Nella barra di navigazione superiore, scegliere **Applicazioni** e selezionare la scheda **Gruppi di scalabilità**.
- 2 Fare clic su **Nuovo gruppo di scalabilità**.
- 3 Selezionare il VDC dell'organizzazione in cui creare il gruppo di scalabilità.
- 4 Immettere un nome e, facoltativamente, una descrizione per il nuovo gruppo di scalabilità.

- 5 Selezionare il numero minimo e massimo di macchine virtuali che potranno essere presenti nel gruppo di scalabilità e fare clic su **Avanti**.
- 6 Selezionare un modello di macchina virtuale per le macchine virtuali del gruppo di scalabilità e un criterio di storage, quindi fare clic su **Avanti**.
- 7 Selezionare una rete per il gruppo di scalabilità.
 - Se il VDC è supportato da NSX-T Data Center, selezionare un bilanciamento del carico.
 - Se si desidera gestire il bilanciamento del carico autonomamente o se non è necessario utilizzare un bilanciamento del carico, selezionare **Ho una rete completamente configurata**.
- 8 Fare clic su **Crea gruppo e aggiungi regole**.

Risultati

VMware Cloud Director avvia l'espansione iniziale del gruppo di scalabilità per raggiungere il numero minimo di macchine virtuali.

Operazioni successive

- [Aggiunta di una regola di scalabilità automatica](#)
- Selezionando **Monitora** dalla visualizzazione dettagli di un gruppo di scalabilità è possibile visualizzare tutte le attività correlate al gruppo. È ad esempio possibile vedere la data e l'ora di creazione del gruppo di scalabilità, tutte le attività di aumento o riduzione per il gruppo, le regole che hanno avviato le attività e così via.
- Eliminare un gruppo di scalabilità. Quando si elimina un gruppo di scalabilità, VMware Cloud Director non elimina alcuna macchina virtuale inclusa nel gruppo di scalabilità. Per ridurre il numero di macchine virtuali, è necessario eliminarle manualmente.

Aggiunta di una regola di scalabilità automatica

A partire da VMware Cloud Director 10.2.2, il provider di servizi può concedere i diritti per la creazione e la gestione di gruppi di scalabilità. È possibile aggiungere regole che attivino l'aumento o la riduzione dei gruppi di scalabilità.

Prerequisiti

[Creazione di un gruppo di scalabilità](#)

Procedura

- 1 Nella barra di navigazione superiore, scegliere **Applicazioni** e selezionare la scheda **Gruppi di scalabilità**.
- 2 Selezionare un gruppo di scalabilità e scegliere **Regole**.
- 3 Fare clic su **Aggiungi regola**.
- 4 Immettere un nome per la regola.

- 5 Scegliere se il gruppo di scalabilità deve essere espanso o ridotto quando la regola viene applicata.
- 6 Selezionare il numero di macchine virtuali che verrà aggiunto o eliminato dal gruppo quando la regola viene applicata.
- 7 Specificare un periodo di raffreddamento, espresso in minuti, dopo ogni ridimensionamento automatico del gruppo.

Le condizioni non potranno attivare un altro ridimensionamento finché non sarà trascorso il periodo di raffreddamento. Il periodo di raffreddamento viene reimpostato quando viene applicata una qualsiasi delle regole del gruppo di scalabilità.

- 8 Aggiungere una condizione che attivi la regola.

Il periodo di durata è il tempo per cui la condizione deve essere valida per attivare la regola. Per attivare la regola devono essere soddisfatte tutte le condizioni.

- 9 (Facoltativo) Per aggiungere un'altra condizione, fare clic su **Aggiungi condizione**.
- 10 Fare clic su **Aggiungi**.

Gestione delle vApp

3

Una vApp è composta da una o più macchine virtuali che comunicano su una rete e utilizzano risorse e servizi in un ambiente distribuito. Una vApp può contenere più macchine virtuali.

A partire da VMware Cloud Director 9.5, le vApp supportano la connettività IPv6. È possibile assegnare indirizzi IPv6 a macchine virtuali connesse a reti IPv6.

Importante Tutti i passaggi per la gestione delle vApp sono documentati nella vista a schede, supponendo che si disponga di più virtual data center. Le stesse procedure possono essere completate anche dalla vista griglia, ma i passaggi possono variare leggermente.

Questo capitolo include i seguenti argomenti:



- [Visualizzazione delle vApp](#)
- [Creazione di una nuova vApp](#)
- [Creazione di una vApp da pacchetto OVF](#)
- [Aggiunta di una vApp da catalogo](#)
- [Creazione di una vApp da un modello di vApp](#)
- [Importazione di una macchina virtuale da vCenter Server come vApp](#)
- [Esecuzione di operazioni di attivazione nelle vApp](#)
- [Apertura di una vApp](#)
- [Modifica proprietà vApp](#)
- [Visualizzazione del diagramma di rete di una vApp](#)
- [Gestione delle reti in una vApp](#)
- [Utilizzo di snapshot](#)
- [Modifica del proprietario di una vApp](#)
- [Spostamento di una vApp in un altro virtual data center](#)
- [Copia di una vApp arrestata in un altro virtual data center](#)
- [Copia di una vApp attivata](#)
- [Aggiunta di una macchina virtuale a una vApp](#)


- [Salvataggio di una vApp come modello di vApp in un catalogo](#)
- [Scaricare una vApp da pacchetto OVF](#)
- [Rinnovo del lease di una vApp](#)
- [Eliminazione di una vApp](#)
- [Eliminazione di più vApp](#)


Visualizzazione delle vApp

Le vApp possono essere visualizzate in una vista griglia o a schede.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Per visualizzare le vApp in una vista griglia, fare clic su . Per visualizzarle in una vista a schede, fare clic su .

L'elenco di vApp viene visualizzato in una griglia o come un elenco di schede.
- 3 (Facoltativo) Configurare la vista griglia in modo che contenga i dettagli che si desidera visualizzare.
 - a Nella vista griglia, fare clic sull'icona **Editor della griglia** ().
 - b Selezionare i dettagli della vApp che si desidera includere nella vista griglia selezionando la casella di controllo accanto a ogni dettaglio da visualizzare.
 - c Per salvare le modifiche, fare clic su **OK**.

I dettagli selezionati vengono visualizzati come colonne per ogni vApp.
- 4 (Facoltativo) Nella vista griglia, fare clic su  a sinistra di una vApp per visualizzare le azioni disponibili per la vApp selezionata.

Ad esempio, è possibile spegnere una vApp.

Creazione di una nuova vApp

Anziché creare una vApp basata su un modello di vApp, è possibile creare una vApp utilizzando macchine virtuali dei cataloghi, macchine virtuali nuove o una combinazione di entrambe.

Durante la creazione di una vApp è necessario specificare un nome e, facoltativamente, una descrizione della vApp. È possibile tornare indietro e aggiungere macchine virtuali alla vApp in un secondo momento.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore vApp** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Selezionare **Nuova vApp**.
- 3 Immettere un nome e, facoltativamente, una descrizione per la vApp.
- 4 (Facoltativo) Se si desidera che la vApp venga attivata al momento della distribuzione, selezionare la casella di controllo **Attiva**.

Nota La vApp può essere attivata solo se include macchine virtuali.

- 5 (Facoltativo) Cercare nel catalogo le macchine virtuali da aggiungere a questa vApp oppure aggiungere una nuova macchina virtuale vuota, facendo clic su **Aggiungi macchina virtuale**.

Se non sono presenti macchine virtuali nel catalogo, creare una macchina virtuale e aggiungerla alla vApp.

- a Immettere il nome e il nome del computer per la macchina virtuale.

Importante Il nome del computer può contenere solo caratteri alfanumerici e trattini. Non può essere costituito solo da cifre e non può contenere spazi.

- b (Facoltativo) Immettere una descrizione significativa.

c Selezionare la modalità di distribuzione della macchina virtuale.

Opzione	Azione
Nuova	<p>È possibile distribuire una nuova macchina virtuale con impostazioni personalizzabili.</p> <ol style="list-style-type: none"> 1 Selezionare una famiglia di sistemi operativi e il sistema operativo. 2 (Facoltativo) Selezionare un'immagine di avvio. 3 (Facoltativo) Selezionare un criterio di posizionamento della macchina virtuale e un criterio di dimensionamento della macchina virtuale. <p>I menu a discesa dei criteri di posizionamento della macchina virtuale e di dimensionamento della macchina virtuale sono visibili solo se il provider di servizi ha pubblicato tali criteri nel VDC dell'organizzazione.</p> <ol style="list-style-type: none"> 4 Selezionare la dimensione della macchina virtuale o fare clic su Opzioni di dimensionamento personalizzate per immettere manualmente le impostazioni di calcolo, memoria e storage. <p>Le dimensioni predefinite della macchina virtuale sono piccole, medie o grandi.</p> <ol style="list-style-type: none"> 5 Specificare le opzioni di storage come il criterio di storage e le dimensioni in GB. 6 Specificare le impostazioni di rete per la macchina virtuale, ad esempio rete, modalità IP, indirizzo IP e NIC primario.
Da modello	<p>È possibile distribuire la macchina virtuale da un modello selezionato nel catalogo dei modelli.</p> <ol style="list-style-type: none"> 1 Selezionare il modello della macchina virtuale dal catalogo. 2 (Facoltativo) Selezionare un criterio di posizionamento della macchina virtuale e un criterio di dimensionamento della macchina virtuale. <p>I menu a discesa dei criteri di posizionamento della macchina virtuale e di dimensionamento della macchina virtuale sono visibili solo se il provider di servizi ha pubblicato tali criteri nel VDC dell'organizzazione. Se il modello selezionato dispone di criteri assegnati, potrebbe essere limitato ai criteri del modello predefiniti.</p> <ol style="list-style-type: none"> 3 (Facoltativo) Scegliere di utilizzare un criterio di storage personalizzato e selezionare il criterio in Criterio di storage personalizzato da utilizzare. 4 Se è disponibile un accordo di licenza con l'utente finale, è necessario leggerlo e accettarlo.

d Per aggiungere la macchina virtuale alla vApp, fare clic su **OK**.

Nel catalogo è ora presente la macchina virtuale aggiuntiva.

- 6 (Facoltativo) Ripetere il [Passaggio 5](#) per ogni macchina virtuale aggiuntiva che si desidera creare nella vApp.
- 7 Per completare la creazione della vApp, fare clic su **Crea**.

Risultati

La vApp viene creata. Quando si attiva la vApp, vengono create e attivate anche le macchine virtuali che contiene.

Creazione di una vApp da pacchetto OVF

È possibile creare e distribuire una vApp direttamente da un pacchetto OVF senza creare un modello di vApp e una voce di catalogo corrispondente.

VMware Cloud Director dispone di restrizioni proprie per le distribuzioni di OVF diverse dalle restrizioni in vCenter Server. Di conseguenza, una distribuzione di OVF riuscita in vCenter Server potrebbe non riuscire in VMware Cloud Director.

VMware Cloud Director supporta OVF 1.1, ma non supporta tutte le sezioni dello schema OVF 1.1. Ad esempio, la sezione `DeploymentOptions` nel file OVF non è supportata.

Una distribuzione di OVF in VMware Cloud Director coinvolge molti componenti, ad esempio `TransferService`, area di spool sul montaggio di NFS, connessione di NFC a vCenter Server, convalida del checksum e così via. Se uno di questi componenti non riesce, il caricamento del file OVF non riesce.

Se si carica un pacchetto OVF con un file manifesto, VMware Cloud Director convalida l'hash SHA-1 del file del descrittore OVF e tutti i file VMDK nei valori del file `manifest.mf`. Se un hash non corrisponde, il caricamento non riesce. Un **amministratore di sistema** può disattivare questo controllo impostando la proprietà `CONFIG` su `ovf.manifest.check.disabled`.

Prerequisiti

- Verificare di disporre di un pacchetto OVF da caricare e delle autorizzazioni per caricare pacchetti OVF e distribuire vApp.
- Verificare che la versione di OVF nel file del descrittore OVF non sia 0.9.
- La dimensione massima supportata per impostazione predefinita di un file descrittore OVF in VMware Cloud Director è 12 MB. È possibile sovrascriverla modificando la `ovf.descriptor.size.max` della proprietà `CONFIG`.
- Verificare che la dimensioni massima consentita predefinita del file manifesto (estensione.mf) sia 1 MB.
- Verificare che il pacchetto OVF sia conforme allo schema OVF XSD.
- Se viene fornita una versione hardware nell'elemento `VirtualSystemType` del file descrittore OVF, verificare che sia precedente alla versione hardware più recente supportata nel VDC in cui si carica il file OVF.
- Se il file del descrittore OVF contiene elementi `ExtraConfig`, verificare che l'**amministratore del sistema** li includa in `AllowedList` degli elementi `extraConfigs`. Gli elementi non inclusi in `AllowedList` causano la mancata riuscita del caricamento del file OVF con un errore di convalida.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su **Aggiungi vApp da OVF**.
- 3 Fare clic sul pulsante **Carica**, individuare una posizione accessibile dal computer e selezionare il file del modello OVF/OVA.

Il percorso può essere il disco rigido locale, una condivisione di rete o un'unità CD/DVD.

Le estensioni di file supportate includono `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` e `.strings`. Se si sceglie di caricare un file OVF, che fa riferimento a più file rispetto a quelli che si sta tentando di caricare, ad esempio un file VMDK, è necessario cercare e selezionare tutti i file.

- 4 Fare clic su **Avanti**.
- 5 Verificare i dettagli del modello OVF/OVA da distribuire e fare clic su **Avanti**.
- 6 Digitare un nome e, facoltativamente, una descrizione per la vApp, quindi fare clic su **Avanti**.
- 7 (Facoltativo) Modificare il nome del computer della vApp in modo che contenga solo caratteri alfanumerici.

Questo passaggio è necessario solo se il nome della vApp contiene spazi o caratteri speciali. Per impostazione predefinita, nel campo del nome del computer viene inserito il nome della macchina virtuale. Tuttavia, i nomi dei computer possono contenere solo caratteri alfanumerici.

- 8 Dal menu a discesa **Criterio di storage**, selezionare un criterio di storage per ogni macchina virtuale nella vApp e fare clic su **Avanti**.
- 9 Selezionare le reti a cui connettere ogni macchina virtuale.
 - Selezionare una rete per ogni macchina virtuale dal menu a discesa **Rete**.
 - È possibile selezionare la casella di controllo **Passare al flusso di lavoro di rete avanzato** e immettere manualmente le impostazioni di rete come la NIC primaria, il tipo di scheda di rete, la rete, l'assegnazione IP e le impostazioni dell'indirizzo IP per ogni macchina virtuale nella vApp.

È possibile configurare proprietà aggiuntive per le macchine virtuali dopo aver eseguito la procedura guidata.

- 10 Fare clic su **Avanti**.

11 Personalizzare l'hardware delle macchine virtuali nella vApp e fare clic su **Avanti.**

Opzione	Descrizione
Numero di CPU virtuali	Immettere il numero di CPU virtuali per ogni macchina virtuale nella vApp. Il numero massimo di CPU virtuali che è possibile assegnare a una macchina virtuale dipende dal numero di CPU logiche nell'host e dal tipo di sistema operativo guest installato nella macchina virtuale.
Core per socket	Immettere il numero di core per socket per ogni macchina virtuale nella vApp. È possibile configurare la modalità di assegnazione delle CPU virtuali in termini di core e core per socket. Stabilire il numero di core della CPU desiderati nella macchina virtuale, quindi selezionare il numero di core per ciascun socket, a seconda che si desideri una CPU single-core, dual-core, tri-core e così via.
Numero di core	Visualizza il numero di core per ogni macchina virtuale nella vApp. Il numero cambia quando si aggiorna il numero di CPU virtuali.
Memoria totale (MB)	Inserire la memoria in MB per ogni macchina virtuale nella vApp. Questa impostazione determina la quantità di memoria dell'host ESXi allocata per la macchina virtuale. Le dimensioni della memoria dell'hardware virtuale determinano la quantità di memoria disponibile per le applicazioni eseguite nella macchina virtuale. Una macchina virtuale non può utilizzare ulteriori risorse di memoria rispetto alle dimensioni della memoria dell'hardware virtuale configurato.

12 Nella pagina Pronto per il completamento, controllare le impostazioni e fare clic su **Fine.****Risultati**

La nuova vApp viene visualizzata nella vista scheda.

Aggiunta di una vApp da catalogo

Se si dispone dell'accesso a un catalogo, è possibile utilizzare i modelli di vApp nel catalogo per creare vApp.

Un modello di vApp può essere basato su un file OVF con proprietà per la personalizzazione delle macchine virtuali della vApp. La vApp eredita queste proprietà. Se una qualsiasi di queste proprietà può essere configurata dall'utente, è possibile specificarne i valori.

Prerequisiti

- Per accedere ai modelli di vApp nei cataloghi pubblici, verificare di essere un **amministratore dell'organizzazione** o un **autore di vApp**.
- Per accedere ai modelli di vApp nei cataloghi dell'organizzazione che risultano essere condivisioni, verificare di essere almeno un **utente di vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su **Nuovo** e selezionare **Aggiungi vApp dal catalogo**.
- 3 Selezionare un modello da importare e fare clic su **Avanti**.
- 4 Immettere un nome e, facoltativamente, una descrizione per la vApp.
- 5 Immettere un lease di runtime e un lease di storage per la vApp, quindi fare clic su **Avanti**.
- 6 Dal menu a discesa **Criterio di storage**, selezionare un criterio di storage per ogni macchina virtuale nella vApp e fare clic su **Avanti**.
- 7 Se i criteri di posizionamento e i criteri di dimensionamento per le macchine virtuali nella vApp sono configurabili, selezionare un criterio per ogni macchina virtuale nel menu a discesa.
- 8 Se le proprietà di calcolo per le macchine virtuali nella vApp sono configurabili, personalizzarle e fare clic su **Avanti**.

Opzione	Descrizione
CPU virtuali	Immettere il numero di CPU virtuali per ogni macchina virtuale nella vApp. Il numero massimo di CPU virtuali che è possibile assegnare a una macchina virtuale dipende dal numero di CPU logiche nell'host e dal tipo di sistema operativo guest installato nella macchina virtuale.
Core per socket	Immettere il numero di core per socket per ogni macchina virtuale nella vApp. È possibile configurare la modalità di assegnazione delle CPU virtuali in termini di core e core per socket. Stabilire il numero di core della CPU desiderati nella macchina virtuale, quindi selezionare il numero di core per ciascun socket, a seconda che si desideri una CPU single-core, dual-core, tri-core e così via.
Numero di core	Visualizza il numero di core per ogni macchina virtuale nella vApp. Il numero cambia quando si aggiorna il numero di CPU virtuali.
Memoria	Inserire la memoria in MB per ogni macchina virtuale nella vApp. Questa impostazione determina la quantità di memoria dell'host ESXi allocata per la macchina virtuale. Le dimensioni della memoria dell'hardware virtuale determinano la quantità di memoria disponibile per le applicazioni eseguite nella macchina virtuale. Una macchina virtuale non può utilizzare ulteriori risorse di memoria rispetto alle dimensioni della memoria dell'hardware virtuale configurato.

- 9 Se le proprietà dell'hardware delle macchine virtuali nella vApp sono configurabili, personalizzare le dimensioni dei dischi rigidi delle macchine virtuali e fare clic su **Avanti**.

- 10 Se le proprietà di rete delle macchine virtuali nella vApp sono configurabili, personalizzarle e fare clic su **Avanti**.
 - a Nella pagina **Configura rete**, selezionare le reti a cui si desidera connettere ciascuna macchina virtuale.
 - b (Facoltativo) Selezionare la casella di controllo per passare al flusso di lavoro di rete avanzato e configurare le impostazioni di rete aggiuntive per le macchine virtuali nella vApp.
- 11 Controllare le impostazioni della vApp e fare clic su **Fine**.

Creazione di una vApp da un modello di vApp

È possibile creare una nuova vApp basata su un modello di vApp memorizzato in un catalogo a cui è possibile accedere.

Se il modello di vApp è basato su un file OVF che include proprietà OVF per la personalizzazione delle macchine virtuali, tali proprietà vengono passate alla vApp. Se una qualsiasi di queste proprietà è configurabile dall'utente, è possibile specificare i valori.

Prerequisiti

- Solo gli amministratori di un'organizzazione e gli autori di vApp possono accedere a modelli di vApp in cataloghi pubblici.
- Gli utenti delle vApp possono accedere ai modelli di vApp in cataloghi dell'organizzazione condivisi.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di vApp**.
L'elenco dei modelli viene visualizzato in una vista griglia.
- 2 Fare clic sul pulsante di opzione accanto al modello di vApp da utilizzare e fare clic su **Crea vApp**.
- 3 Immettere un nome e, facoltativamente, una descrizione della vApp.
- 4 Specificare il periodo di tempo, espresso in ore o giorni, per cui è possibile eseguire questa vApp prima che venga arrestata automaticamente.
- 5 Specificare per quante ore o giorni la vApp arrestata dovrà continuare a rimanere disponibile prima di essere cancellata automaticamente.
- 6 Fare clic su **Avanti**.
- 7 Selezionare il virtual data center in cui si desidera creare la vApp.
- 8 Selezionare un criterio di storage.
- 9 Fare clic su **Avanti**.

- 10 In VMware Cloud Director 10.2.2 e versioni successive, configurare i criteri di posizionamento e dimensionamento della macchina virtuale.

A partire dalla versione 10.2.2, i criteri di posizionamento sono globali ed è possibile pubblicarli in più VDC del provider e modelli di vApp includendo informazioni dei criteri sia di dimensionamento che di posizionamento.

- 11 Selezionare le reti a cui connettere ogni macchina virtuale.

- Selezionare una rete per ogni macchina virtuale dal menu a discesa **Rete**.
- È possibile selezionare la casella di controllo **Passare al flusso di lavoro di rete avanzato** e immettere manualmente le impostazioni di rete come la NIC primaria, il tipo di scheda di rete, la rete, l'assegnazione IP e le impostazioni dell'indirizzo IP per ogni macchina virtuale nella vApp.

È possibile configurare proprietà aggiuntive per le macchine virtuali dopo aver eseguito la procedura guidata.

- 12 Fare clic su **Avanti**.

- 13 Personalizzare l'hardware delle macchine virtuali nella vApp e fare clic su **Avanti**.

Opzione	Descrizione
Numero di CPU virtuali	Immettere il numero di CPU virtuali per ogni macchina virtuale nella vApp. Il numero massimo di CPU virtuali che è possibile assegnare a una macchina virtuale dipende dal numero di CPU logiche nell'host e dal tipo di sistema operativo guest installato nella macchina virtuale.
Core per socket	Immettere il numero di core per socket per ogni macchina virtuale nella vApp. È possibile configurare la modalità di assegnazione delle CPU virtuali in termini di core e core per socket. Stabilire il numero di core della CPU desiderati nella macchina virtuale, quindi selezionare il numero di core per ciascun socket, a seconda che si desideri una CPU single-core, dual-core, tri-core e così via.
Numero di core	Visualizza il numero di core per ogni macchina virtuale nella vApp. Il numero cambia quando si aggiorna il numero di CPU virtuali.
Memoria totale (MB)	Inserire la memoria in MB per ogni macchina virtuale nella vApp. Questa impostazione determina la quantità di memoria dell'host ESXi allocata per la macchina virtuale. Le dimensioni della memoria dell'hardware virtuale determinano la quantità di memoria disponibile per le applicazioni eseguite nella macchina virtuale. Una macchina virtuale non può utilizzare ulteriori risorse di memoria rispetto alle dimensioni della memoria dell'hardware virtuale configurato.
Proprietà disco rigido	Immettere le dimensioni del disco rigido della macchina virtuale in MB.

- 14 Nella pagina Pronto per il completamento, controllare le impostazioni e fare clic su **Fine**.

Risultati

La nuova vApp viene visualizzata nella vista scheda.

Importazione di una macchina virtuale da vCenter Server come vApp

Se si dispone di diritti di **amministratore di sistema**, è possibile importare le macchine virtuali di vCenter Server come vApp in VMware Cloud Director.

Quando si importa una macchina virtuale, si perdono le impostazioni di prenotazione, limite e condivisione configurate in vCenter Server. Le macchine virtuali importate ottengono le proprie impostazioni di allocazione risorse dal virtual data center dell'organizzazione in cui si trovano.

Prerequisiti

Per visualizzare e importare macchine virtuali da vCenter Server, verificare di disporre di diritti di **amministratore di sistema**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su **Nuovo** e selezionare **Importa da vCenter**.
- 3 Dal menu a discesa, selezionare un'istanza di vCenter Server da cui importare una macchina virtuale.
- 4 Selezionare una macchina virtuale da importare.
- 5 Immettere un nome e, facoltativamente, una descrizione per la vApp.
- 6 Dal menu a discesa, selezionare un virtual data center in cui archiviare ed eseguire la vApp.
- 7 (Facoltativo) Dal menu a discesa, selezionare un criterio di storage per la vApp.
- 8 (Facoltativo) Per eliminare la macchina virtuale di origine, attivare l'opzione **Sposta macchina virtuale**.
- 9 Fare clic su **Importa**.

Esecuzione di operazioni di attivazione nelle vApp

È possibile eseguire operazioni di attivazione nelle vApp, ad esempio l'attivazione, la disattivazione, la sospensione o la reimpostazione di una vApp.


Attivazione di una vApp

L'avvio di una vApp comporta l'attivazione di tutte le macchine virtuali nella vApp che non sono ancora attivate.

Prerequisiti

Si supponga di essere almeno un autore di vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp che si desidera attivare, selezionare **Attiva**.

Risultati

La vApp viene attivata.


Disattivazione di una vApp

La disattivazione di una vApp comporta la disattivazione di tutte le macchine virtuali nella vApp. Per eseguire determinate azioni, come l'aggiunta di una vApp a un catalogo oppure la copia o lo spostamento di una vApp in un altro VDC, è innanzitutto necessario disattivare la vApp.

Prerequisiti

È necessario che la vApp sia avviata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp che si desidera arrestare, selezionare **Disattiva**.
- 4 Fare clic su **OK**.

Risultati

Tutte le macchine virtuali nella vApp e la vApp stessa vengono disattivate.


Reimpostazione di una vApp

La reimpostazione di una vApp cancella lo stato (memoria, cache e così via) della vApp, ma quest'ultima continua a funzionare.

Prerequisiti

La vApp è avviata e le macchine virtuali al suo interno sono attivate.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.

- 3 Dal menu **Azioni** della vApp da reimpostare, selezionare **Reimposta**.

Risultati

Lo stato viene cancellato e la vApp continua a funzionare.


Sospensione di una vApp

La sospensione di una vApp ne preserva lo stato corrente scrivendo la memoria sul disco.

Prerequisiti

La vApp è in esecuzione.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp da sospendere, selezionare **Sospendi**.

Risultati

La vApp viene sospesa e il relativo stato viene mantenuto.


Annullamento dello stato sospeso di una vApp

Se una vApp è nello stato di sospensione e non è più necessario riprendere a utilizzarla, è possibile ignorare tale stato. Se si ignora lo stato di sospensione, la memoria salvata viene rimossa e la vApp viene disattivata.

Prerequisiti

La vApp deve essere nello stato di sospensione.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp sospesa, selezionare **Ignora stato sospeso**.

Risultati

Lo stato viene ignorato e la vApp viene disattivata.

Attivazione di più vApp

È possibile attivare più vApp contemporaneamente. Questa azione comporta l'attivazione di tutte le macchine virtuali nella vApp che non sono ancora attivate.

Prerequisiti

Verificare di essere almeno un **autore di vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp che si desidera attivare.
- 4 Dal menu **Azioni**, selezionare **Attiva**.
- 5 Fare clic su **OK** per confermare.

Disattivazione di più vApp

È possibile disattivare più vApp contemporaneamente. Questa azione comporta la disattivazione di tutte le macchine virtuali nelle vApp. Per eseguire determinate azioni, come l'aggiunta di una vApp a un catalogo oppure la copia o lo spostamento di una vApp in un altro virtual data center, è innanzitutto necessario disattivare la vApp.

Prerequisiti

- Verificare che le vApp siano state avviate.
- Verificare di essere almeno un **autore di vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp che si desidera disattivare.
- 4 Dal menu **Azioni**, selezionare **Disattiva**.
- 5 Fare clic su **OK** per confermare.

Rimozione dello stato sospeso di più vApp

Se più vApp hanno stato sospeso e non è più necessario riprenderne l'uso, è possibile rimuovere lo stato sospeso delle vApp contemporaneamente. Se si rimuove lo stato sospeso, la memoria salvata viene rimossa e le vApp vengono disattivate.

Prerequisiti

- Verificare che le vApp siano in stato di sospensione.
- Verificare di essere almeno un **autore di vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp sospese che si desidera disattivare.
- 4 Dal menu **Azioni**, scegliere **Ignora stato sospeso**.

Risultati

Le vApp vengono disattivate.

Reimpostazione di più vApp

La reimpostazione di più vApp contemporaneamente ne cancella lo stato, che include memoria, cache e così via, ma le vApp continuano a funzionare.

Prerequisiti

- Verificare che le vApp siano state avviate e che le macchine virtuali nelle vApp siano attivate.
- Verificare di essere almeno un **autore di vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp che si desidera reimpostare.
- 4 Dal menu **Azioni**, selezionare **Reimposta** e fare clic su **OK** per confermare.

Risultati

Lo stato di ogni vApp viene cancellato e le vApp continuano a funzionare.

Sospensione di più vApp

La sospensione di più vApp contemporaneamente ne preserva lo stato corrente scrivendo la memoria sul disco.

Prerequisiti

Verificare che le vApp siano in esecuzione.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp che si desidera sospendere.
- 4 Dal menu **Azioni** della vApp da sospendere, selezionare **Sospendi** e fare clic su **OK** per confermare.


Risultati

Le vApp vengono sospese e il loro stato viene mantenuto.

Apertura di una vApp

È possibile aprire una vApp per visualizzare le macchine virtuali e le reti che contiene. È inoltre possibile visualizzare un diagramma che mostra come sono connesse le macchine virtuali e le reti.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
Dalla vista a schede, è possibile visualizzare le informazioni generali di ogni vApp, ad esempio il nome, lo stato di alimentazione, le informazioni sul lease, la data di creazione, il proprietario, il numero di macchine virtuali associate alla vApp, il numero totale di CPU, lo storage e la memoria totali e le reti associate.
- 3 Per visualizzare le impostazioni dettagliate di una vApp selezionata, fare clic su **Dettagli** nella scheda della vApp.

Modifica proprietà vApp

È possibile modificare le proprietà di una vApp esistente, inclusi il nome e la descrizione, le impostazioni del lease, l'ordine di avvio delle macchine virtuali nella vApp, le impostazioni di condivisione e le impostazioni di rete.


Modifica delle proprietà generali della vApp

È possibile rivedere e modificare il nome, la descrizione e altre proprietà generali di una vApp.

Prerequisiti

Verificare che la vApp sia disattivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli** per visualizzare e modificare le proprietà della vApp.
- 4 Rivedere e modificare le proprietà desiderate e fare clic su **Salva**.

Opzione	Azione
Nome	Immettere un nuovo nome per la vApp.
Descrizione	Digitare una descrizione facoltativa della vApp.
Virtual data center	Nome del data center a cui appartiene la vApp.
Snapshot	Se è presente uno snapshot, vengono visualizzati i relativi dettagli.
Lease	Selezionare Rinnova per rinnovare il lease. <ol style="list-style-type: none"> a Consente di pianificare il lease di runtime in numero di ore o giorni. Definisce per quanto tempo è possibile eseguire la vApp prima che venga arrestata automaticamente. b Consente di pianificare il lease dello storage in numero di ore o giorni. Definisce per quanto tempo la vApp rimarrà disponibile prima di essere eliminata automaticamente.

Risultati

Le impostazioni generali vengono salvate.

Modifica dell'ordine di avvio e arresto delle macchine virtuali in una vApp


È possibile configurare l'ordine di avvio e arresto delle macchine virtuali all'interno della vApp. Configurare l'ordine di avvio e arresto se nelle macchine virtuali sono installate applicazioni che devono essere avviate e arrestate in un determinato ordine.

Queste impostazioni sono utili se è necessario avviare e arrestare le macchine virtuali in un ordine specifico. Ad esempio, una macchina virtuale che ospita un server di database, un'altra che ospita un server applicazioni e un'ultima che ospita un server Web. Per assicurare il corretto funzionamento delle funzioni correlate, il server di database deve essere avviato per primo, seguito dal server applicazioni e, infine, dal server Web.

Prerequisiti

Verificare che la vApp sia disattivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Fare clic sulla scheda **Ordine di avvio e arresto** e fare clic su **Modifica**.
- 5 Modificare le proprietà dell'ordine di avvio e arresto per ogni macchina virtuale e fare clic su **OK**.

Opzione	Azione
Ordine di avvio	Immettere l'ordine in cui si desidera che la macchina virtuale venga avviata. È necessario inserire un valore per ogni macchina presente nella sequenza.
Azione di avvio	Selezionare un'azione di avvio. L'azione di avvio determina quello che accade a una macchina virtuale all'avvio della vApp che la contiene. Per impostazione predefinita, questa opzione è impostata su Attiva .
Attesa avvio	Immettere il tempo di attesa dell'avvio. Il tempo di attesa dell'avvio è la quantità di tempo (in secondi) che dovrà trascorrere prima che VMware Cloud Director avvi la macchina successiva nella sequenza.
Azione di arresto	Selezionare l'azione di arresto. L'azione di arresto è l'azione che la macchina virtuale esegue quando si arresta la vApp che la contiene. Se si sceglie Disattiva , la macchina virtuale viene disattivata senza eseguire azioni di spegnimento che ne assicurino la stabilità (l'azione equivale a staccare la spina dalla presa elettrica). Selezionare questa azione se VMware Tools non è installato. In caso contrario, scegliere Spegni , che assicura la stabilità della macchina al momento dello spegnimento.
Attesa arresto	Immettere il tempo di attesa dell'arresto. Il tempo di attesa dell'arresto è la quantità di tempo (in secondi) che dovrà trascorrere prima che VMware Cloud Director spenga la macchina virtuale successiva nella sequenza.

Modifica delle proprietà guest di una vApp


Se una vApp include proprietà OVF configurabili dall'utente, è possibile controllare e modificare tali proprietà.

Se una macchina virtuale nella vApp include un valore per una proprietà configurabile dall'utente con lo stesso nome, il valore della macchina virtuale ha la precedenza.

Prerequisiti

Verificare che la vApp venga arrestata e che le proprietà guest possano essere configurate dall'utente.


Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e scegliere **Macchine virtuali** nel pannello sinistro.
- 2 Fare clic su  per visualizzare l'elenco in una vista a schede e, facoltativamente, ordinare l'elenco delle macchine virtuali dal menu a discesa **Ordinamento**.
- 3 Nella scheda della macchina virtuale che si desidera modificare, fare clic su **Dettagli**.
- 4 Fare clic su **Proprietà guest**, quindi su **Modifica**.
- 5 Modificare le proprietà guest della vApp e fare clic su **OK**.

Condivisione di una vApp

È possibile condividere le vApp con altri gruppi o utenti dell'organizzazione. I controlli di accesso impostati determinano le operazioni che è possibile eseguire nelle vApp condivise.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli** e scorrere verso il basso fino alle proprietà di condivisione della vApp.

4 Selezionare gli utenti con cui si intende condividere la vApp e fare clic su **Salva**.

Opzione	Azione
Condividi con chiunque nell'organizzazione	<p>Selezionare questa opzione per eseguire la condivisione con tutti gli utenti dell'organizzazione e selezionare il livello di accesso.</p> <ul style="list-style-type: none"> ■ Selezionare Controllo completo per concedere il controllo completo. <p>Tutti gli utenti dell'organizzazione possono aprire, avviare, salvare una vApp come modello di vApp, aggiungere il modello a un catalogo, cambiare il proprietario della vApp, copiare in un catalogo e modificare le proprietà.</p> <ul style="list-style-type: none"> ■ Per concedere l'accesso in sola lettura, selezionare Sola lettura.
Condividi con utenti o gruppi specifici	<p>Selezionare questa opzione per condividere la vApp solo con gli utenti specifici.</p> <ol style="list-style-type: none"> Selezionare i nomi nel pannello Utenti e gruppi senza accesso per spostarli nel pannello Utenti e gruppi con accesso. Selezionare un livello di accesso per gli utenti e i gruppi specifici. <ul style="list-style-type: none"> ■ Selezionare Controllo completo per concedere il controllo completo. <p>Gli utenti che dispongono del controllo completo possono aprire, avviare, salvare una vApp come modello di vApp, aggiungere il modello a un catalogo, cambiare il proprietario della vApp, copiare in un catalogo e modificare le proprietà.</p> <ul style="list-style-type: none"> ■ Per concedere l'accesso in sola lettura, selezionare Sola lettura.

Risultati

La vApp viene condivisa con gli utenti o i gruppi specifici.


Visualizzazione del diagramma di rete di una vApp

Un diagramma di rete di vApp offre una visualizzazione grafica delle macchine virtuali e delle reti in una vApp.

Prerequisiti

Per visualizzare il diagramma di rete di vApp, la vApp deve contenere meno di 40 macchine virtuali. Se la vApp contiene più di 40 macchine virtuali, il diagramma non è disponibile.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.

4 Fare clic sulla scheda **Diagramma di rete**.

Viene visualizzato il diagramma che mostra le connessioni tra le macchine virtuali e le reti nella vApp. Un asterisco rappresenta una scheda NIC primaria. Una NIC è di colore verde se è connessa e di colore bianco se non è connessa.

5 (Facoltativo) Per evidenziare le reti e le macchine virtuali connesse, fare clic su una rete o su una macchina virtuale.

Gli oggetti connessi e le connessioni tra di essi vengono evidenziati.

Operazioni successive

È possibile aggiungere macchine virtuali o reti da questa pagina.

Gestione delle reti in una vApp

Le macchine virtuali in una vApp possono connettersi a reti di vApp (isolate o instradate) e reti di virtual data center dell'organizzazione (dirette o con priorità applicata). È possibile aggiungere reti di diversi tipi a una vApp per gestire più scenari di rete.

Le macchine virtuali nella vApp possono connettersi alle reti disponibili in una vApp. Se si desidera connettere una macchina virtuale a una rete diversa, è necessario innanzitutto aggiungerla alla vApp.

Una vApp può includere reti di vApp e reti di virtual data center dell'organizzazione. Una rete di vApp può essere isolata o instradata. Una rete di vApp isolata è contenuta all'interno della vApp. È inoltre possibile instradare una rete di vApp verso una rete di virtual data center dell'organizzazione per fornire la connettività alle macchine virtuali esterne alla vApp. Per le reti di vApp instradate, è possibile configurare servizi di rete, ad esempio un firewall e il routing statico.

Nota I VDC dell'organizzazione supportati da NSX Data Center for vSphere sono compatibili con le reti di vApp instradate isolate e dirette.

I VDC dell'organizzazione supportati da NSX-T Data Center sono compatibili con le reti di vApp isolate e dirette.

È possibile connettere una vApp direttamente a una rete di virtual data center dell'organizzazione. Se si dispone di più vApp che contengono macchine virtuali identiche connesse alla stessa rete di virtual data center dell'organizzazione e si desidera avviare le vApp contemporaneamente, è possibile applicare la priorità alla vApp. In questo modo le macchine virtuali potranno essere attivate senza conflitti, isolando i relativi indirizzi MAC e IP.



Le reti aggiunte alla vApp utilizzano il pool di reti associato al virtual data center dell'organizzazione in cui è stata creata la vApp.

Visualizzazione di reti di vApp

È possibile accedere e visualizzare le reti in una vApp.

Prerequisiti

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Fare clic sulla scheda **Reti**.
Viene visualizzato l'elenco delle reti, se presenti. È possibile visualizzare informazioni su ciascuna rete, come nome, gateway, netmask, connessione e conservazione delle risorse IP e NAT.
- 5 (Facoltativo) Per modificare le colonne visualizzate, fare clic sull'icona **Editor della griglia** () e selezionare o deselezionare le caselle di controllo delle colonne da visualizzare o nascondere, rispettivamente.

Applicazione della priorità in una rete di vApp


L'attivazione di macchine virtuali identiche incluse in vApp diverse potrebbe causare un conflitto. Per consentire l'attivazione di macchine virtuali identiche in vApp diverse senza conflitti, è necessario applicare la priorità nelle vApp.

L'applicazione della priorità in una vApp isola gli indirizzi MAC e IP delle macchine virtuali e cambia il tipo di connessione delle reti VDC dell'organizzazione da Diretta a Con priorità applicata. Nelle reti con priorità applicata il firewall viene abilitato automaticamente e configurato in modo che sia consentito solo il traffico in uscita. Quando si applica la priorità in una vApp, è anche possibile configurare regole NAT e firewall nelle reti con priorità applicata.

Prerequisiti

- È possibile applicare la priorità solo a reti di vApp dirette. Se la vApp utilizza più di una rete e le altre reti sono, ad esempio, instradate, l'applicazione della priorità viene eseguita solo per la rete diretta.
- Le macchine virtuali nella vApp che utilizzano la rete diretta devono essere arrestate, in modo che la rete di vApp diretta non risulti attualmente in uso.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.

- 4 Fare clic sulla scheda **Reti**.
- 5 Se nella vApp non è applicata la priorità, fare clic sul pulsante **Modifica**.
- 6 Attivare l'opzione **Applica priorità a vApp** e fare clic su **OK**.

Risultati

Gli indirizzi IP e MAC delle macchine virtuali diventano isolati. È possibile attivare macchine virtuali identiche in vApp diverse senza generare conflitti.

Aggiunta di una rete a una vApp

È possibile aggiungere una rete a una vApp per rendere la rete disponibile per le macchine virtuali nella vApp. In una vApp è possibile aggiungere una rete vApp o una rete di virtual data center dell'organizzazione.


Le connessioni possono essere dirette o con priorità applicata. L'applicazione di priorità consente di attivare macchine virtuali identiche in vApp diverse senza causare conflitti attraverso l'isolamento degli indirizzi MAC e IP delle macchine virtuali.

Quando l'applicazione delle priorità è abilitata e la vApp è attiva, viene creata una rete isolata dal pool di reti di virtual data center dell'organizzazione. Un gateway edge viene creato e collegato sia alla rete isolata sia alla rete di virtual data center dell'organizzazione. Il traffico da e verso le macchine virtuali passa attraverso il gateway edge che converte gli indirizzi IP utilizzando NAT e proxy-AR. Questo consente a un router di smistare il traffico tra due reti utilizzando lo stesso spazio IP.

Prerequisiti

Per aggiungere una rete di virtual data center dell'organizzazione, l'amministratore deve averla creata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Azioni** e selezionare **Aggiungi rete**.

4 Selezionare il tipo di rete da aggiungere.

Opzione	Azione
Rete VDC dell'organizzazione	Selezionare una rete di virtual data center dell'organizzazione nell'elenco delle reti disponibili.
Reti di vApp	<ul style="list-style-type: none"> a Immettere un nome e, facoltativamente, una descrizione per la rete. b Immettere il CIDR del gateway di rete. c (Facoltativo) Immettere i DNS primario e secondario e il suffisso DNS. d (Facoltativo) Scegliere se consentire la VLAN guest. e (Facoltativo) Immettere le impostazioni del pool di IP statici, ad esempio gli intervalli IP. f (Facoltativo) Per abilitare la connessione a una rete di virtual data center dell'organizzazione, attivare l'opzione Connetti a una rete VDC dell'organizzazione e selezionare una rete nell'elenco.

5 Fare clic su **Aggiungi**.

Risultati

La rete viene aggiunta alla vApp.

Operazioni successive

Connettere una macchina virtuale della vApp alla rete.

Configurazione dei servizi di rete per una rete di vApp

È possibile configurare servizi di rete, ad esempio DHCP, firewall, NAT (Network Address Translation) e routing statico per determinate reti di vApp.

I servizi di rete disponibili dipendono dal tipo di rete di vApp.

Tabella 3-1. Servizi di rete disponibili per ogni tipo di rete

Tipo di rete di vApp	DHCP	Firewall	NAT	Routing statico
Diretta				
Instradata	X	X	X	X
Isolata	X			


Nota I VDC dell'organizzazione supportati da NSX Data Center for vSphere sono compatibili con le reti di vApp instradate isolate e dirette.

I VDC dell'organizzazione supportati da NSX-T Data Center sono compatibili con le reti di vApp isolate e dirette.

Visualizzazione e modifica dei dettagli di rete generali

È possibile visualizzare e modificare i dettagli di rete di vApp generali, ad esempio il nome della rete e la descrizione.


Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Nella scheda **Generale**, esaminare le informazioni sulla rete.
- 6 Fare clic su **Modifica**.
- 7 Modificare il nome e la descrizione della rete di vApp.
- 8 Fare clic su **Salva**.

Modifica delle impostazioni del pool di IP statici di una rete di vApp

È possibile configurare una rete di vApp per fornire indirizzi IP statici alle macchine virtuali nella vApp estraendoli da un pool statico di indirizzi IP.


Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Nella scheda **Gestione IP** fare clic su **Pool statici**.
- 6 Fare clic su **Modifica**.
- 7 Immettere un intervallo IP e fare clic su **Aggiungi**.
- 8 Fare clic su **Salva**.

Modifica delle impostazioni DNS di una rete di vApp

Dopo aver creato una rete di vApp e, è possibile visualizzare e modificare le impostazioni DNS in qualsiasi momento.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.

- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Nella scheda **Gestione IP** fare clic su **DNS**.
Vengono visualizzate le impostazioni DNS.
- 6 Fare clic su **Modifica**.
- 7 Modificare il DNS primario e secondario e il suffisso DNS.
- 8 Fare clic su **Salva**.

Configurazione di DHCP per una rete di vApp


È possibile configurare determinate reti di vApp in modo che forniscano servizi DHCP alle macchine virtuali incluse nella vApp.

Quando per una rete di vApp viene abilitato il DHCP, a tale rete viene connessa una scheda NIC sulla macchina virtuale della vApp, e il DHCP viene selezionato come modalità IP per tale scheda NIC. Quando la macchina virtuale viene attivata, VMware Cloud Director le assegna un indirizzo IP DHCP.

Prerequisiti

- Verificare che la rete di vApp sia instradata o isolata.
- Verificare che la vApp si trovi in un virtual data center dell'organizzazione supportato da NSX Data Center for vSphere.

Procedura


- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Nella scheda **Gestione IP**, fare clic su **DHCP**.
Viene visualizzato lo stato DHCP.
- 6 Fare clic su **Modifica**.
- 7 Fare clic su **Abilitato**.
- 8 Nella casella di testo **Pool di IP**, immettere un intervallo di indirizzi IP.
VMware Cloud Director utilizza questi indirizzi per soddisfare le richieste DHCP. L'intervallo di indirizzi IP DHCP non può sovrapporsi con il pool di IP statici della rete di vApp.
- 9 Impostare il tempo di lease predefinito e massimo in secondi.

10 Fare clic su **Salva**.

Visualizzazione delle allocazioni di IP per la rete di vApp

È possibile esaminare le allocazioni di IP per le reti nella vApp di appartenenza.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Nella scheda **Gestione IP** fare clic su **Allocazioni IP**.

Vengono visualizzati gli indirizzi IP allocati.

Configurazione del routing statico per una rete di vApp


È possibile configurare determinate reti di vApp in modo che forniscano servizi di routing statico per consentire la comunicazione tra le macchine virtuali che si trovano in reti di vApp diverse.

Qualsiasi route statica che si crea viene attivata automaticamente.

Prerequisiti

Una rete di vApp instradata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Nella scheda **Routing**, fare clic su **Modifica**.

È possibile attivare o disattivare il routing statico per la rete.

Aggiunta di routing statico per una rete di vApp

È possibile aggiungere route statiche tra due reti di vApp instradate verso la stessa rete di virtual data center dell'organizzazione. Le route statiche consentono il traffico tra le reti.


Non è possibile aggiungere route statiche a una vApp con priorità applicata o tra reti che si sovrappongono. Dopo aver aggiunto una route statica a una rete di vApp, configurare le regole del firewall della rete per consentire il traffico sulla route statica. Per le vApp con route statiche, selezionare l'uso degli indirizzi IP assegnati fino all'eliminazione della vApp o delle reti associate.

Le route statiche funzionano solo quando sono in esecuzione le vApp che le contengono. Se si modifica la rete principale di una vApp, eliminare una vApp o una rete di vApp. Se la vApp include route statiche, tali route non possono funzionare ed è necessario rimuoverle manualmente.

Prerequisiti

- Due reti di vApp sono instradate verso la stessa rete di virtual data center dell'organizzazione.
- Le reti di vApp si trovano in vApp che sono state avviate almeno una volta.
- Il routing statico viene abilitato su entrambe le reti di vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Nella scheda **Routing**, in Routing statico fare clic su **Aggiungi**.
Vengono visualizzati gli indirizzi IP allocati.
- 6 Immettere il nome della route statica.
- 7 Immettere l'indirizzo di rete in formato CIDR.
L'indirizzo di rete è destinato alla rete di vApp a cui si desidera aggiungere una route statica.
- 8 Immettere l'indirizzo IP dell'hop successivo.
L'indirizzo IP dell'hop successivo è l'indirizzo IP esterno del router di quella rete di vApp.
- 9 Fare clic su **Salva**.
- 10 Ripetere la stessa procedura per la seconda rete di vApp.

Esempio: Esempio di routing statico

Rete di vApp 1 e Rete di vApp 2 sono entrambe instradate verso Rete di org condivisa. È possibile creare una route statica su ogni rete di vApp per consentire il traffico tra le reti. Le informazioni sulle reti di vApp possono essere utilizzate per creare le route statiche.

Tabella 3-2. Informazioni sulla rete

Nome rete	Specifica rete	Indirizzo IP esterno del router
Rete di vApp 1	192.168.1.0/24	192.168.0.100
Rete di vApp 2	192.168.2.0/24	192.168.0.101
Rete di org condivisa	192.168.0.0/24	ND

Sulla rete di vApp 1, creare una route statica verso la Rete di vApp 2. Sulla rete di vApp 2, creare una route statica verso Rete di vApp 1.

Tabella 3-3. Impostazioni del routing statico

Reti di vApp	Nome della route	Rete	Indirizzo IP dell'hop successivo
Rete di vApp 1	tovapp2	192.168.2.0/24	192.168.0.101
Rete di vApp 2	tovapp1	192.168.1.0/24	192.168.0.100

Aggiunta di una regola di port forwarding a una rete di vApp

È possibile configurare determinate reti di vApp affinché forniscano il port forwarding attraverso l'aggiunta di una regola di mapping NAT.

Il port forwarding, infatti, consente di accedere ai servizi in esecuzione sulle macchine virtuali nella rete di vApp.


Quando si configura il port forwarding, VMware Cloud Director mappa una porta esterna a un servizio in esecuzione su una macchina virtuale dedicata al traffico in entrata.

Quando si aggiunge una regola di port forwarding a una rete di vApp, viene visualizzata alla fine dell'elenco delle regole di mappatura NAT. Per informazioni su come impostare l'ordine di applicazione delle regole di port forwarding, vedere

Prerequisiti

- Verificare che la rete di vApp sia instradata.
- Verificare che il firewall nella rete di vApp sia attivato. Se si disattiva il firewall, le regole di mappatura NAT non vengono più applicate alla rete di vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Fare clic su **Servizi** e quindi su **Modifica**.

- 6 Per abilitare la rete NAT, attivare l'opzione NAT.
- 7 Dal menu a discesa **Tipo di NAT**, selezionare **Port forwarding** e fare clic su **Aggiungi**.
- 8 (Facoltativo) Per abilitare il mascheramento IP, selezionare la casella di controllo.
- 9 Configurare la regola di port forwarding.
 - a Selezionare una porta esterna.
 - b Selezionare una porta a cui eseguire l'inoltro.
 - c Selezionare un'interfaccia della macchina virtuale.
 - d Selezionare un protocollo per il tipo di traffico da inoltrare.
- 10 Fare clic su **Salva**.

Operazioni successive

Se necessario, riorganizzare le regole di port forwarding utilizzando i pulsanti **Sposta su** o **Sposta giù**.

Aggiunta di una regola di traduzione IP a una rete di vApp


È possibile configurare determinate reti di vApp affinché forniscano la traduzione IP aggiungendo una regola di mappatura NAT.

Quando si crea una regola di traduzione IP per una rete, vCloud Director aggiunge una regola DNAT e SNAT al gateway edge associato al gruppo di porte della rete. La regola DNAT traduce un indirizzo IP esterno in un indirizzo IP interno per il traffico in entrata. La regola SNAT traduce un indirizzo IP interno in un indirizzo IP esterno per il traffico in uscita.

Prerequisiti

- Verificare che la rete di vApp sia instradata.
- Verificare che il firewall nella rete di vApp sia attivato. Se si disattiva il firewall, le regole di mappatura NAT non vengono più applicate alla rete di vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti** fare clic su una rete per visualizzarne i dettagli.
- 5 Fare clic su **Servizi** e quindi su **Modifica**.
- 6 Per abilitare la rete NAT, attivare l'opzione NAT.
- 7 Dal menu a discesa **Tipo di NAT**, selezionare **Conversione IP** e fare clic su **Aggiungi**.

- 8 Selezionare un'interfaccia della macchina virtuale e fare clic su **Mantieni**.
- 9 Selezionare una modalità di mappatura.
- 10 Se si seleziona la modalità di mappatura **Manuale**, immettere un indirizzo IP esterno.
- 11 Fare clic su **Salva**.

Operazioni successive

Se necessario, riorganizzare le regole di conversione IP utilizzando i pulsanti **Sposta su** o **Sposta giù**.


Eliminazione di una rete di vApp

È possibile eliminare dalla vApp una rete non più necessaria.

Prerequisiti

La vApp viene arrestata e nessuna macchina virtuale della vApp viene connessa alla rete.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nella scheda della vApp selezionata, fare clic su **Dettagli**.
- 4 Nella scheda **Reti**, selezionare la rete che si desidera eliminare, quindi fare clic su **Elimina** e confermare l'eliminazione.

Utilizzo di snapshot

La creazione di uno snapshot consente di conservare lo stato e i dati delle macchine virtuali in una vApp associati a un momento specifico. Uno snapshot non è progettato per essere utilizzato per periodi di tempo prolungati o in sostituzione del backup della vApp.

È consigliabile utilizzare uno snapshot durante l'aggiornamento delle macchine virtuali in una vApp. Ad esempio, prima di aggiornare le macchine virtuali, è possibile creare uno snapshot per conservare i dati relativi al momento precedente l'aggiornamento. A tale scopo, prima di eseguire l'aggiornamento è necessario salvare uno snapshot. Se l'aggiornamento viene eseguito senza problemi, è possibile scegliere di rimuovere lo snapshot. Questa operazione comporterà il commit delle modifiche apportate durante l'aggiornamento. Tuttavia, se si verifica un problema, ripristinando lo snapshot è possibile ripristinare lo stato della vApp salvato prima dell'aggiornamento.

Creazione dello snapshot di una vApp


Se si crea lo snapshot di una vApp, si creano snapshot di tutte le macchine virtuali nella vApp. Dopo aver creato lo snapshot, è possibile utilizzarlo per ripristinare tutte le macchine virtuali nella vApp oppure rimuoverlo, se non è necessario.

Gli snapshot delle vApp hanno alcune limitazioni.

- Gli snapshot non acquisiscono le configurazioni delle NIC.
- Se una macchina virtuale presente nella vApp è connessa a un disco denominato, non è possibile creare uno snapshot della vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.

- 2 Fare clic su  per visualizzare le vApp in una vista a schede.

- 3 Dal menu **Azioni** della vApp di cui si desidera creare uno snapshot, scegliere **Crea snapshot**.

Se si crea uno snapshot di una vApp, viene sostituito lo snapshot eventualmente esistente.

- 4 (Facoltativo) Scegliere se creare lo snapshot della memoria della vApp.

Quando si acquisisce lo stato della memoria della vApp, lo snapshot conserva lo stato attivo della vApp e delle macchine virtuali nella vApp. Lo snapshot della memoria viene creato in un istante preciso, ad esempio per aggiornare software ancora in esecuzione. Se si crea uno snapshot della memoria e l'aggiornamento non viene completato come previsto oppure il software non soddisfa le aspettative, è possibile ripristinare lo stato precedente della macchina virtuale.

Quando si acquisisce lo stato della memoria, i file della vApp non richiedono la disattivazione. Se non si acquisisce lo stato della memoria, lo snapshot non salva lo stato attivo della vApp e i dischi sono coerenti con l'arresto anomalo del sistema, a meno che non vengano disattivati.

- 5 (Facoltativo) Scegliere se disattivare il file system guest.

Per eseguire questa operazione è necessario che nelle macchine virtuali nella vApp sia installato VMware Tools. Quando si disattiva una macchina virtuale, VMware Tools disattiva il file system della macchina virtuale. Un'operazione di disattivazione garantisce che un disco di snapshot rappresenti uno stato coerente dei file system guest. Gli snapshot con disattivazione sono appropriati per backup automatici o periodici. Ad esempio, se non si conosce l'attività della macchina virtuale, ma si desidera ripristinare alcuni backup recenti, è possibile disattivare i file.

Non è possibile disattivare vApp con dischi di grande capacità.

- 6 Fare clic su **OK**.

Risultati

Viene creato uno snapshot della vApp.

Operazioni successive

È possibile ripristinare tutte le macchine virtuali nella vApp allo snapshot più recente.


Ripristino di una vApp a una snapshot

È possibile ripristinare lo stato che tutte le macchine virtuali in una vApp avevano al momento della creazione della snapshot della vApp.

Prerequisiti

Verificare che esista uno snapshot per la vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp da ripristinare, selezionare **Ripristina snapshot**.
- 4 Fare clic su **OK**.

Risultati

Lo stato dello snapshot viene ripristinato per tutte le macchine virtuali nella vApp.

Rimozione dello snapshot di una vApp


È possibile rimuovere lo snapshot di una vApp.

Quando si rimuove uno snapshot della vApp, lo stato delle macchine virtuali nello snapshot viene eliminato definitivamente. La rimozione di uno snapshot non influisce sullo stato corrente della vApp.

Prerequisiti

È necessario avere creato uno snapshot della vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp per cui si desidera rimuovere lo snapshot, selezionare **Rimuovi snapshot**.

4 Fare clic su **OK**.

Risultati

Lo snapshot viene rimosso.

Creazione di snapshot di più vApp

Se si creano snapshot di più vApp, si creano snapshot di tutte le macchine virtuali nelle vApp. Dopo aver creato gli snapshot, è possibile utilizzarli per ripristinare tutte le macchine virtuali nelle vApp oppure rimuoverli, se non sono necessari.

Gli snapshot delle vApp hanno alcune limitazioni.

- Gli snapshot non acquisiscono le configurazioni delle NIC.
- Se una macchina virtuale presente in una vApp è connessa a un disco denominato, non è possibile creare uno snapshot della vApp.
- La creazione degli snapshot di più vApp non comporta la creazione di snapshot della memoria delle vApp e non disattiva il file system guest delle vApp. Se si desidera creare uno snapshot della memoria delle vApp o disattivare il file system guest, è necessario creare snapshot individuali per ogni vApp. Vedere [Creazione dello snapshot di una vApp](#).

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp per cui si desidera creare gli snapshot.
- 4 Dal menu **Azioni**, selezionare **Crea snapshot**, quindi fare clic su **OK** per confermare.

Operazioni successive

- È possibile ripristinare tutte le macchine virtuali nelle vApp agli snapshot più recenti. Vedere [Ripristino delle snapshot di più vApp](#).
- È possibile rimuovere gli snapshot delle vApp. Vedere [Rimozione degli snapshot di più vApp](#).

Rimozione degli snapshot di più vApp

Se gli snapshot di più vApp non sono necessari, è possibile rimuoverli contemporaneamente.

Quando si rimuove uno snapshot della vApp, lo stato delle macchine virtuali nello snapshot viene eliminato definitivamente. La rimozione di uno snapshot non influisce sullo stato corrente della vApp.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.

- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp di cui si desidera rimuovere gli snapshot.
- 4 Dal menu **Azioni**, selezionare **Rimuovi snapshot**.

Ripristino delle snapshot di più vApp

È possibile ripristinare lo stato che tutte le macchine virtuali in più vApp avevano al momento della creazione delle snapshot delle vApp.

Prerequisiti

Verificare che per le vApp che si desidera ripristinare esistano snapshot.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp che si desidera ripristinare agli snapshot più recenti.
- 4 Dal menu **Azioni**, selezionare **Ripristina snapshot**.
- 5 Fare clic su **OK** per confermare.


Modifica del proprietario di una vApp

È possibile cambiare il proprietario di una vApp se, ad esempio, lascia l'azienda o cambia ruolo.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Nel menu **Azioni** della vApp di cui si desidera cambiare il proprietario, selezionare **Cambia proprietario**.
- 4 Selezionare un utente nell'elenco.
- 5 Fare clic su **OK**.

Risultati

Il proprietario della vApp viene cambiato.


Spostamento di una vApp in un altro virtual data center

Quando si sposta una vApp in un altro virtual data center, tale vApp viene rimossa dal virtual data center di origine.

Prerequisiti

- Si dispone almeno del ruolo **Autore vApp**.
- La vApp è disattivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp che si desidera spostare, selezionare **Sposta in**.
- 4 Selezionare il virtual data center in cui si desidera spostare la vApp e fare clic su **OK**.
- 5 (Facoltativo) Selezionare il criterio di storage.
- 6 Fare clic su **OK**.

Risultati

La vApp viene rimossa dal data center di origine e spostata nel data center di destinazione.


Copia di una vApp arrestata in un altro virtual data center

Quando si copia una vApp in un altro virtual data center, la vApp originale rimane nel virtual data center di origine.

Prerequisiti

- Si dispone almeno del ruolo **Autore vApp**.
- La vApp è disattivata.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp da copiare, selezionare **Copia in**.
- 4 Digitare un nome e una descrizione.
- 5 Selezionare il virtual data center in cui si desidera creare la copia della vApp.

6 (Facoltativo) Selezionare un criterio di storage.

7 Fare clic su **OK**.

Risultati

La vApp viene copiata con il nome e la descrizione forniti per il virtual data center specificato.

Copia di una vApp attivata


Per creare una vApp basata su una vApp esistente, è possibile copiarne una e modificarla in base alle proprie esigenze. Non è necessario disattivare le macchine virtuali nella vApp prima di copiare la vApp. Lo stato di memoria delle macchine virtuali in esecuzione viene mantenuto nella vApp copiata.

Prerequisiti

Verificare che siano soddisfatte le seguenti condizioni.

- È necessario disporre almeno del ruolo **Utente vApp**.
- Il virtual data center dell'organizzazione è supportato da vCenter Server 5.5 o versioni successive.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp da copiare, selezionare **Copia in**.
- 4 Digitare un nome e una descrizione.
- 5 Selezionare il virtual data center in cui si desidera creare la copia della vApp.
- 6 (Facoltativo) Selezionare un criterio di storage.
- 7 Fare clic su **OK**.

Risultati

Viene creata una copia della vApp, che si trova nello stato di sospensione. La vApp copiata viene abilitata per l'applicazione delle priorità di rete.

Operazioni successive

Modificare le proprietà di rete della nuova vApp o attivare la vApp.

Aggiunta di una macchina virtuale a una vApp


È possibile aggiungere macchine virtuali a una vApp.

Prerequisiti

Per accedere alle macchine virtuali nei cataloghi pubblici, è necessario essere **Amministratore organizzazione** o **Autore vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.

- 2 Fare clic su  per visualizzare le vApp in una vista a schede.

- 3 Dal menu **Azioni** della vApp a cui si desidera aggiungere una macchina virtuale, selezionare **Aggiungi macchina virtuale**.

L'elenco delle macchine virtuali associate alla vApp viene visualizzato nella finestra **Aggiungi macchine virtuali**.

- 4 Per creare una nuova macchina virtuale e associarla automaticamente alla vApp, fare clic su **Aggiungi macchina virtuale**.
- 5 Immettere il nome e il nome del computer per la macchina virtuale.

Importante Il nome del computer può contenere solo caratteri alfanumerici e trattini. Non può essere costituito solo da cifre e non può contenere spazi.

- 6 (Facoltativo) Immettere una descrizione significativa.
- 7 Selezionare se si desidera che la macchina virtuale venga accesa subito dopo la creazione.

8 Selezionare la modalità di distribuzione della macchina virtuale.

Opzione	Azione
Nuova	<p>È possibile distribuire una nuova macchina virtuale con impostazioni personalizzabili.</p> <ul style="list-style-type: none"> a Selezionare una famiglia di sistemi operativi e il sistema operativo. b (Facoltativo) Selezionare un'immagine di avvio. c Selezionare il criterio di calcolo. d Selezionare la dimensione della macchina virtuale o fare clic su Opzioni di dimensionamento personalizzate per immettere manualmente le impostazioni di calcolo, memoria e storage. <p>Le opzioni di dimensionamento predefinite sono Piccola, Media o Grande.</p> <ul style="list-style-type: none"> e Specificare le impostazioni di storage della macchina virtuale, ad esempio i criteri di storage e la dimensione in GB. f Specificare le impostazioni di rete per la macchina virtuale, ad esempio rete, modalità IP, indirizzo IP e NIC primario.
Da modello	<p>È possibile distribuire la macchina virtuale da un modello selezionato nel catalogo dei modelli.</p> <ul style="list-style-type: none"> a Selezionare il modello della macchina virtuale dal catalogo. b (Facoltativo) Scegliere di utilizzare un criterio di storage personalizzato e selezionare il criterio in Criterio di storage personalizzato da utilizzare. c Se è disponibile un accordo di licenza con l'utente finale, è necessario leggerlo e accettarlo.

9 Fare clic su **OK** per creare la macchina virtuale.

10 Fare clic su **Aggiungi** per aggiungere la macchina virtuale alla vApp.

Salvataggio di una vApp come modello di vApp in un catalogo

Se si aggiunge una vApp a un catalogo, tale vApp viene convertita in un modello di vApp.


A partire da VMware Cloud Director 10.2.2, quando si aggiunge una vApp a un catalogo, il modello di vApp include i criteri di posizionamento e dimensionamento della vApp di origine come tag non modificabili.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Autore vApp** predefinito o un set di diritti equivalente.
- L'organizzazione deve disporre di un catalogo e di un virtual data center con spazio disponibile.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.

- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp da aggiungere a un catalogo, scegliere **Aggiungi al catalogo**.

Nota È possibile aggiungere una vApp a un catalogo anche se le macchine virtuali che appartengono alla vApp sono in esecuzione. Tuttavia, se si seleziona una vApp in esecuzione, questa viene aggiunta al catalogo come modello di vApp e tutte le macchine virtuali si trovano nello stato di sospensione.

- 4 Selezionare il catalogo di destinazione dal menu a discesa **Catalogo**.
- 5 Immettere un nome e, facoltativamente, una descrizione per il modello di vApp.
- 6 (Facoltativo) Selezionare **Sovrascrivi l'elemento di catalogo** se si desidera che il nuovo elemento del catalogo sovrascriva qualsiasi modello di vApp esistente e selezionare l'elemento del catalogo da sovrascrivere.

Ad esempio, quando si carica una nuova versione di una vApp nel catalogo, è possibile sovrascrivere la versione precedente.

- 7 Specificare come verrà utilizzato il modello.

L'impostazione viene applicata durante la creazione di una vApp basata sul modello di vApp. Viene invece ignorata quando si crea una vApp utilizzando singole macchine virtuali provenienti dal modello.

Opzione	Descrizione
Crea copia identica	Selezionare questa opzione per creare una copia identica della vApp quando si crea una vApp dal modello di vApp.
Personalizza impostazioni macchina virtuale	Selezionare questa opzione per consentire la personalizzazione delle impostazioni della macchina virtuale quando si crea una vApp dal modello di vApp.

- 8 Per completare la creazione del modello di vApp, fare clic su **OK**.

Risultati

Il modello di vApp viene visualizzato nel catalogo specificato.


Scaricare una vApp da pacchetto OVF

È possibile scaricare una vApp come pacchetto OVF o come OVA, ovvero una distribuzione di file singola dello stesso pacchetto di file OVF.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Autore vApp** predefinito o un set di diritti equivalente.
- Verificare che la vApp sia disattivata e non distribuita.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Fare clic su  per visualizzare le vApp in una vista a schede.
- 3 Dal menu **Azioni** della vApp che si desidera scaricare, selezionare **Scarica**.
- 4 Selezionare il formato in cui si desidera scaricare la vApp.
- 5 (Facoltativo) Selezionare **Mantieni informazioni di identità** per includere gli indirizzi UUID e MAC delle macchine virtuali che si trovano nella vApp nel pacchetto OVF scaricato.
Questa opzione limita la portabilità del pacchetto e deve essere utilizzata solo quando è necessario.
- 6 Fare clic su **OK** per confermare la selezione e avviare il download.

Risultati

Per impostazione predefinita, il pacchetto viene scaricato nella cartella `Download` del browser.

Rinnovo del lease di una vApp

Se il lease di una vApp è scaduto o sta per scadere, è possibile rinnovarlo.

Prerequisiti

Verificare che sia stato assegnato il ruolo predefinito **Utente vApp** o una serie di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Selezionare la vApp di cui si desidera rinnovare il lease.
- 3 Dal menu **Azioni**, selezionare **Rinnova lease**.
- 4 Rinnovare il lease di runtime della vApp.
 - a Selezionare la casella di controllo **Lease di runtime**
 - b Dal menu a discesa, selezionare un valore per il lease di runtime.
È possibile selezionare un valore in ore o giorni oppure impostare il lease su **Nessuna scadenza**. Gli **amministratori di sistema** possono limitare la lunghezza massima che è possibile scegliere.

5 Rinnovare il lease di storage della vApp.

- a Selezionare la casella di controllo **Lease dello storage**.
- b Dal menu a discesa, selezionare un valore per il lease dello storage.

È possibile selezionare un valore in ore o giorni oppure impostare il lease su **Nessuna scadenza**. Gli **amministratori di sistema** possono limitare la lunghezza massima che è possibile scegliere.

Eliminazione di una vApp

È possibile eliminare una vApp. Dopo l'eliminazione, la vApp viene rimossa dall'organizzazione.

Prerequisiti

È necessario arrestare la vApp.

È necessario essere almeno un **autore vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Selezionare la vApp che si desidera eliminare.
- 3 Dal menu **Azioni**, selezionare **Elimina**.
- 4 Fare clic su **OK**.

Risultati

La vApp viene eliminata.

Eliminazione di più vApp

Per rimuovere più vApp dall'organizzazione, è possibile eliminarle contemporaneamente.

Prerequisiti

- Verificare che le vApp siano state arrestate.
- Verificare di essere almeno un **autore di vApp**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **vApp** nel pannello sinistro.
- 2 Attivare l'opzione **Multiselezione**.
- 3 Selezionare le vApp che si desidera eliminare.
- 4 Dal menu **Azioni**, selezionare **Elimina**.

5 Per confermare, fare clic su **Elimina**.

Utilizzo dei cluster di Kubernetes

4

È possibile creare cluster Kubernetes con nodi di dimensioni diverse dai criteri di VDC dell'organizzazione esistenti.

Kubernetes Container Clusters è il plug-in di Container Service Extension per VMware Cloud Director. È possibile utilizzare il plug-in Kubernetes Container Clusters nel VMware Cloud Director Tenant Portal per distribuire cluster con cluster nativi e VMware Tanzu Kubernetes Grid Integrated Edition (TKGI). È possibile creare cluster Tanzu Kubernetes senza il plug-in Kubernetes Container Clusters.

Se abilitato in un cluster vSphere, VMware vSphere® with VMware Tanzu™ offre la possibilità di creare cluster Kubernetes upstream in pool di risorse dedicati. Per ulteriori informazioni, vedere la guida *Configurazione e gestione di vSphere with Kubernetes* nella documentazione di vSphere.

Quando un provider di servizi crea un criterio Kubernetes del VDC del provider e pubblica il criterio in un VDC dell'organizzazione, crea un criterio Kubernetes del VDC dell'organizzazione. È possibile utilizzare il plug-in Kubernetes Container Clusters per creare i cluster di Tanzu Kubernetes applicando uno dei criteri Kubernetes del VDC dell'organizzazione.

Opzioni di runtime Kubernetes

- Cluster di Tanzu Kubernetes: è possibile utilizzare l'opzione di runtime Kubernetes vSphere per creare cluster di Tanzu Kubernetes gestiti da vSphere with VMware Tanzu. Questa opzione offre ulteriori funzionalità, tuttavia, potrebbe essere più costosa. Per ulteriori informazioni, vedere la guida *Configurazione e gestione di vSphere with Kubernetes* nella documentazione di vSphere.
- Cluster nativi: il plug-in Kubernetes Container Clusters gestisce i cluster con il runtime Kubernetes nativo. Questi cluster hanno una funzionalità di elevata disponibilità ridotta con un unico nodo del piano di controllo, offrono meno scelte di volumi persistenti e nessuna automazione di rete. Tuttavia, potrebbero avere un costo inferiore.
- Cluster TKGI: VMware Tanzu Kubernetes Grid Integrated Edition è una soluzione di container creata appositamente per rendere operativo Kubernetes per le aziende e i provider di servizi multi-cloud. Alcune delle sue funzionalità sono la disponibilità elevata, la scalabilità automatica, i controlli di integrità, nonché la riparazione automatica e gli aggiornamenti in sequenza per i cluster Kubernetes. Per ulteriori informazioni sui cluster TKGI, vedere la documentazione di *VMware Tanzu Kubernetes Grid Integrated Edition*.

Questo capitolo include i seguenti argomenti:

- [Aggiunta di un criterio Kubernetes del VDC dell'organizzazione](#)
- [Modifica del criterio Kubernetes del VDC dell'organizzazione](#)
- [Creazione di un cluster Tanzu Kubernetes](#)
- [Creazione di un cluster Kubernetes nativo](#)
- [Creazione di un cluster VMware Tanzu Kubernetes Grid Integrated Edition](#)
- [Configurazione dell'accesso esterno a un servizio in un cluster Tanzu Kubernetes](#)

Aggiunta di un criterio Kubernetes del VDC dell'organizzazione

Se si dispone di diritti di **amministratore di sistema**, è possibile aggiungere un criterio Kubernetes del VDC dell'organizzazione utilizzando un criterio Kubernetes del VDC del provider. È possibile utilizzare il criterio Kubernetes del VDC dell'organizzazione per creare i cluster di Tanzu Kubernetes.

Quando si aggiunge o si pubblica un criterio Kubernetes del VDC del provider in un VDC dell'organizzazione, il criterio viene reso disponibile per i tenant mediante la creazione di un criterio del VDC dell'organizzazione. I tenant possono utilizzare i criteri Kubernetes del VDC dell'organizzazione disponibili per sfruttare la capacità Kubernetes durante la creazione dei cluster di Tanzu Kubernetes. Un criterio Kubernetes incapsula il posizionamento, la qualità dell'infrastruttura e le classi di storage del volume persistente. I criteri Kubernetes possono avere diversi limiti di calcolo.

È possibile aggiungere più criteri Kubernetes del VDC dell'organizzazione a un singolo VDC dell'organizzazione. È possibile utilizzare un singolo criterio Kubernetes del VDC del provider per creare più criteri Kubernetes del VDC dell'organizzazione. È possibile utilizzare i criteri Kubernetes del VDC dell'organizzazione come indicatore della qualità del servizio. Ad esempio, è possibile pubblicare un criterio Kubernetes Gold che consente una selezione delle classi di macchine guaranteed e una classe di storage rapida o un criterio Kubernetes Silver che consente una selezione delle classi di macchine best effort e una classe di storage lenta.

Prerequisiti

- Verificare di disporre di un ruolo di **amministratore di sistema** o di un ruolo che includa un set di diritti equivalente. Tutti gli altri ruoli possono solo visualizzare i criteri Kubernetes del VDC dell'organizzazione.
- Verificare che nell'ambiente sia presente almeno un VDC del provider supportato da un cluster Supervisore. I VDC del provider supportati da un cluster Supervisore sono contrassegnati con un'icona di Kubernetes nella scheda **VDC del provider** del Service Provider Admin Portal. Per ulteriori informazioni su vSphere with VMware Tanzu in VMware Cloud Director, vedere [Utilizzo di vSphere with Kubernetes in VMware Cloud Director](#) nella *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*.

- Verificare di aver effettuato l'accesso a un VDC dell'organizzazione Flex.
- Familiarizzare con i tipi di classi di macchine virtuali per i cluster di Tanzu Kubernetes. Consultare la guida *Configurazione e gestione di vSphere with Kubernetes* nella documentazione di vSphere.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Data center** e quindi su **Virtual data center**.
- 2 Selezionare un virtual data center dell'organizzazione.
- 3 Nel pannello sinistro, in **Impostazioni**, selezionare **Criteri Kubernetes** e fare clic su **Aggiungi**.
Viene visualizzata la procedura guidata **Pubblica nel VDC dell'organizzazione**.
- 4 Immettere il nome e la descrizione di un tenant visibile per il criterio Kubernetes del VDC dell'organizzazione e fare clic su **Avanti**.
- 5 Selezionare il criterio Kubernetes del VDC del provider che si desidera utilizzare e fare clic su **Avanti**.
- 6 Selezionare i limiti di memoria e CPU per i cluster di Tanzu Kubernetes creati in questo criterio.
I limiti massimi dipendono dalle allocazioni di CPU e memoria del VDC dell'organizzazione. Quando si aggiunge il criterio, i limiti selezionati agiscono come valori massimi per i tenant.
- 7 Scegliere se si desidera riservare la CPU e la memoria per i nodi del cluster di Tanzu Kubernetes creati in questo criterio e fare clic su **Avanti**.
Sono disponibili due edizioni per ogni tipo di classe: guaranteed e best effort. Una classe guaranteed riserva completamente le sue risorse configurate, mentre una classe best effort consente di eseguire l'overcommit delle risorse. In base alla selezione, nella pagina successiva della procedura guidata è possibile selezionare tra tipi di classi di macchine virtuali guaranteed o best effort.
 - Selezionare **Sì** per i tipi di classe di macchine virtuali guaranteed per le prenotazioni complete di CPU e memoria.
 - Selezionare **No** per i tipi di classi di macchine virtuali best effort senza prenotazioni di CPU e memoria.
- 8 Nella pagina **Classi macchina** della procedura guidata, selezionare uno o più tipi di classi di macchine virtuali disponibili per questo criterio.
Le classi di macchine selezionate sono gli unici tipi di classe disponibili per i tenant quando si aggiunge il criterio al VDC dell'organizzazione.
- 9 Selezionare uno o più criteri di storage.
- 10 Rivedere le scelte e fare clic su **Pubblica**.

Risultati

Le informazioni sui criteri pubblicati vengono visualizzate nell'elenco dei criteri Kubernetes. Il criterio pubblicato crea uno spazio dei nomi Supervisore nel cluster Supervisore con i limiti delle risorse specificati dal criterio.

I tenant possono iniziare a utilizzare il criterio Kubernetes per creare i cluster di Tanzu Kubernetes. VMware Cloud Director posiziona ogni cluster di Tanzu Kubernetes creato in questo criterio Kubernetes nello stesso spazio dei nomi Supervisore. I limiti delle risorse dei criteri diventano limiti delle risorse per lo spazio dei nomi Supervisore. Tutti i cluster di Tanzu Kubernetes creati dal tenant nello spazio dei nomi Supervisore competono per le risorse entro questi limiti.

Operazioni successive

- Eliminare un criterio Kubernetes del VDC dell'organizzazione.
- Utilizzando il Service Provider Admin Portal, è possibile gestire le quote delle risorse dell'organizzazione. Vedere [Gestione delle quote nel consumo di risorse di un'organizzazione](#) nella *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*.
- [Gestione delle quote delle risorse di un gruppo](#) o [Gestione delle quote delle risorse di un utente](#)

Modifica del criterio Kubernetes del VDC dell'organizzazione

Se si dispone di diritti di **amministratore di sistema**, è possibile modificare il criterio Kubernetes del VDC dell'organizzazione per modificarne la descrizione e i limiti di CPU e memoria.

Prerequisiti

Verificare di disporre di un ruolo di **amministratore di sistema** o di un ruolo che includa un set di diritti equivalente. Tutti gli altri ruoli possono solo visualizzare i criteri Kubernetes del VDC dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Data center** e quindi su **Virtual data center**.
- 2 Selezionare un virtual data center dell'organizzazione.
- 3 Nel pannello sinistro, in **Impostazioni**, fare clic su **Criteri Kubernetes**.
- 4 Selezionare il criterio Kubernetes del VDC dell'organizzazione che si desidera modificare e fare clic su **Modifica**.

Viene visualizzata la procedura guidata **Modifica criterio Kubernetes VDC**.

- 5 Modificare la descrizione del criterio Kubernetes del VDC dell'organizzazione e fare clic su **Avanti**.

Il nome del criterio è collegato allo spazio dei nomi Supervisore, creato durante la pubblicazione del criterio; non può essere modificato.

- 6 Modificare il limite di CPU e memoria per il criterio Kubernetes del VDC dell'organizzazione e fare clic su **Avanti**.

Non è possibile modificare la prenotazione della CPU e della memoria.

- 7 Rivedere i dettagli dei nuovi criteri e fare clic su **Salva**.

Operazioni successive

- Eliminare un criterio Kubernetes del VDC dell'organizzazione.
- Utilizzando il Service Provider Admin Portal, è possibile modificare le quote delle risorse dell'organizzazione. Vedere [Gestione delle quote nel consumo di risorse di un'organizzazione](#) nella *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*.
- Modificare le quote di gruppi e utenti. Vedere [Gestione delle quote delle risorse di un gruppo](#) o [Gestione delle quote delle risorse di un utente](#).

Creazione di un cluster Tanzu Kubernetes

È possibile creare cluster Tanzu Kubernetes utilizzando il plug-in Kubernetes Container Clusters.

Per ulteriori informazioni sulle diverse opzioni di runtime Kubernetes per la creazione del cluster, vedere [Capitolo 4 Utilizzo dei cluster di Kubernetes](#).

È possibile gestire i cluster Kubernetes anche utilizzando la CLI Container Service Extension. Vedere la documentazione relativa a [Container Service Extension](#).

VMware Cloud Director esegue il provisioning dei cluster Tanzu Kubernetes con il PodSecurityPolicy Admission Controller abilitato. È necessario creare un criterio di sicurezza pod per distribuire i carichi di lavoro. Per informazioni sull'implementazione dell'uso dei criteri di sicurezza pod in Kubernetes, vedere l'argomento *Utilizzo dei criteri di sicurezza pod con i cluster Kubernetes Tanzu* nella *Guida alla configurazione e alla gestione di vSphere with Kubernetes*.

Prerequisiti

- Verificare che il provider di servizi abbia pubblicato il plug-in Kubernetes Container Clusters nell'organizzazione. Il plug-in si trova nella barra di navigazione superiore in **Altro > Kubernetes Container Clusters**.
- Verificare che nel proprio VDC dell'organizzazione sia presente almeno un criterio Kubernetes del VDC dell'organizzazione. Per aggiungere un criterio Kubernetes del VDC dell'organizzazione, vedere [Aggiunta di un criterio Kubernetes del VDC dell'organizzazione](#).
- Verificare che il provider di servizi abbia pubblicato il bundle dei diritti **vmware:tkgcluster Entitlement** nell'organizzazione e abbia concesso il diritto **Edit: Tanzu Kubernetes Guest Cluster** per la creazione e la modifica dei cluster Tanzu Kubernetes. Per poter eliminare i cluster, è necessario disporre del diritto **Full Control: Tanzu Kubernetes Guest Cluster**.
- Verificare che il provider di servizi abbia creato una voce di elenco di controllo di accesso (ACL) con informazioni sul livello di accesso.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Altro > Kubernetes Container Clusters**.
- 2 (Facoltativo) Se il VDC dell'organizzazione è abilitato per la creazione del cluster TKGI, nella pagina **Kubernetes Container Clusters**, selezionare la scheda **vSphere con Tanzu e nativo**.
- 3 Fare clic su **Nuovo**.
- 4 Selezionare l'opzione di runtime **vSphere con Tanzu** e fare clic su **Avanti**.
- 5 Immettere un nome per il nuovo cluster Kubernetes e fare clic su **Avanti**.
- 6 Selezionare il VDC dell'organizzazione in cui si desidera distribuire un cluster Tanzu Kubernetes e fare clic su **Avanti**.
- 7 Selezionare un criterio Kubernetes del VDC dell'organizzazione e una versione di Kubernetes, quindi fare clic su **Avanti**.

VMware Cloud Director mostra un set predefinito di versioni di Kubernetes che non sono collegate ad alcun VDC dell'organizzazione o criterio Kubernetes. Queste versioni sono un'impostazione globale. Per modificare l'elenco delle versioni disponibili, utilizzare lo strumento di gestione delle celle per eseguire il comando `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v version_numbers` con i numeri di versione separati da virgole.

- 8 Selezionare il numero di piano di controllo e nodi di lavoro nel nuovo cluster.
- 9 Selezionare le classi di macchine per il piano di controllo e i nodi di lavoro, quindi fare clic su **Avanti**.
- 10 Selezionare una classe di storage dei criteri Kubernetes per il piano di controllo e i nodi di lavoro, quindi fare clic su **Avanti**.
- 11 (Facoltativo) In VMware Cloud Director 10.2.2 e versioni successive, specificare un intervallo di indirizzi IP per i servizi Kubernetes e un intervallo per i pod Kubernetes, quindi fare clic su **Avanti**.

Il routing CIDR (Classless Inter-Domain Routing) è un metodo per il routing IP e l'allocazione degli indirizzi IP.

Opzione	Descrizione
<code>Pods CIDR</code>	Specifica un intervallo di indirizzi IP da utilizzare per i pod Kubernetes. Il valore predefinito è 192.168.0.0/16. La dimensione della subnet dei pod deve essere maggiore o uguale a /24. Questo valore non deve sovrapporsi alle impostazioni di Supervisor Cluster. È possibile immettere un intervallo di IP.
<code>Services CIDR</code>	Specifica un intervallo di indirizzi IP da utilizzare per i servizi Kubernetes. Il valore predefinito è 10.96.0.0/12. Questo valore non deve sovrapporsi alle impostazioni di Supervisor Cluster. È possibile immettere un intervallo di IP.

12 Controllare le impostazioni del cluster e fare clic su **Fine**.

Operazioni successive

- Ridimensionare il cluster di Kubernetes se si desidera modificare il numero di nodi di lavoro.
- Scaricare il file kubeconfig. Lo strumento della riga di comando kubectl utilizza i file kubeconfig per ottenere informazioni su cluster, utenti, spazi dei nomi e meccanismi di autenticazione.
- Eliminare un cluster Kubernetes.

Creazione di un cluster Kubernetes nativo

È possibile creare cluster Kubernetes gestiti da Container Service Extension 3.0 con il plug-in Kubernetes Container Clusters.

Per ulteriori informazioni sulle diverse opzioni di runtime Kubernetes per la creazione del cluster, vedere [Capitolo 4 Utilizzo dei cluster di Kubernetes](#).

È possibile gestire i cluster Kubernetes anche utilizzando la CLI Container Service Extension. Vedere la documentazione relativa a [Container Service Extension](#).

Prerequisiti

- Verificare che il provider di servizi abbia pubblicato il plug-in Kubernetes Container Clusters nell'organizzazione. Kubernetes Container Clusters è il plug-in di Container Service Extension per VMware Cloud Director. Il plug-in si trova nella barra di navigazione superiore in **Altro > Kubernetes Container Clusters**.
- Verificare che il provider di servizi abbia completato la configurazione del server Container Service Extension 3.0 e abbia pubblicato un criterio di posizionamento nativo di Container Service Extension nel VDC dell'organizzazione.
- Verificare che il provider di servizi abbia pubblicato il bundle dei diritti **cse:nativeCluster Entitlement** nell'organizzazione e abbia concesso il diritto **Edit CSE:NATIVECLUSTER** per la creazione e la modifica dei cluster Kubernetes nativi. Per poter eliminare i cluster, è necessario disporre del diritto **Full Control CSE:NATIVECLUSTER**.
- Verificare che il provider di servizi abbia creato una voce di elenco di controllo di accesso (ACL) con informazioni sul livello di accesso.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Altro > Kubernetes Container Clusters**.
- 2 (Facoltativo) Se il VDC dell'organizzazione è abilitato per la creazione del cluster TKGI, nella pagina **Kubernetes Container Clusters**, selezionare la scheda **vSphere con Tanzu e nativo**.
- 3 Fare clic su **Nuovo**.
- 4 Selezionare l'opzione di runtime Kubernetes **Nativa**.
- 5 Immettere un nome e selezionare un modello Kubernetes dall'elenco.

- 6 (Facoltativo) Immettere una descrizione per il nuovo cluster Kubernetes e una chiave pubblica SSH.
- 7 Fare clic su **Avanti**.
- 8 Selezionare il VDC dell'organizzazione in cui si desidera distribuire un cluster nativo e fare clic su **Avanti**.
- 9 Selezionare il numero di piani di controllo e nodi di lavoro e, facoltativamente, i criteri di dimensionamento per i nodi.
- 10 Fare clic su **Avanti**.
- 11 Se si desidera distribuire una macchina virtuale aggiuntiva con il software NFS, attivare **Abilita NFS**.
- 12 (Facoltativo) Selezionare i criteri di storage per il piano di controllo e i nodi di lavoro.
- 13 Fare clic su **Avanti**.
- 14 Selezionare una rete per il cluster Kubernetes e fare clic su **Avanti**.
- 15 Controllare le impostazioni del cluster e fare clic su **Fine**.

Operazioni successive

- Ridimensionare il cluster di Kubernetes se si desidera modificare il numero di nodi di lavoro.
- Scaricare il file kubeconfig. Lo strumento della riga di comando kubectl utilizza i file kubeconfig per ottenere informazioni su cluster, utenti, spazi dei nomi e meccanismi di autenticazione.
- Eliminare un cluster Kubernetes.

Creazione di un cluster VMware Tanzu Kubernetes Grid Integrated Edition

È possibile creare cluster VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) utilizzando Container Service Extension.

Per ulteriori informazioni sulle diverse opzioni di runtime Kubernetes per la creazione del cluster, vedere [Capitolo 4 Utilizzo dei cluster di Kubernetes](#).

È possibile gestire i cluster Kubernetes anche utilizzando la CLI Container Service Extension. Vedere la documentazione relativa a [Container Service Extension](#).

Prerequisiti

- Verificare che il provider di servizi abbia pubblicato il plug-in Kubernetes Container Clusters nell'organizzazione. Kubernetes Container Clusters è il plug-in di Container Service Extension per VMware Cloud Director. Il plug-in si trova nella barra di navigazione superiore in **Altro > Kubernetes Container Clusters**.

- Verificare che il provider di servizi abbia completato la configurazione del server Container Service Extension 3.0 e abbia pubblicato i metadati di abilitazione TKGI di Container Service Extension nel VDC dell'organizzazione.
- Verificare di disporre del diritto **{cse}:PKS DEPLOY RIGHT**.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Altro > Kubernetes Container Clusters**.
- 2 Nella pagina **Kubernetes Container Clusters**, selezionare la scheda **TKGI** e fare clic su **Nuovo**.
Viene aperta la procedura guidata **Crea nuovo cluster TKGI**.
- 3 Selezionare il VDC dell'organizzazione in cui si desidera distribuire un cluster TKGI e fare clic su **Avanti**.

Il caricamento dell'elenco potrebbe richiedere più tempo perché VMware Cloud Director richiede le informazioni dal server CSE.
- 4 Immettere un nome per il nuovo cluster TKGI e selezionare il numero di nodi di lavoro.

I cluster TKGI devono includere almeno un nodo di lavoro.
- 5 Fare clic su **Avanti**.
- 6 Controllare le impostazioni del cluster e fare clic su **Fine**.
- 7 (Facoltativo) Fare clic sul pulsante **Aggiorna** sul lato destro della pagina in cui il nuovo cluster TKGI viene visualizzato nell'elenco dei cluster.

Operazioni successive

- Ridimensionare il cluster di Kubernetes se si desidera modificare il numero di nodi di lavoro.
- Scaricare il file kubeconfig. Lo strumento della riga di comando kubectl utilizza i file kubeconfig per ottenere informazioni su cluster, utenti, spazi dei nomi e meccanismi di autenticazione.
- Eliminare un cluster Kubernetes.

Configurazione dell'accesso esterno a un servizio in un cluster Tanzu Kubernetes

A partire da VMware Cloud Director 10.2.2, i cluster Tanzu Kubernetes sono raggiungibili per impostazione predefinita solo da subnet IP di reti all'interno dello stesso virtual data center dell'organizzazione in cui viene creato un cluster. Se necessario, è possibile configurare manualmente l'accesso esterno a servizi specifici in un cluster Tanzu Kubernetes.

Quando un criterio Kubernetes del VDC viene pubblicato in un VDC dell'organizzazione, viene automaticamente eseguito il provisioning di un criterio del firewall nel gateway edge del cluster per consentire l'accesso al cluster da origini autorizzate all'interno del VDC. Viene inoltre aggiunta automaticamente una regola SNAT di sistema ai gateway edge NSX-T Data Center all'interno del VDC dell'organizzazione per garantire che il gateway edge del cluster sia raggiungibile dai carichi di lavoro nel VDC dell'organizzazione.

Nota Se il virtual data center dell'organizzazione fa parte di un gruppo di NSX-T Data Center, il gateway edge del cluster non è raggiungibile dagli altri VDC del gruppo di data center.

Il criterio del firewall di cui viene eseguito il provisioning nel gateway edge del cluster e la regola SNAT nel gateway edge NSX-T Data Center non possono essere rimossi, a meno che un **amministratore di sistema** non elimini il criterio Kubernetes dal VDC.

Se necessario, è possibile configurare manualmente l'accesso da una rete esterna a un servizio specifico in un cluster Tanzu Kubernetes. A tale scopo, è necessario creare una regola DNAT nel gateway edge NSX-T Data Center che garantisca che il traffico proveniente da posizioni esterne venga inoltrato al gateway edge del cluster.

Prerequisiti

- Verificare che l'infrastruttura cloud sia supportata da vSphere 7.0 Update 1C, 7.0 Update 2 o versioni successive. Contattare l'**amministratore di sistema**.
- Assicurarsi di essere un **amministratore dell'organizzazione**.
- Verificare che l'**amministratore di sistema** abbia creato un gateway edge NSX-T Data Center all'interno del virtual data center dell'organizzazione in cui si trova il cluster Tanzu Kubernetes.
- Verificare che l'indirizzo IP pubblico che si desidera utilizzare per il servizio sia stato allocato all'interfaccia del gateway edge in cui si desidera aggiungere una regola DNAT.
- Utilizzare il comando `get services my-service` dello strumento da riga di comando `kubectl` per recuperare l'IP esterno per il servizio che si desidera esporre.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge e, in **Servizi**, fare clic su **NAT**.
- 3 Per aggiungere una regola, fare clic su **Nuovo**.
- 4 Configurare una regola DNAT per il servizio che si desidera connettere a una rete esterna.

Opzione	Descrizione
Nome	Immettere un nome significativo per la regola.
Descrizione	(Facoltativo) Immettere una descrizione per la regola.
Stato	Per abilitare la regola al momento della creazione, attivare l'interruttore Stato .

Opzione	Descrizione
Tipo di interfaccia	Dal menu a discesa, selezionare DNAT.
IP esterno	Immettere l'indirizzo IP pubblico del servizio. L'indirizzo IP immesso deve appartenere all'intervallo di IP sottoallocato del gateway edge NSX-T Data Center.
Applicazione	Lasciare vuota la casella.
IP interno	Immettere l'indirizzo IP del servizio allocato dal pool in entrata di Kubernetes.
Porta interna	(Facoltativo) Immettere il numero della porta a cui viene indirizzato il traffico in entrata.
Registrazione	(Facoltativo) Per registrare la conversione degli indirizzi da parte di questa regola, attivare l'opzione Registrazione .

5 Fare clic su **Salva**.

Operazioni successive

Se si desidera fornire l'accesso ad altre applicazioni pubblicate come servizi Kubernetes da reti esterne, è necessario configurare regole DNAT aggiuntive per ciascuna di esse.

Utilizzo delle reti

5

Per fornire un'infrastruttura di rete altamente flessibile e sicura in un ambiente cloud multifunzione, VMware Cloud Director utilizza un'architettura di rete a più livelli con quattro categorie di reti. Le categorie di reti sono reti esterne, reti di Virtual Data Center (VDC) dell'organizzazione, reti di gruppi di data center e reti di vApp. La maggior parte dei tipi di rete di VMware Cloud Director richiede oggetti di infrastruttura aggiuntivi, ad esempio gateway edge e pool di reti.

Reti esterne

Una rete esterna fornisce un'interfaccia di uplink che connette reti e macchine virtuali nell'ambiente di VMware Cloud Director a reti esterne, ad esempio una VPN, una intranet aziendale o Internet.

Una rete esterna è supportata da una singola rete di vSphere, da più reti di vSphere o da un router logico NSX-T Data Center di livello 0.

Solo un **amministratore di sistema** può creare una rete esterna. Per ulteriori informazioni sulle reti esterne, vedere *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*.

Pool di reti

Un pool di reti è una raccolta di segmenti di rete di livello 2 isolati che è possibile utilizzare per creare reti di vApp e determinati tipi di reti VDC dell'organizzazione su richiesta.

I pool di reti devono essere creati prima delle reti VDC dell'organizzazione e delle reti di vApp. Se non esistono, l'unica opzione di rete disponibile per un'organizzazione è la connessione diretta a una rete esterna.

Solo un **amministratore di sistema** può creare un pool di reti.

Per ulteriori informazioni sui pool di reti, vedere *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*.

Reti VDC dell'organizzazione

Le reti virtual data center (VDC) dell'organizzazione consentono alle vApp di comunicare tra loro o con reti esterne all'organizzazione.

A seconda della connessione della rete VDC dell'organizzazione a una rete esterna, sono disponibili diversi tipi di reti VDC dell'organizzazione.

Le reti VDC dell'organizzazione offrono connessioni dirette o instradate a reti esterne oppure possono essere isolate dalle reti esterne e dalle altre reti VDC dell'organizzazione. Le connessioni instradate richiedono un gateway edge e un pool di reti nel VDC dell'organizzazione.

Un **amministratore di sistema** o un **amministratore dell'organizzazione** crea reti VDC dell'organizzazione e le assegna all'organizzazione.

In un VDC dell'organizzazione appena creato non è disponibile alcuna rete. Dopo che un **amministratore di sistema** ha creato l'infrastruttura di rete richiesta, un **amministratore dell'organizzazione** può creare e gestire la maggior parte dei tipi di reti VDC dell'organizzazione.

Reti di gruppi di data center supportate da NSX Data Center for vSphere

Una rete supportata da NSX Data Center for vSphere che si estende a un gruppo di data center. Un gruppo di data center può includere da uno a sedici VDC dell'organizzazione in una distribuzione di VMware Cloud Director singola o multisito.

Reti di gruppi di data center supportate da NSX-T Data Center

Le reti di gruppi di data center sono un tipo di reti VDC dell'organizzazione condivise tra uno o più VDC, a cui le vApp possono connettersi.

Un **amministratore di sistema** o un **amministratore dell'organizzazione** crea reti di gruppi di data center e ne definisce l'ambito in un singolo gruppo di VDC.

VMware Cloud Director supporta reti di gruppi di data center isolate, importate, dirette e instradate supportate da NSX-T Data Center.

Reti di vApp

Le reti di vApp consentono alle macchine virtuali di comunicare tra loro oppure, collegandosi a una rete VDC dell'organizzazione, con le macchine virtuali di altre vApp.

Una rete di vApp è contenuta all'interno della vApp. Una rete di vApp può essere isolata da altre reti o connessa a una rete VDC dell'organizzazione.

Ogni vApp contiene una rete di vApp. La rete viene creata quando viene distribuita la vApp e viene eliminata quando la distribuzione della vApp viene annullata.

Un **amministratore dell'organizzazione** configura e controlla le reti di vApp.

Tipi di rete in una vApp

Le macchine virtuali in una vApp possono connettersi a reti di vApp, che possono essere isolate, dirette o instradate, nonché a reti VDC dell'organizzazione.

Nota I VDC dell'organizzazione supportati da NSX Data Center for vSphere sono compatibili con le reti di vApp instradate, isolate e dirette.

I VDC dell'organizzazione supportati da NSX-T Data Center sono compatibili con le reti di vApp isolate e dirette.

È possibile aggiungere reti di diversi tipi a una vApp per gestire più scenari di rete.

Le macchine virtuali nella vApp possono connettersi alle reti disponibili in una vApp. Se si desidera connettere una macchina virtuale a una rete diversa, è innanzitutto necessario aggiungere tale rete alla vApp.

Una vApp può includere reti di vApp e reti VDC dell'organizzazione. Una rete di vApp isolata è contenuta all'interno della vApp.

È inoltre possibile instradare una rete di vApp verso una rete VDC dell'organizzazione per fornire la connettività alle macchine virtuali esterne alla vApp. Per le reti di vApp instradate, è possibile configurare servizi di rete, ad esempio un firewall e il routing statico.

Una vApp può essere connessa direttamente a una rete VDC dell'organizzazione.

Se si dispone di più vApp che contengono macchine virtuali identiche connesse alla stessa rete VDC dell'organizzazione e si desidera avviare le vApp contemporaneamente, è possibile applicare la priorità alle vApp. In questo modo le macchine virtuali potranno essere attivate senza conflitti, isolando i relativi indirizzi MAC e IP.

Per informazioni, vedere [Gestione delle reti in una vApp](#).

Gateway edge

Un gateway Edge fornisce una rete VDC dell'organizzazione instradata con connettività a reti esterne e può fornire servizi come bilanciamento del carico, NAT e firewall. VMware Cloud Director supporta gateway edge IPv4 e IPv6.

I gateway edge richiedono NSX Data Center for vSphere o NSX-T Data Center.

Questo capitolo include i seguenti argomenti:

- [Gestione delle reti Virtual Data Center dell'organizzazione](#)
- [Gestione di reti di gruppi di data center con NSX-T Data Center](#)
- [Gestione di reti di gruppi di data center con NSX Data Center for vSphere](#)
- [Gestione dei servizi gateway edge NSX Data Center for vSphere](#)

■ Gestione dei gateway edge NSX-T Data Center

Gestione delle reti Virtual Data Center dell'organizzazione

Un **amministratore di sistema** o un **amministratore dell'organizzazione** crea reti VDC dell'organizzazione e le assegna al VDC dell'organizzazione o a un gruppo di VDC dell'organizzazione. Un **amministratore dell'organizzazione** può eseguire diverse attività, tra cui visualizzare informazioni sulle reti e configurare servizi di rete.

È possibile utilizzare reti VDC dell'organizzazione dirette, instradate, isolate o del gruppo di data center supportate da NSX Data Center for vSphere.

È possibile utilizzare reti VDC dell'organizzazione instradate, isolate e importate e dirette supportate da NSX-T Data Center. È possibile utilizzare anche reti di gruppi di data center instradate, isolate e importate supportate da NSX-T Data Center.

Tabella 5-1. Tipi di reti VDC dell'organizzazione

Rete di tipo data center	Descrizione
Diretta	<p>Una rete VDC dell'organizzazione con una connessione diretta a una delle reti esterne sottoposte a provisioning da parte dell'amministratore di sistema e supportate dalle risorse di vSphere.</p> <p>Le reti dirette sono supportate per i VDC dell'organizzazione supportati da NSX Data Center for vSphere e, a partire da VMware Cloud Director 10.2.2, per i VDC dell'organizzazione supportati da NSX-T Data Center.</p> <p>Le reti dirette sono accessibili da più VDC dell'organizzazione.</p> <p>Le macchine virtuali appartenenti a diversi VDC dell'organizzazione possono connettersi a questa rete e visualizzarne il traffico.</p> <p>Una rete diretta fornisce connettività di livello 2 diretta alle macchine virtuali esterne al VDC dell'organizzazione, che possono connettersi direttamente a quelle interne.</p> <hr/> <p>Nota Solo l'amministratore di sistema può aggiungere una rete VDC dell'organizzazione diretta.</p> <hr/> <p>Può essere IPv4 o IPv6.</p>
Isolata (interna)	<p>Le reti isolate sono accessibili solo dallo stesso VDC dell'organizzazione. Solo le macchine virtuali incluse in questo VDC dell'organizzazione possono connettersi alla rete interna del VDC dell'organizzazione e visualizzarne il traffico.</p> <p>Le reti isolate sono supportate per i VDC dell'organizzazione supportati da NSX-T Data Center e per NSX Data Center for vSphere del VDC dell'organizzazione.</p> <p>La rete isolata del VDC dell'organizzazione fornisce a un VDC dell'organizzazione una rete privata e isolata a cui possono connettersi più macchine virtuali e vApp. Inoltre, non offre connettività alle macchine virtuali esterne al VDC dell'organizzazione, che pertanto non possono connettersi a quelle interne.</p>
Instradata	<p>Le reti instradate sono accessibili solo dallo stesso VDC dell'organizzazione. Solo le macchine virtuali incluse nel VDC dell'organizzazione possono connettersi a tale rete.</p> <p>Questo tipo di rete fornisce anche accesso controllato a una rete esterna. Gli amministratori di sistema o l'amministratore dell'organizzazione possono configurare le impostazioni NAT (Network Address Translation), del firewall e VPN in modo da rendere determinate macchine virtuali accessibili dalla rete esterna.</p> <p>Può essere IPv4 o IPv6.</p>

Tabella 5-1. Tipi di reti VDC dell'organizzazione (continua)

Rete di tipo data center	Descrizione
Commutatore logico NSX-T Data Center importato	Le reti di NSX-T Data Center importate sono segmenti logici creati in NSX-T Data Center e utilizzano un commutatore logico NSX-T Data Center esistente. Vengono importate in un'organizzazione specifica come rete VDC dell'organizzazione. Nota Solo un amministratore di sistema può importare una rete di NSX-T Data Center.
Reti di gruppi di data center supportate da NSX Data Center for vSphere	Questa rete fa parte della rete di un gruppo di data center estesa a un gruppo di data center. Un gruppo di data center può includere da uno a sedici VDC dell'organizzazione in una distribuzione di VMware Cloud Director singola o multisito. Le macchine virtuali connesse a questa rete sono connesse alla rete estesa sottostante.
Reti di gruppi di data center supportate da NSX-T Data Center	Le reti di gruppi di data center sono un tipo di reti VDC dell'organizzazione supportate da NSX-T Data Center condivise tra uno o più VDC e a cui le vApp possono connettersi. Le reti di gruppi di data center possono essere isolate, importate o instradate e richiedono NSX-T Data Center.

Tutti i passaggi per gestire le reti VDC dell'organizzazione sono documentati supponendo che si disponga di un ambiente con più VDC.

Visualizzazione delle reti VDC dell'organizzazione disponibili

È possibile visualizzare le reti di virtual data center dell'organizzazione disponibili.

Prerequisiti

Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.

Procedura

- ◆ Nella barra di navigazione superiore, fare clic su **Rete**.

Risultati

Nella scheda **Reti**, viene visualizzato un elenco delle reti disponibili che è possibile filtrare in base a vari criteri.

Operazioni successive

È possibile aggiungere una rete VDC dell'organizzazione. È inoltre possibile modificare, aumentare l'ambito, eliminare o reimpostare una rete VDC dell'organizzazione esistente.

Aggiunta di una rete di virtual data center dell'organizzazione isolata

È possibile aggiungere una rete di VDC dell'organizzazione isolata, accessibile solo da questa organizzazione. Inoltre, non offre connettività alle macchine virtuali esterne all'organizzazione, che pertanto non possono connettersi a quelle interne.

È possibile aggiungere una combinazione di reti VDC dell'organizzazione isolate e instradate in modo da soddisfare le esigenze dell'organizzazione. Ad esempio, è possibile isolare una rete contenente informazioni riservate e creare una rete distinta associata a un gateway edge e connessa a Internet.

È possibile creare una rete di VDC isolata, supportata da un pool di reti. Il provider di servizi può anche creare una rete di VDC isolata supportata da un commutatore logico NSX-T.

È possibile creare solo una rete di VDC dell'organizzazione isolata IPv4.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Nella scheda **Reti**, fare clic su **Nuovo**.
- 3 Nella pagina **Ambito**, selezionare **Virtual data center dell'organizzazione**, selezionare un VDC in cui creare la rete e fare clic su **Avanti**.
- 4 Nella pagina **Seleziona tipo di rete**, selezionare **Isolata** e fare clic su **Avanti**.
- 5 Immettere un nome significativo per la rete.
- 6 Immettere le impostazioni CIDR (Classless Inter-Domain Routing) per la rete.
Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.
- 7 Immettere una descrizione della rete VDC dell'organizzazione.
- 8 (Facoltativo) Se il VDC in cui viene creata la rete è supportato da NSX Data Center for vSphere, attivare l'opzione **Condivisa** per rendere la rete VDC dell'organizzazione disponibile per gli altri VDC dell'organizzazione all'interno della stessa organizzazione.

Un possibile utilizzo di questa opzione si verifica quando un'applicazione è presente in un VDC dell'organizzazione che ha un pool di allocazioni o un pool di prenotazioni impostato come modello di allocazione. In questo caso, potrebbe non essere disponibile spazio sufficiente per l'esecuzione di più macchine virtuali. Per risolvere il problema è possibile creare un VDC dell'organizzazione secondario con Pay-As-You-Go ed eseguire temporaneamente più macchine virtuali in tale rete.

Nota I VDC dell'organizzazione devono essere supportati dallo stesso VDC del provider.

- 9 Fare clic su **Avanti**.

10 (Facoltativo) Per riservare uno o più indirizzi IP per l'assegnazione a macchine virtuali che richiedono indirizzi IP statici, configurare i **Pool IP statici** per la rete.

a Immettere l'indirizzo IP o l'intervallo di indirizzi IP e fare clic su **Aggiungi**.

Ripetere questo passaggio per aggiungere più indirizzi o intervalli di indirizzi IP statici.

b (Facoltativo) Per modificare o rimuovere gli indirizzi IP e gli intervalli di indirizzi IP, fare clic su **Modifica** o **Rimuovi**.

11 Fare clic su **Avanti**.

12 (Facoltativo) Configurare le impostazioni DNS.

Opzione	Azione
DNS primario	Immettere l'indirizzo IP del server DNS primario.
DNS secondario	Immettere l'indirizzo IP del server DNS secondario.
Suffisso DNS	Immettere il suffisso DNS. Il suffisso DNS è il nome DNS senza il nome host.

13 Fare clic su **Avanti**.

14 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Aggiunta di una rete di virtual data center dell'organizzazione instradata

Per controllare l'accesso a una rete esterna, è possibile aggiungere una rete VDC dell'organizzazione instradata. Gli **amministratori di sistema** e gli **amministratori dell'organizzazione** possono configurare le impostazioni NAT (Network Address Translation), del firewall e VPN in modo da rendere determinate macchine virtuali accessibili dalla rete esterna.

È possibile aggiungere una combinazione di reti VDC dell'organizzazione isolate o instradate in modo da soddisfare le esigenze dell'organizzazione. Ad esempio, è possibile aggiungere una rete associata a un gateway edge e connessa a Internet e creare una rete isolata che contiene informazioni riservate.

È possibile aggiungere una rete di VDC dell'organizzazione IPv4 o IPv6 instradata.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Rete**.

2 Nella scheda **Reti**, fare clic su **Nuovo**.

3 Nella pagina **Ambito**, selezionare **Virtual data center dell'organizzazione**, selezionare un VDC in cui creare la rete e fare clic su **Avanti**.

- 4 Nella pagina **Seleziona tipo di rete**, selezionare **Instradata** e fare clic su **Avanti**.

- 5 Immettere un nome significativo per la rete.

- 6 Immettere le impostazioni CIDR (Classless Inter-Domain Routing) per la rete.

Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.

- 7 Immettere una descrizione della rete VDC dell'organizzazione.

- 8 (Facoltativo) Se il VDC in cui viene creata la rete è supportato da NSX Data Center for vSphere, attivare l'opzione **Condivisa** per rendere la rete VDC dell'organizzazione disponibile per gli altri VDC dell'organizzazione all'interno della stessa organizzazione.

Un possibile utilizzo di questa opzione si verifica quando all'interno di un VDC dell'organizzazione è presente un'applicazione con un pool di allocazioni o un pool di prenotazioni impostato come modello di allocazione. In questo caso, potrebbe non essere disponibile spazio sufficiente per l'esecuzione di più macchine virtuali. Per risolvere il problema è possibile creare un VDC dell'organizzazione secondario con Pay-As-You-Go ed eseguire temporaneamente più macchine virtuali in tale rete.

Nota I VDC dell'organizzazione devono condividere lo stesso pool di reti.

- 9 Fare clic su **Avanti**.

- 10 Nella pagina **Connessione edge**, selezionare un gateway edge a cui associare la rete VDC dell'organizzazione.

Se il VDC dell'organizzazione include più gateway edge, è necessario selezionarne uno a cui connettere questa rete. Per supportare un'altra rete instradata, il gateway edge deve includere un valore almeno pari a 1 nella colonna N. reti disponibili.

- 11 Dal menu a discesa **Tipo di interfaccia**, selezionare il tipo di interfaccia.

Opzione	Descrizione
Interna	Si connette a una delle interfacce interne del gateway edge. Il numero massimo di reti consentite è 9.
Distribuito	Crea la rete in un router logico distribuito connesso al gateway edge. Il numero massimo di reti consentite è 400.
Interfaccia secondaria	Estende una rete VDC dell'organizzazione. VMware Cloud Director identifica la rete da utilizzare per l'estensione tramite VPN L2. VMware Cloud Director, grazie alla virtualizzazione della rete NSX, crea un tipo di interfaccia del trunk per questa rete. Il numero massimo di reti consentite è 200.

- 12 (Facoltativo) Per abilitare l'assegnazione di tag alle VLAN guest in questa rete, attivare l'opzione **VLAN guest consentita**.

- 13 Fare clic su **Avanti**.

14 (Facoltativo) Per riservare uno o più indirizzi IP per l'assegnazione a macchine virtuali che richiedono indirizzi IP statici, configurare i **Pool IP statici** per la rete.

a Immettere l'indirizzo IP o l'intervallo di indirizzi IP e fare clic su **Aggiungi**.

Ripetere questo passaggio per aggiungere più indirizzi o intervalli di indirizzi IP statici.

b (Facoltativo) Per modificare o rimuovere gli indirizzi IP e gli intervalli di indirizzi IP, fare clic su **Modifica** o **Rimuovi**.

15 Fare clic su **Avanti**.

16 (Facoltativo) Configurare le impostazioni DNS.

Opzione	Azione
DNS primario	Immettere l'indirizzo IP del server DNS primario.
DNS secondario	Immettere l'indirizzo IP del server DNS secondario.
Suffisso DNS	Immettere il suffisso DNS. Il suffisso DNS è il nome DNS senza il nome host.

17 Fare clic su **Avanti**.

18 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Aggiunta di una rete di virtual data center dell'organizzazione diretta

Per connettersi a una rete esterna tramite un route diretta, gli **amministratori di sistema** possono configurare una connessione diretta.

A partire da VMware Cloud Director 10.2.2, è supportata la creazione di reti dirette in VDC dell'organizzazione supportati da NSX-T Data Center e NSX Data Center for vSphere.

Se si accede al portale tenant di VMware Cloud Director come **amministratore dell'organizzazione** e si tenta di creare una rete di virtual data center dell'organizzazione diretta, viene visualizzato un messaggio che indica che non si dispone di diritti sufficienti.

Prerequisiti

Verificare di disporre dei diritti di **amministratore di sistema**.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Nella scheda **Reti**, fare clic su **Nuovo**.
- 3 Nella pagina **Ambito**, selezionare **Virtual data center dell'organizzazione**, selezionare un VDC in cui creare la rete e fare clic su **Avanti**.
- 4 Nella pagina **Tipo di rete**, selezionare **Diretta** e fare clic su **Avanti**.
- 5 Immettere un nome significativo per la rete.
- 6 Immettere una descrizione della rete VDC dell'organizzazione.

- 7 (Facoltativo) Per rendere la rete VDC dell'organizzazione disponibile per gli altri VDC all'interno della stessa organizzazione, attivare l'opzione **Condivisa**.
- 8 Nella pagina **Connessione di rete esterna**, selezionare la rete esterna a cui si desidera connettere direttamente la nuova rete di virtual data center dell'organizzazione e fare clic su **Avanti**.
- 9 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Aggiunta di una rete VDC dell'organizzazione con un commutatore logico NSX-T Data Center importato

Gli **Amministratori di sistema** possono creare una rete VDC dell'organizzazione importando un commutatore logico da un'istanza di NSX-T Manager associata.

Prerequisiti

- Verificare di disporre dei diritti di **amministratore di sistema**.
- Verificare che il virtual data center del provider che supporta il virtual data center dell'organizzazione di destinazione sia associato a un'istanza di NSX-T Manager.
- È necessario creare almeno un commutatore logico NSX-T non utilizzato dalle altre reti di virtual data center dell'organizzazione.

Per informazioni sulla creazione e sulla configurazione di commutatori logici NSX-T, vedere la *Guida per l'amministratore di NSX-T Data Center*.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Nella scheda **Reti**, fare clic su **Nuovo**.
- 3 Nella pagina **Ambito**, selezionare **Virtual data center dell'organizzazione**, selezionare un VDC in cui creare la rete e fare clic su **Avanti**.
- 4 Nella pagina **Tipo di rete**, selezionare **Importato** e poi **Commutatore logico NSX-T**, quindi fare clic su **Avanti**.
- 5 Nell'elenco dei commutatori logici NSX-T disponibili, selezionare il commutatore di destinazione e fare clic su **Avanti**.
- 6 Immettere un nome significativo per la rete.
- 7 Immettere le impostazioni CIDR (Classless Inter-Domain Routing) per la rete.
Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.
Se il commutatore è configurato con una subnet, le informazioni vengono prepopolate.
- 8 Immettere una descrizione della rete VDC dell'organizzazione.
- 9 Fare clic su **Avanti**.

10 (Facoltativo) Configurare le impostazioni DNS e il pool di IP statici.

È possibile aggiungere più indirizzi IP e intervalli di IP.

11 Fare clic su **Avanti**.

12 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Modifica delle impostazioni generali di una rete di virtual data center dell'organizzazione

È possibile modificare le proprietà delle reti VDC dell'organizzazione.

Prerequisiti

Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.

Procedura

- 1** Nella barra di navigazione superiore, fare clic su **Rete**.
- 2** Nella scheda **Reti**, fare clic sul nome della rete VDC dell'organizzazione che si desidera modificare.
- 3** Nella scheda **Generale**, fare clic su **Modifica**.
 - a** Modificare il nome e la descrizione della rete.
 - b** Se il VDC in cui viene creata la rete è supportato da NSX Data Center for vSphere, attivare o disattivare l'opzione **Condivisa** per rendere la rete VDC dell'organizzazione disponibile per gli altri VDC dell'organizzazione all'interno della stessa organizzazione.
- 4** Fare clic su **Salva**.

Connessione di una rete di virtual data center dell'organizzazione a un gateway edge

Dopo aver creato una rete VDC dell'organizzazione, è possibile connettere la rete a un gateway edge.

A partire dalla versione 10.1, VMware Cloud Director supporta la connessione a un gateway edge per le reti VDC dell'organizzazione supportate da NSX Data Center for vSphere o NSX-T Data Center.

Prerequisiti

Questa operazione richiede uno dei ruoli predefiniti di **amministratore dell'organizzazione** o **amministratore di sistema** oppure un ruolo dotato dei diritti **Rete VDC dell'organizzazione: Modifica proprietà** e **Gruppo di VDC: Visualizza** pubblicati nell'organizzazione.

Procedura

- 1** Nella barra di navigazione superiore, fare clic su **Rete**.

- 2 Fare clic sul nome della rete VDC dell'organizzazione che si desidera connettere a un gateway edge.
- 3 Nella scheda **Generale**, fare clic su **Modifica**.
- 4 Fare clic su **Connessione**.
- 5 Connettere la rete a un gateway edge.
 - a Attivare l'opzione **Connetti a un gateway edge**.
 - b Selezionare il gateway edge con cui stabilire la connessione nell'elenco dei gateway edge disponibili.
 - c Selezionare il tipo di interfaccia.
 - d Per consentire una VLAN guest, attivare l'opzione **VLAN guest consentita**.
- 6 Fare clic su **Salva**.

Risultati

La rete VDC dell'organizzazione si connette a un gateway edge e da isolata diventa instradata.

Disconnessione di una rete VDC dell'organizzazione da un gateway edge

Se si disconnette una rete VDC dell'organizzazione da un gateway edge, è possibile convertirla da instradata a isolata.

A partire dalla versione 10.1, la connessione a un gateway edge e la disconnessione da un gateway edge sono supportate per le reti VDC dell'organizzazione supportate da NSX Data Center for vSphere o NSX-T Data Center.

Prerequisiti

Questa operazione richiede uno dei ruoli predefiniti di **amministratore dell'organizzazione** o **amministratore di sistema** oppure un ruolo con il diritto **Rete VDC dell'organizzazione: Modifica proprietà**.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete VDC dell'organizzazione che si desidera disconnettere.
- 3 Nella scheda **Generale**, fare clic su **Modifica**.
- 4 Fare clic su **Connessione**.
- 5 Per disconnettere la rete dal gateway edge, disattivare l'opzione **Connetti a un gateway edge**.
- 6 Fare clic su **Salva**.

Risultati

La rete VDC dell'organizzazione è stata disconnessa da un gateway edge. La rete VDC dell'organizzazione è stata convertita da instradata a isolata.

Conversione dell'interfaccia di una rete VDC dell'organizzazione instradata

È possibile modificare l'interfaccia di una rete da interna a interfaccia secondaria o routing distribuito, ad esempio modificando le proprietà di rete.

Nota Le reti inter-VDC non possono essere convertite.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete VDC dell'organizzazione che si desidera modificare.
- 3 Nella scheda **Generale**, fare clic su **Modifica**.
- 4 Fare clic su **Connessione**.
- 5 Dal menu a discesa **Tipo di interfaccia**, selezionare il tipo di interfaccia.

Opzione	Descrizione
Interna	Si connette a una delle interfacce interne del gateway edge. Il numero massimo di reti consentite è 9.
Distribuito	Crea la rete in un router logico distribuito connesso al gateway edge. Il numero massimo di reti consentite è 400.
Interfaccia secondaria	Estende una rete VDC dell'organizzazione. VMware Cloud Director identifica la rete da utilizzare per l'estensione tramite VPN L2. VMware Cloud Director, grazie alla virtualizzazione della rete NSX, crea un tipo di interfaccia del trunk per questa rete. Il numero massimo di reti consentite è 200.

- 6 Fare clic su **Salva**.

Visualizzazione degli indirizzi IP utilizzati per la rete di virtual data center dell'organizzazione

È possibile visualizzare un elenco degli indirizzi IP del pool di IP della rete del virtual data center dell'organizzazione attualmente in uso.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare che la rete sia una rete di virtual data center dell'organizzazione isolata o instradata.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete di cui si desidera visualizzare gli indirizzi IP utilizzati.
- 3 Nella sezione **Gestione IP**, fare clic su **Utilizzo IP** per verificare quali indirizzi IP sono attualmente in uso.

Aggiunta di indirizzi IP al pool di IP di una rete di virtual data center dell'organizzazione

Se una rete di virtual data center dell'organizzazione sta esaurendo gli indirizzi IP, è possibile aggiungerne altri al pool di IP.

Non è possibile aggiungere indirizzi IP alle reti esterne di virtual data center dell'organizzazione che hanno una connessione diretta.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare che la rete sia una rete di virtual data center dell'organizzazione isolata o instradata.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete che si desidera modificare.
- 3 Nella sezione **Gestione IP**, fare clic sulla scheda **Pool di IP statici**.
- 4 Fare clic sul pulsante **Modifica** a destra.

Nella finestra **Modifica rete** sono visualizzati il CIDR del gateway e gli intervalli di indirizzi IP, se presenti.

- 5 Nella casella di testo **Pool IP statici**, immettere l'indirizzo IP o l'intervallo di indirizzi IP e fare clic su **Aggiungi**.

Nota Per le reti inter-VDC, gli indirizzi IP non devono sovrapporsi agli indirizzi IP assegnati alle altre reti VDC dell'organizzazione presenti nella stessa rete estesa.

- 6 Fare clic su **Salva**.

Risultati

L'indirizzo IP o l'intervallo di indirizzi IP viene aggiunto al pool di IP della rete.

Modifica o rimozione di intervalli IP utilizzati in una rete di virtual data center dell'organizzazione

Se una rete di virtual data center dell'organizzazione contiene indirizzi IP non più necessari, è possibile modificare gli indirizzi o eliminarli dal pool di IP.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare che la rete sia una rete di virtual data center dell'organizzazione isolata o instradata.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete che si desidera modificare.
- 3 Nella sezione **Gestione IP**, fare clic su **Pool di IP statici**.
- 4 Fare clic sul pulsante **Modifica** a destra.
 - Per modificare un intervallo di indirizzi IP, selezionare l'intervallo, apportare le modifiche necessarie e fare clic su **Modifica**.
 - Per rimuovere un intervallo di indirizzi IP, selezionare l'intervallo e fare clic su **Rimuovi**.
- 5 Fare clic su **Salva**.

Modifica delle impostazioni DNS di una rete di virtual data center dell'organizzazione

È possibile modificare le impostazioni DNS di una rete di virtual data center dell'organizzazione.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare che la rete sia una rete di virtual data center dell'organizzazione isolata o instradata.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete che si desidera modificare.
- 3 Nella sezione **Gestione IP**, fare clic su **DNS**.
- 4 Fare clic sul pulsante **Modifica** a destra.

- 5 Se necessario, modificare le informazioni relative a DNS primario, DNS secondario e suffisso DNS.
- 6 Fare clic su **Salva**.

Configurazione delle impostazioni DHCP per una rete di virtual data center dell'organizzazione isolata

È possibile modificare le impostazioni DHCP di una rete VDC dell'organizzazione isolata supportata da NSX Data Center for vSphere. Il servizio DHCP di una rete di VDC dell'organizzazione fornisce indirizzi IP dal rispettivo pool di indirizzi alle NIC delle macchine virtuali configurate per richiedere un indirizzo dal DHCP. Il servizio fornisce l'indirizzo quando la macchina virtuale viene accesa.

A partire dalla versione 10.2, VMware Cloud Director supporta le impostazioni DHCP per IPv4 e IPv6. È possibile configurare le impostazioni IPv6 utilizzando l'API VMware Cloud Director.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare che la rete sia una rete di virtual data center dell'organizzazione isolata.
- Verificare che la rete sia supportata da NSX Data Center for vSphere.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete che si desidera modificare.
- 3 Nella sezione **Gestione IP**, fare clic su **DHCP**.
- 4 Per abilitare DHCP, fare clic su **Modifica** a destra di **Servizio Pool DHCP**.
- 5 Attivare il **Servizio Pool DHCP** e fare clic su **Salva**.

Gli indirizzi richiesti dai client DHCP vengono recuperati da un pool DHCP.

- 6 Creare un pool DHCP per la rete.
 - a Fare clic su **Nuovo**.
 - b Specificare un intervallo di indirizzi IP per il pool.
L'intervallo di indirizzi IP specificato non può sovrapporsi al pool di indirizzi IP statici per il virtual data center dell'organizzazione.
 - c Specificare la durata predefinita dei lease per gli indirizzi DHCP espressa in secondi.
Il valore predefinito è 3.600 secondi.
 - d Specificare la durata massima dei lease per gli indirizzi DHCP espressa in secondi.
Questo è il periodo di tempo massimo per cui vengono concessi gli indirizzi IP assegnati da DHCP alle macchine virtuali. Il valore predefinito è 7.200 secondi.

7 Fare clic su **Salva**.

Aggiunta di un pool DHCP a una rete di virtual data center dell'organizzazione instradata supportata da NSX-T Data Center

È possibile aggiungere pool DHCP a una rete VDC dell'organizzazione instradata supportata da NSX-T Data Center.

Nota L'eliminazione o l'aggiornamento dei pool DHCP non è supportato per le reti VDC dell'organizzazione supportate da NSX-T Data Center.

Prerequisiti

- Queste operazioni richiedono i ruoli predefiniti di **amministratore dell'organizzazione** o **amministratore di sistema** oppure un ruolo che includa un set di diritti equivalente.
- Verificare che la rete sia una rete di virtual data center dell'organizzazione instradata.
- Verificare che la rete sia supportata da NSX-T Data Center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete che si desidera modificare.
- 3 Nella sezione **Gestione IP**, fare clic su DHCP.
- 4 Per aggiungere un pool DHCP, fare clic su **Nuovo**.
- 5 Specificare un intervallo di indirizzi IPv4 per il pool.
- 6 Fare clic su **Salva**.

Modifica o eliminazione di un pool DHCP esistente per una rete di virtual data center dell'organizzazione isolata supportata da NSX Data Center for vSphere

Se un pool DHCP all'interno della rete di virtual data center dell'organizzazione isolata non è più necessario, è possibile eliminare il pool supportato da NSX Data Center for vSphere oppure modificarlo.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare che la rete sia una rete di virtual data center dell'organizzazione isolata.
- Verificare che la rete di virtual data center dell'organizzazione sia supportata da NSX Data Center for vSphere.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul nome della rete che si desidera modificare.
- 3 Fare clic sulla sezione **Gestione IP**, quindi fare clic su **DHCP**.
- 4 Modificare o eliminare un pool DHCP esistente.

Opzione	Azione
Modificare un pool DHCP.	<ol style="list-style-type: none"> 1 Selezionare il pool DHCP che si desidera modificare. 2 Fare clic sul pulsante Modifica. 3 Aggiornare l'intervallo di indirizzi IP per il pool. 4 Modificare la durata predefinita dei lease per gli indirizzi DHCP espressa in secondi. 5 Modificare la durata massima dei lease per gli indirizzi DHCP espressa in secondi. 6 Fare clic su Salva.
Eliminare un pool DHCP.	<ol style="list-style-type: none"> 1 Selezionare il pool DHCP che si desidera eliminare. 2 Fare clic sul pulsante Elimina.

Reimpostazione di una rete di virtual data center dell'organizzazione

Se i servizi di rete, ad esempio le impostazioni DHCP o le impostazioni del firewall associate a una rete di virtual data center dell'organizzazione, non funzionano nel modo previsto, è possibile reimpostare la rete.

Quando si reimposta la rete di virtual data center dell'organizzazione, si forza la ridistribuzione del gateway del servizio DHCP della rete. Questa operazione comporta un'interruzione temporanea dei servizi DHCP e durante la reimpostazione della rete non è disponibile alcun servizio di rete.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- La rete non è connessa ad alcuna macchina virtuale, vApp o altra rete.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Selezionare una rete VDC dell'organizzazione.
- 3 Fare clic su **Reimposta** e confermare l'operazione di reimpostazione.

Eliminazione di una rete di virtual data center dell'organizzazione

Se una rete di virtual data center dell'organizzazione non è più necessaria, è possibile eliminarla.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

- La rete non è connessa a macchine virtuali, vApp o altre reti.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul pulsante di opzione accanto al nome della rete di destinazione e fare clic su **Elimina**.
- 3 Per confermare, fare clic su **OK**.

Gestione di reti di gruppi di data center con NSX-T Data Center

A partire dalla versione 10.2, VMware Cloud Director supporta le reti di gruppi di data center supportate da NSX-T Data Center.

Per creare una rete di più VDC dell'organizzazione, è innanzitutto necessario raggruppare i VDC e quindi creare una rete di gruppi condivisi con tali VDC.

Le reti di gruppi di data center supportate da NSX-T Data Center forniscono la condivisione di rete di livello 2, la configurazione del punto di uscita singolo attivo e le regole DFW (firewall distribuito) che vengono applicate a un gruppo di data center.

Gruppo di data center

Un gruppo di data center funge da router inter-VDC che fornisce amministrazione di rete centralizzata, configurazione del punto di uscita e traffico est-ovest fra tutte le reti all'interno del gruppo. Un gruppo di data center può contenere da uno a sedici VDC configurati per la condivisione di un punto di uscita attivo.

Zona di disponibilità

Una zona di disponibilità rappresenta i cluster di elaborazione o i domini di errore di elaborazione che sono disponibili per la rete. Per impostazione predefinita, la zona di disponibilità è il VDC del provider.

Importante L'**amministratore di sistema** deve configurare le zone di disponibilità per le reti dei gruppi con NSX-T Data Center impostando un valore **Calcola ambito del provider** per l'istanza di vCenter Server e, facoltativamente, per i VDC del provider supportati dall'istanza di vCenter Server. Per impostazione predefinita, l'ambito del provider di elaborazione di un VDC del provider viene copiato dall'istanza di vCenter Server che esegue il backup di questo VDC. Un **amministratore di sistema** può differenziare l'ambito del provider di elaborazione per i vari VDC del provider supportati da un'istanza di vCenter Server singola. Ad esempio, è possibile disporre di un'istanza di vCenter Server con un ambito **Germany** e un VDC del provider con un ambito **Munich**.

L'**amministratore di sistema** può inoltre riconfigurare la zona di disponibilità come l'ambito del provider di rete, che in genere rappresenta l'istanza di vCenter Server sottostante con l'NSX-T Manager associato.

Punto di uscita

Un gateway edge NSX-T Data Center esistente configurato per connettere un gruppo di data center a una rete esterna.

Rete del gruppo di data center

Una rete di livello 2 che viene condivisa tra tutti i VDC in un gruppo di data center.

Gestione dei gruppi di data center con un tipo di provider di rete NSX-T Data Center

Dopo aver creato un gruppo di data center con un tipo di provider di rete NSX-T Data Center, è possibile aggiungere data center al gruppo, rimuoverli e modificare le impostazioni del gruppo.

Un gruppo di data center può includere fino a sedici virtual data center.

I VDC rimossi dal gruppo di data center non devono disporre di carichi di lavoro collegati a nessuna delle reti che partecipano al gruppo di data center.

Creazione di un gruppo di data center con un tipo di provider di rete NSX-T Data Center

È possibile raggruppare da uno a sedici VDC in un gruppo di data center con tipo di provider di rete NSX-T Data Center.

Prerequisiti

Verificare di essere un **amministratore dell'organizzazione**, un **amministratore di sistema** o di disporre di un ruolo che includa un insieme di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
- 2 Fare clic su **Nuovo**.
- 3 Nella pagina **VDC di avvio**, selezionare un VDC supportato da NSX-T Data Center per avviare il gruppo.
- 4 Immettere un nome e, facoltativamente, una descrizione per il nuovo gruppo di data center.
- 5 Nella pagina **VDC partecipanti**, selezionare i data center aggiuntivi per il nuovo gruppo di data center e fare clic su **Avanti**.
- 6 Rivedere i dettagli del gruppo di data center e fare clic su **Fine**.

Risultati

Il gruppo appena creato viene visualizzato nell'elenco dei gruppi di data center.

Operazioni successive

Creare una rete per il gruppo di data center con un tipo di provider di rete NSX-T Data Center.

Visualizzazione e modifica delle impostazioni generali di un gruppo di data center con un tipo di provider di rete NSX-T Data Center

È possibile visualizzare e modificare i gruppi di data center con un tipo di provider di rete NSX-T Data Center nell'organizzazione.

Prerequisiti

Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo con un insieme di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.
- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Nel riquadro **Impostazioni generali**, fare clic su **Modifica**.
- 4 Modificare il nome e, facoltativamente, la descrizione del gruppo di data center, quindi fare clic su **Salva** per confermare.

Gestione dei VDC partecipanti in un gruppo di data center

È possibile selezionare quali VDC devono far parte di un gruppo di VDC e comunicare tra loro.

Prerequisiti

Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo con un insieme di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.
- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Fare clic su **VDC partecipanti**, quindi fare clic su **Gestisci**.
- 4 Selezionare i VDC che si desidera includere nel gruppo e fare clic su **Salva** per confermare.

Sincronizzazione di un gruppo di data center con un tipo di provider di rete NSX-T Data Center

Per verificare che tutti i VDC che partecipano a un gruppo di data center siano ancora presenti e siano configurati correttamente, è possibile sincronizzare il gruppo di data center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Fare clic **Sincronizza** e confermare.

Utilizzo del firewall distribuito in un gruppo di data center con un tipo di provider di rete NSX-T Data Center

A partire dalla versione 10.2, VMware Cloud Director supporta un servizio firewall distribuito per i gruppi di data center con il tipo di provider di rete NSX-T Data Center.

Quando si abilita un firewall distribuito per un gruppo di data center con il tipo di provider di rete NSX-T Data Center, si crea un singolo criterio di sicurezza predefinito che viene applicato al gruppo di data center.

In qualità di **amministratore dell'organizzazione**, è possibile creare e modificare le regole del firewall distribuito aggiuntive che sono associate al criterio di protezione predefinito del gruppo di data center.

Il servizio firewall distribuito non è abilitato per impostazione predefinita. Dopo l'abilitazione del firewall distribuito, è possibile creare set di IP e gruppi di sicurezza per semplificare la creazione delle regole del firewall distribuito.

Nota Le regole del firewall distribuito create si applicano solo ai carichi di lavoro collegati alle reti dei gruppi di data center.

Attivazione del firewall distribuito per un gruppo di data center con un tipo di provider di rete NSX-T Data Center

Utilizzando un firewall distribuito, è possibile applicare un set di regole del firewall di livello 3 in un singolo gruppo di data center.

Il firewall distribuito non è abilitato per impostazione predefinita. Quando viene abilitato, si crea un unico criterio di sicurezza predefinito.

Prerequisiti

Assicurarsi di essere un **amministratore di sistema**.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Nella sezione **Firewall distribuito**, fare clic su **Attiva** e confermare che si desidera attivare il firewall distribuito.

Operazioni successive

Creare le regole del firewall distribuito.

Aggiunta di un set di IP a un gruppo di data center

Per creare regole del firewall distribuito e aggiungerle a un gruppo di data center, è innanzitutto necessario creare set di IP. I set di IP sono gruppi di indirizzi IP e reti a cui si applicano le regole del firewall distribuito. La combinazione di più oggetti in set di IP consente di ridurre il numero totale di regole del firewall distribuito da creare.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.
- 3 In Sicurezza, fare clic su **Set di IP**.
- 4 Fare clic su **Nuovo**.
- 5 Immettere un nome significativo e, facoltativamente, una descrizione per il nuovo set di IP.
- 6 Immettere un indirizzo IPv4, un indirizzo IPv6 o un intervallo di indirizzi in un formato CIDR, quindi fare clic su **Aggiungi**.
- 7 Per modificare un indirizzo IP o un intervallo di indirizzi IP esistente, fare clic su **Modifica** e modificare il valore.
- 8 Per confermare, fare clic su **Salva**.

Creazione di un gruppo di sicurezza in un gruppo di data center con un tipo di provider di rete NSX-T Data Center

Prima di creare regole del firewall distribuito per un gruppo di data center, è possibile raggruppare le reti di gruppi di data center in gruppi di sicurezza a cui applicare le regole.

I gruppi di sicurezza sono gruppi di reti di gruppi di data center a cui si applicano le regole del firewall distribuito. Il raggruppamento di reti consente di ridurre il numero totale di regole del firewall distribuito da creare.

Prerequisiti

Verificare di disporre di almeno una rete di gruppi di data center supportata da NSX-T Data Center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.
- 3 In Sicurezza, fare clic su **Gruppi di sicurezza**, quindi fare clic su **Nuovo**.
- 4 Digitare un nome e, facoltativamente, una descrizione per il gruppo di sicurezza, quindi fare clic su **Salva**.

Il nuovo gruppo di sicurezza viene visualizzato nell'elenco.

- 5 Selezionare il gruppo di sicurezza appena creato e fare clic su **Gestisci membri**.
- 6 Selezionare le reti del gruppo di data center da aggiungere al gruppo di sicurezza.
- 7 Fare clic su **Salva**.

Operazioni successive

[Aggiunta di una regola del firewall distribuito a un gruppo di data center con un tipo di provider di rete NSX-T Data Center](#)

Aggiunta di un profilo delle porte dell'applicazione a un gruppo di data center

Per creare regole del firewall distribuito, è possibile utilizzare profili delle porte dell'applicazione preconfigurati e profili delle porte dell'applicazione personalizzati.

I profili delle porte dell'applicazione includono una combinazione di un protocollo e una porta o un gruppo di porte, che vengono utilizzati per i servizi firewall. Oltre ai profili delle porte predefiniti preconfigurati, è possibile creare profili delle porte dell'applicazione personalizzati.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.
- 3 In Sicurezza, fare clic su **Profili porte applicazione**.
- 4 Nel riquadro **Applicazioni personalizzate**, fare clic su **Nuova**.
- 5 Immettere un nome e, facoltativamente, una descrizione per il profilo della porta dell'applicazione.

- 6 Nel menu a discesa **Protocollo**, selezionare il protocollo.
- 7 Immettere una porta, o un intervallo di porte separate da virgole, e fare clic su **Salva**.
- 8 Ripetere i passaggi per configurare altri profili di porta.

Operazioni successive

Utilizzare i profili delle porte dell'applicazione per creare le regole del firewall distribuito.

Aggiunta di una regola del firewall distribuito a un gruppo di data center con un tipo di provider di rete NSX-T Data Center

Le regole del firewall distribuito create si applicano solo ai carichi di lavoro collegati alle reti dei gruppi di data center.

Prerequisiti

Verificare che il servizio firewall distribuito per il gruppo di data center sia abilitato.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.
- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Fare clic sulla scheda **Firewall distribuito** a sinistra.
- 4 Fare clic su **Modifica regole**.
- 5 Per aggiungere una regola del firewall, fare clic su **Nuova in cima**.
- 6 Configurare la regola.

Opzione	Descrizione
Nome	Immettere un nome per la regola.
Stato	Per abilitare la regola al momento della creazione, attivare l'opzione Stato .
Applicazioni	(Opzionale) Per selezionare un profilo di porta specifico a cui applicare la regola, attivare l'interruttore Applicazioni e fare clic su Salva .
Contesto	(Facoltativo) Selezionare un profilo del contesto NSX-T Data Center per la regola.
Origine	Selezionare il traffico di origine e fare clic su Mantieni . <ul style="list-style-type: none"> ■ Per consentire o impedire il traffico da qualsiasi indirizzo di origine, attivare Qualsiasi origine. ■ Per consentire o impedire il traffico da set di IP o gruppi di sicurezza specifici, selezionare i set di IP e i gruppi di sicurezza dall'elenco.

Opzione	Descrizione
Destinazione	<p>Selezionare il traffico di destinazione e fare clic su Mantieni.</p> <ul style="list-style-type: none"> ■ Per consentire o negare il traffico verso qualsiasi indirizzo di destinazione, attivare Qualsiasi destinazione. ■ Per consentire o impedire il traffico verso set di IP o gruppi di sicurezza specifici, selezionare i set di IP e i gruppi di sicurezza dall'elenco.
Azione	<p>Dal menu a discesa Azione, selezionare se consentire o negare il traffico da o verso origini specifiche.</p> <ul style="list-style-type: none"> ■ Selezionare Accetta per consentire il traffico da o verso le origini, le destinazioni e i servizi specificati. ■ Selezionare Nega per bloccare il traffico da o verso le origini, le destinazioni e i servizi specificati.
Protocollo IP	Selezionare se applicare la regola al traffico IPv4 o IPv6.
Abilita registrazione.	Per registrare la conversione degli indirizzi da parte di questa regola, attivare l'interruttore Abilita registrazione .

7 Fare clic su **Salva**.

8 Per configurare regole aggiuntive, ripetere i passaggi.

Risultati

Dopo che sono state create, le regole del firewall vengono visualizzate nell'elenco delle regole del firewall distribuite. È possibile spostare verso l'alto o verso il basso, modificare o eliminare le regole in base alle proprie esigenze.

Disattivazione del criterio del firewall distribuito predefinito

Se si desidera disattivare il servizio firewall distribuito, è innanzitutto necessario disattivare il criterio del firewall distribuito predefinito.

Quando si disattiva il criterio predefinito, è possibile modificare le regole del firewall distribuito, ma tali regole non vengono più applicate.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.
- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Fare clic sulla scheda **Firewall distribuito** a sinistra.
- 4 Nella scheda **Criterio predefinito** sopra l'elenco delle regole del firewall distribuito, fare clic su **Disabilita** e confermare l'azione.

Risultati

Il criterio predefinito viene disattivato. Le altre regole del firewall distribuito possono essere modificate, ma non vengono applicate.

Disattivazione del servizio firewall distribuito

Se non si desidera utilizzare il servizio firewall distribuito, è possibile disattivarlo.

Quando si disattiva il servizio firewall distribuito per un gruppo di data center, la configurazione delle regole di sicurezza per questo gruppo viene eliminata in modo permanente e non può essere recuperata.

Prerequisiti

[Disattivazione del criterio del firewall distribuito predefinito](#)

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.
- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Fare clic su **Generale**.
- 4 Nel riquadro **Firewall distribuito** a destra, fare clic su **Disattiva** e confermare l'azione.

Risultati

Il servizio firewall distribuito è disattivato e la configurazione delle regole di sicurezza viene eliminata.

Gestione delle reti del gruppo di data center con un tipo di provider di rete NSX-T Data Center

Dopo aver creato e configurato un gruppo di data center, è possibile creare e gestire reti del gruppo di data center estese ai VDC partecipanti.

È possibile utilizzare reti del gruppo di data center dell'organizzazione instradate, isolate e importate supportate da NSX-T Data Center.

Una rete del gruppo di data center può avere come ambito solo un singolo gruppo di data center.

È possibile aumentare l'ambito di una rete esistente da un VDC dell'organizzazione a un gruppo di data center.

È possibile aggiungere tutti i tipi di reti a un gruppo di data center.

Importante Gli indirizzi IP nelle reti che partecipano a un gruppo di data center non devono sovrapporsi, anche se le reti sono isolate.

Tabella 5-2. Tipi di reti del gruppo di data center

Tipo di rete del gruppo di data center	Descrizione
Isolata	Una rete del gruppo di data center isolata è accessibile solo dai VDC dello stesso gruppo di data center. Solo le macchine virtuali del gruppo di data center possono connettersi alla rete del gruppo di data center isolata e visualizzarne il traffico.
Instradata	Una rete del gruppo di data center instradata fornisce l'accesso controllato a una rete esterna tramite un gateway edge NSX-T Data Center che fa parte del gruppo di data center.
Importata	Una rete del gruppo di data center importata utilizza un commutatore logico di NSX-T Data Center esistente. Solo un amministratore di sistema può importare una rete.

Creazione di una rete di gruppi di data center isolati supportata da un NSX-T Data Center

È possibile aggiungere una rete di gruppi di data center isolati, accessibile solo alle macchine virtuali nel gruppo di data center. Le macchine virtuali esterne a questa rete non hanno alcuna connettività a questa, indipendentemente dal fatto che siano connesse ad altre reti nello stesso gruppo di data center.

Prerequisiti

- Assicurarsi di essere un **amministratore dell'organizzazione**.
- Assicurarsi di aver creato un gruppo di data center con un tipo di provider di rete NSX-T Data Center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Nella scheda **Reti**, fare clic su **Nuovo**.
- 3 Nella pagina **Ambito**, selezionare **Gruppo di data center** e selezionare un gruppo con il provider di rete NSX-T Data Center in cui si desidera creare la rete.
- 4 Nella pagina **Tipo di rete**, selezionare **Isolata** e fare clic su **Avanti**.
- 5 Immettere un nome significativo per la rete.
- 6 Immettere le impostazioni CIDR (Classless Inter-Domain Routing) per la rete.
Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.
- 7 Immettere una descrizione della rete VDC dell'organizzazione.
- 8 Fare clic su **Avanti**.

- 9 (Facoltativo) Per riservare uno o più indirizzi IP per l'assegnazione a macchine virtuali che richiedono indirizzi IP statici, configurare i **Pool IP statici** per la rete.
- Immettere l'indirizzo IP o l'intervallo di indirizzi IP e fare clic su **Aggiungi**.
Ripetere questo passaggio per aggiungere più indirizzi o intervalli di indirizzi IP statici.
 - (Facoltativo) Per modificare o rimuovere gli indirizzi IP e gli intervalli di indirizzi IP, fare clic su **Modifica** o **Rimuovi**.
- 10 (Facoltativo) Configurare le impostazioni DNS.

Opzione	Azione
DNS primario	Immettere l'indirizzo IP del server DNS primario.
DNS secondario	Immettere l'indirizzo IP del server DNS secondario.
Suffisso DNS	Immettere il suffisso DNS. Il suffisso DNS è il nome DNS senza il nome host.

- 11 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Creazione di una rete di gruppi di data center instradata supportata da NSX-T Data Center

Per controllare l'accesso a una rete esterna, è possibile aggiungere una rete di gruppi di data center instradata.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo con un insieme di diritti equivalente.
- Assicurarsi di aver creato un gruppo di data center con un tipo di provider di rete NSX-T Data Center.
- Assicurarsi di aver impostato come ambito di un gateway edge NSX-T Data Center esistente il gruppo di data center in cui si desidera creare una rete instradata.

Procedura

- Nella barra di navigazione superiore, fare clic su **Rete**.
- Nella scheda **Reti**, fare clic su **Nuovo**.
- Nella pagina **Ambito**, selezionare **Gruppo di data center** e selezionare un gruppo con il provider di rete NSX-T Data Center in cui si desidera creare la rete.
- Nella pagina **Tipo di rete**, selezionare **Instradata** e fare clic su **Avanti**.
Se è presente un solo gateway edge che ha come ambito il gruppo di data center, questo viene automaticamente assegnato alla rete.
- Se sono presenti più NSX-T Data Center disponibili per il gruppo di data center, selezionare un gateway edge dall'elenco e fare clic su **Avanti**.

- 6 Immettere un nome significativo per la rete.
- 7 Immettere le impostazioni CIDR (Classless Inter-Domain Routing) per la rete.
Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.
- 8 Immettere una descrizione della rete VDC dell'organizzazione.
- 9 Fare clic su **Avanti**.
- 10 (Facoltativo) Per riservare uno o più indirizzi IP per l'assegnazione a macchine virtuali che richiedono indirizzi IP statici, configurare i **Pool IP statici** per la rete.
 - a Immettere l'indirizzo IP o l'intervallo di indirizzi IP e fare clic su **Aggiungi**.
Ripetere questo passaggio per aggiungere più indirizzi o intervalli di indirizzi IP statici.
 - b (Facoltativo) Per modificare o rimuovere gli indirizzi IP e gli intervalli di indirizzi IP, fare clic su **Modifica** o **Rimuovi**.
- 11 (Facoltativo) Configurare le impostazioni DNS.

Opzione	Azione
DNS primario	Immettere l'indirizzo IP del server DNS primario.
DNS secondario	Immettere l'indirizzo IP del server DNS secondario.
Suffisso DNS	Immettere il suffisso DNS. Il suffisso DNS è il nome DNS senza il nome host.

- 12 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Creazione di una rete dei gruppi di data center con un commutatore logico NSX-T importato

Gli **amministratori di sistema** possono creare una rete VDC dell'organizzazione importando un segmento da un'istanza di NSX-T Manager associata.

Prerequisiti

- Assicurarsi di essere un **amministratore di sistema**.
- Assicurarsi di aver creato un gruppo di data center con un tipo di provider di rete NSX-T Data Center.
- Verificare che il virtual data center del provider che supporta il gruppo di virtual data center di destinazione sia associato a un'istanza di NSX-T Manager.
- Assicurarsi di aver creato almeno un commutatore logico NSX-T non utilizzato da altre reti.
Per informazioni sulla creazione e sulla configurazione di commutatori logici NSX-T, vedere la *Guida per l'amministratore di NSX-T Data Center*.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.

- 2 Nella scheda **Reti**, fare clic su **Nuovo**.
- 3 Nella pagina **Ambito**, selezionare **Gruppo di data center** e selezionare un gruppo con il provider di rete NSX-T Data Center in cui si desidera creare la rete.
- 4 Nella pagina **Tipo di rete**, selezionare **Importato** e fare clic su **Avanti**.
- 5 Nell'elenco dei commutatori logici NSX-T disponibili selezionare il commutatore di destinazione e fare clic su **Avanti**.
- 6 Immettere un nome significativo per la rete.
- 7 Immettere le impostazioni CIDR (Classless Inter-Domain Routing) per la rete.
Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.
- 8 Immettere una descrizione della rete VDC dell'organizzazione.
- 9 Fare clic su **Avanti**.
- 10 (Facoltativo) Per riservare uno o più indirizzi IP per l'assegnazione a macchine virtuali che richiedono indirizzi IP statici, configurare i **Pool IP statici** per la rete.
 - a Immettere l'indirizzo IP o l'intervallo di indirizzi IP e fare clic su **Aggiungi**.
Ripetere questo passaggio per aggiungere più indirizzi o intervalli di indirizzi IP statici.
 - b (Facoltativo) Per modificare o rimuovere gli indirizzi IP e gli intervalli di indirizzi IP, fare clic su **Modifica** o **Rimuovi**.
- 11 (Facoltativo) Configurare le impostazioni DNS.

Opzione	Azione
DNS primario	Immettere l'indirizzo IP del server DNS primario.
DNS secondario	Immettere l'indirizzo IP del server DNS secondario.
Suffisso DNS	Immettere il suffisso DNS. Il suffisso DNS è il nome DNS senza il nome host.

- 12 Nella pagina **Pronto per il completamento**, controllare le impostazioni e fare clic su **Fine**.

Aumento dell'ambito di una rete VDC dell'organizzazione supportata da NSX-T Data Center

Dopo aver aumentato l'ambito di una rete VDC dell'organizzazione in una rete di gruppi di data center, è possibile connettere i carichi di lavoro di tutti i data center che partecipano al gruppo di data center.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo con un insieme di diritti equivalente.

- Assicurarsi di aver creato un gruppo di data center con un tipo di provider di rete NSX-T Data Center.
- Assicurarsi che sia stata creata una rete VDC dell'organizzazione supportata da NSX-T Data Center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul pulsante di opzione accanto alla rete VDC dell'organizzazione di cui si desidera aumentare l'ambito e fare clic su **Aumenta ambito**.
- 3 Selezionare un gruppo di data center dall'elenco dei gruppi di data center e fare clic su **OK** per confermare.

Risultati

L'ambito della rete viene aumentato a una rete di gruppi di data center. Nell'elenco delle reti, viene elencato come ambito del gruppo di data center selezionato.

Riduzione dell'ambito di una rete di gruppi di data center supportata da NSX-T Data Center

È possibile ridurre l'ambito di una rete di gruppi di data center supportata da NSX-T Data Center a una rete VDC dell'organizzazione.

Se si riduce l'ambito di una rete di gruppi di data center a una singola rete VDC dell'organizzazione, è necessario fornire connettività di rete ai carichi di lavoro che appartengono solo al VDC dell'organizzazione.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo con un insieme di diritti equivalente.
- Assicurarsi di aver creato una rete VDC con ambito definito in un gruppo di data center con tipo di provider di rete NSX-T Data Center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sul pulsante di opzione accanto alla rete del gruppo di data center di cui si desidera ridurre l'ambito e fare clic su **Riduci ambito**.
- 3 Nell'elenco dei VDC che sono membri della rete del gruppo, selezionare il VDC che si desidera impostare come ambito della rete e quindi fare clic su **OK**.

Risultati

L'ambito della rete viene ridotto a una singola rete VDC dell'organizzazione.

Gestione dei punti di uscita dei gruppi di data center con un tipo di provider di rete NSX-T Data Center

Per instradare il traffico in ingresso e in uscita da una rete del gruppo di data center a una rete esterna, è possibile configurare un gateway edge NSX-T Data Center come punto di uscita per un gruppo di data center.

Quando si configura un gateway edge come punto di uscita per un gruppo di data center, è necessario aumentarne l'ambito al gruppo di data center. Il gateway edge diventa condiviso tra tutti i data center che partecipano al gruppo. Tutte le reti instradate collegate al gateway edge vengono collegate al gruppo di data center, che ne costituisce l'ambito.

Tutti i servizi del gateway edge continuano a far parte delle funzioni del gateway edge. Per ulteriori informazioni, vedere [Gestione dei gateway edge NSX-T Data Center](#).

Se un VDC è un membro del gruppo di data center e non sono collegati carichi di lavoro a nessuna delle reti instradate che non fanno parte dell'ambito di destinazione, è possibile rimuovere un gateway edge da un gruppo di data center e impostarne l'ambito su un singolo VDC.

È possibile aggiungere un gateway edge alla rete di un gruppo di data center isolata, convertendola in una rete di data center instradata. È inoltre possibile rimuovere la connessione a un gateway edge dalla rete di un gruppo di data center, convertendo la rete instradata in una rete del gruppo di data center isolata.

Aggiunta di un gateway edge NSX-T Data Center a un gruppo di data center

Per configurare un gateway edge di NSX-T Data Center come punto di uscita per un gruppo di data center, aumentare l'ambito del gateway edge. Il gateway diventa quindi condiviso tra tutti i data center che partecipano al gruppo.

Quando si definisce un gruppo di data center come ambito di un gateway edge, tutte le reti instradate collegate al gateway edge vengono collegate al gruppo di data center che ne costituisce l'ambito.

Tutte le nuove reti instradate che vengono collegate al gateway edge appartengono al gruppo di data center.

Una rete instradata collegata a un gateway edge che ha come ambito un VDC può partecipare a un gruppo di data center solo se l'ambito dell'edge viene aumentato a questo gruppo di data center.

Prerequisiti

Verificare di aver associato un gateway edge NSX-T Data Center esistente a uno dei VDC che partecipano al gruppo di data center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Fare clic su **Gateway edge**, quindi su **Aggiungi edge**.
- 4 Selezionare uno dei gateway edge disponibili e fare clic su **Salva**.

Risultati

L'ambito del gateway edge viene aumentato al gruppo di data center. La modifica dell'ambito non influisce sui servizi o sulle reti sottostanti esistenti.

Riduzione dell'ambito di un gateway edge NSX-T Data Center a un VDC

È possibile ridurre l'ambito di un gateway edge NSX-T Data Center a un VDC specifico rimuovendo il gateway edge dal gruppo di data center che ne costituisce l'ambito.

Quando si riduce l'ambito di un gateway edge a un VDC specifico, restano tutti gli oggetti del gruppo di sicurezza utilizzati dal gateway edge. I gruppi di sicurezza utilizzati esclusivamente dal firewall distribuito continuano a far parte del gruppo di VDC.

Prerequisiti

- Verificare che il VDC a cui si desidera ridurre l'ambito del gateway edge sia membro del gruppo di data center.
- Verificare che non siano presenti carichi di lavoro collegati a reti instradate che non fanno parte dell'ambito del gateway edge di destinazione.
- Verificare che nel gruppo di data center non siano presenti gruppi di sicurezza o set di IP utilizzati sia dal gateway edge sia dal firewall distribuito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.
- 2 Fare clic sul gruppo di data center di destinazione.
- 3 Fare clic su **Gateway edge**, quindi su **Rimuovi edge**.
- 4 Selezionare un VDC a cui ridurre l'ambito del gateway edge e fare clic su **Salva**.

Gestione di reti di gruppi di data center con NSX Data Center for vSphere

Per creare una rete su più virtual data center dell'organizzazione, è innanzitutto necessario raggruppare i virtual data center, quindi creare una rete VDC che rientra nell'ambito del gruppo di data center.

VMware Cloud Director supporta le reti di gruppi di data center per i virtual data center dell'organizzazione supportati da NSX Data Center for vSphere con un punto di uscita attivo e un punto di uscita in standby per un singolo dominio di errore di rete.

Un gruppo di data center supportato da NSX Data Center for vSphere può avere una configurazione del punto di uscita comune, una configurazione del punto di uscita per ogni dominio di errore di rete o una configurazione del gruppo locale.

Gruppo di data center

Un gruppo di data center funge da router del gruppo di virtual data center che fornisce amministrazione di rete centralizzata, configurazione di più punti di uscita in più virtual data center e traffico est-ovest tra tutte le reti all'interno del gruppo. Un gruppo di data center può contenere da uno a sedici virtual data center configurati per la condivisione di più punti di uscita. Un gruppo di data center può avere una delle seguenti configurazioni dei punti di uscita:

Tabella 5-3. Tipo di configurazione dei punti di uscita per gruppi di data center supportati da NSX Data Center for vSphere

Tipo di configurazione dei punti di uscita	Descrizione
Configurazione comune dei punti di uscita	<p>È possibile configurare il gruppo di data center con un punto di uscita attivo e un punto di uscita in standby. I due punti di uscita sono comuni a tutti i virtual data center di tutti i domini di errore di rete nel gruppo di data center.</p> <p>Un gruppo di data center con questa configurazione può includere data center da un massimo di quattro domini di errore di rete.</p>
Configurazione dei punti di uscita per il dominio di errore	<p>È possibile configurare il gruppo di data center con un punto di uscita attivo e un punto di uscita in standby per ogni dominio di errore di rete nel gruppo di data center.</p> <p>Un gruppo di data center con questa configurazione può includere data center da un massimo di quattro domini di errore di rete.</p>
Configurazione di un gruppo locale	<p>I virtual data center dell'organizzazione di un gruppo di data center locale sono supportati da una singola istanza di vCenter Server. È possibile configurare il gruppo di data center locale con un punto di uscita attivo e un punto di uscita in standby per un singolo dominio di errore di rete.</p>

Un'organizzazione può includere più gruppi di data center. Un virtual data center dell'organizzazione può appartenere a più gruppi di data center.

I virtual data center inclusi in un gruppo possono appartenere a siti di VMware Cloud Director diversi. Vedere [Configurazione e gestione di distribuzioni multisito](#).

Dominio di errore di rete

Ambito del provider di rete, che in genere rappresenta l'istanza di vCenter Server sottostante con l'istanza di NSX Manager associata.

Punto di uscita

Gateway edge che connette un gruppo di data center o un dominio di errore di rete a Internet. Il gateway edge deve appartenere a un virtual data center del gruppo di data center. Le route BGP sono configurate nel gateway edge che rappresenta il punto di uscita e il router universale del gruppo di virtual data center o del dominio di errore di rete. I percorsi esistenti sul gateway edge non vengono toccati.

Rete estesa

Rete di livello 2 che viene estesa a tutti i virtual data center in un gruppo di data center. Può essere solo IPv4.

Gestione dei gruppi di data center con il tipo di provider di rete di NSX Data Center for vSphere

Dopo aver creato un gruppo di data center supportato da NSX Data Center for vSphere, è possibile modificare la topologia di rete di un gruppo di data center. È possibile aggiungere e rimuovere virtual data center dal gruppo. È possibile scambiare, sostituire e rimuovere punti di uscita. È possibile correggere errori di configurazione eseguendo diverse attività di sincronizzazione.

Non è possibile convertire una configurazione di uscita comune in una configurazione di uscita per dominio di errore o viceversa.

Creazione e configurazione di un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione dei punti di uscita comune

È possibile creare e configurare un gruppo di virtual data center supportato da NSX Data Center for vSphere con una configurazione di uscita comune impostando una coppia di gateway edge che fungono da punti di uscita attivo e in standby per tutti i virtual data center del gruppo.

Prerequisiti

- Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.
- L'**amministratore di sistema** deve abilitare i virtual data center di destinazione per le reti inter-VDC.

Procedura

- 1 [Creazione di un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita comune](#)

È possibile raggruppare da uno a sedici virtual data center in un gruppo di data center con una configurazione di uscita comune.

2 Aggiunta di un punto di uscita attivo a un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

Per connettere il gruppo di data center a Internet, è necessario aggiungere un punto di uscita attivo alla sua topologia di rete.

3 Aggiunta di un punto di uscita di standby a un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

Nei gruppi di virtual data center con configurazioni con punti di uscita comuni, è possibile aggiungere un punto di uscita secondario, che agisce come punto di uscita in standby per gli scenari di tolleranza d'errore.

Creazione di un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita comune

È possibile raggruppare da uno a sedici virtual data center in un gruppo di data center con una configurazione di uscita comune.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic su **Nuovo**.

- 3 Nella pagina **VDC di avvio**, selezionare un VDC per avviare il gruppo di VDC.

- 4 Immettere un nome e, facoltativamente, una descrizione per il nuovo gruppo di data center.

- 5 Selezionare **Punti di uscita comuni** e fare clic su **Avanti**.

- 6 Nella pagina **VDC partecipanti**, selezionare i data center aggiuntivi per il nuovo gruppo di data center e fare clic su **Avanti**.

La pagina **Data center** contiene un elenco dei VDC che l'**amministratore di sistema** ha abilitato per le reti tra virtual data center.

- 7 Rivedere i dettagli del gruppo di data center e fare clic su **Fine**.

Risultati

Il gruppo di virtual data center appena creato viene elencato nella vista **Gruppi di data center**.

Aggiunta di un punto di uscita attivo a un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

Per connettere il gruppo di data center a Internet, è necessario aggiungere un punto di uscita attivo alla sua topologia di rete.

Prerequisiti

L'**amministratore di sistema** ha creato almeno un gateway edge in uno dei virtual data center del gruppo.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Fare clic su **Aggiungi punto di uscita**.

La pagina **Aggiungi punto di uscita** che si apre fornisce un elenco dei gateway edge che appartengono ai virtual data center del gruppo.

- 4 Selezionare il gateway edge che si desidera agisca come punto di uscita attivo per questo gruppo di data center e fare clic su **Aggiungi**.

Risultati

Sul gateway edge che rappresenta il punto di uscita e il router universale del gruppo di virtual data center, vengono configurati i percorsi di routing BGP. I percorsi esistenti sul gateway edge non vengono toccati.

Il diagramma della topologia di rete viene aggiornato con il punto di uscita appena aggiunto. Il traffico dai virtual data center del gruppo a Internet è rappresentato da una linea blu continua.

Aggiunta di un punto di uscita di standby a un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

Nei gruppi di virtual data center con configurazioni con punti di uscita comuni, è possibile aggiungere un punto di uscita secondario, che agisce come punto di uscita in standby per gli scenari di tolleranza d'errore.

Prerequisiti

Oltre al gateway edge che agisce come punto di uscita attivo, è necessario disporre di almeno un altro gateway edge in ogni virtual data center del gruppo.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

3 Fare clic su **Aggiungi punto di uscita in standby**.

Viene aperta la pagina **Aggiungi punto di uscita in standby** contenente un elenco dei gateway edge inutilizzati che appartengono ai virtual data center del gruppo. Il gateway edge che viene utilizzato dal punto di uscita attivo in questo gruppo di virtual data center non viene visualizzato.

4 Selezionare il gateway edge che si desidera agisca come punto di uscita in standby per questo gruppo di data center e fare clic su **Aggiungi**.

Risultati

Nel gateway edge che rappresenta il punto di uscita e il router universale del dominio di errore di rete, vengono configurati i percorsi BGP. La configurazione non influisce sulle route esistenti nel gateway edge.

Il diagramma della topologia di rete viene aggiornato con il punto di uscita appena aggiunto. Il traffico dai virtual data center del gruppo a Internet negli scenari di tolleranza d'errore è rappresentato da una linea blu tratteggiata.

Creazione e configurazione di un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione dei punti di uscita per dominio di errore

È possibile creare e configurare un gruppo di virtual data center supportato da NSX Data Center for vSphere con una configurazione dei punti di uscita per dominio di errore configurando un gateway edge che funge da punto di uscita attivo per ciascun dominio di errore di rete nel gruppo. In un gruppo di data center con una configurazione dei punti di uscita per dominio di errore non è possibile creare punti di uscita in standby.

Prerequisiti

Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.

Procedura

1 [Creazione di un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita del dominio di errore](#)

È possibile raggruppare da uno a sedici virtual data center in un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita del dominio di errore.

2 [Aggiunta di un punto di uscita per un dominio di errore](#)

Per connettere a Internet i virtual data center di un dominio di errore di rete di un gruppo di data center supportato da NSX Data Center for vSphere, è necessario aggiungere un punto di uscita a tale dominio di errore di rete. È possibile aggiungere un punto di uscita a ciascun dominio di errore di rete del gruppo di data center. In un gruppo di data center con configurazione del punto di uscita per il dominio di errore, i punti di uscita in standby non sono supportati.

Creazione di un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita del dominio di errore

È possibile raggruppare da uno a sedici virtual data center in un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita del dominio di errore.

Prerequisiti

L'**amministratore di sistema** ha abilitato i virtual data center di destinazione per le reti inter-VDC.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic su **Nuovo**.

- 3 Immettere un nome e, facoltativamente, una descrizione per il nuovo gruppo di data center.

- 4 Selezionare **Punti di uscita per dominio di errore** e fare clic su **Avanti**.

- 5 Nella pagina **VDC partecipanti**, selezionare i data center aggiuntivi per il nuovo gruppo di data center e fare clic su **Avanti**.

La pagina **Data center** contiene un elenco dei VDC che l'**amministratore di sistema** ha abilitato per le reti tra virtual data center.

- 6 Rivedere i dettagli del gruppo di data center e fare clic su **Fine**.

Risultati

Il gruppo di virtual data center appena creato viene elencato nella vista **Gruppi di data center**.

Aggiunta di un punto di uscita per un dominio di errore

Per connettere a Internet i virtual data center di un dominio di errore di rete di un gruppo di data center supportato da NSX Data Center for vSphere, è necessario aggiungere un punto di uscita a tale dominio di errore di rete. È possibile aggiungere un punto di uscita a ciascun dominio di errore di rete del gruppo di data center. In un gruppo di data center con configurazione del punto di uscita per il dominio di errore, i punti di uscita in standby non sono supportati.

Prerequisiti

Oltre ai gateway edge in uso come punti di uscita in questo gruppo di data center, è necessario disporre almeno di un gateway edge inutilizzato in ogni virtual data center del gruppo.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

3 Nel diagramma della topologia di rete, fare clic sul dominio di errore di rete di destinazione.

I domini di errore di rete sono rappresentati da linee continue e dai rispettivi nomi nella parte inferiore del diagramma.

Il dominio di errore selezionato viene contrassegnato in blu.

4 Fare clic su **Aggiungi punto di uscita**.

La pagina **Aggiungi punto di uscita attivo** che viene aperta include un elenco dei gateway edge che appartengono ai virtual data center del gruppo.

5 Selezionare il gateway edge che si desidera agisca come punto di uscita per questo dominio di errore e fare clic su **Aggiungi**.

Risultati

Nel gateway edge che rappresenta il punto di uscita e il router universale del dominio di errore di rete, vengono configurati i percorsi BGP. I percorsi esistenti sul gateway edge non vengono toccati.

Il diagramma della topologia di rete viene aggiornato con il punto di uscita appena aggiunto. Il traffico dai virtual data center nel dominio di errore di rete a Internet è rappresentato da una linea blu continua.

Creazione e configurazione di un gruppo di virtual data center locale con il tipo di provider di rete di NSX Data Center for vSphere

A partire dalla versione 10.1, VMware Cloud Director supporta i gruppi di data center supportati da NSX Data Center for vSphere con un punto di uscita attivo e un punto di uscita in standby per un unico dominio di errore di rete.

I virtual data center dell'organizzazione di un gruppo locale sono supportati da una singola istanza di vCenter Server.

In un gruppo di data center locale, è possibile impostare una coppia di gateway edge, ovvero un punto di uscita attivo e un punto di uscita in standby, per supportare gli scenari di disponibilità elevata e ripristino di emergenza all'interno dello stesso dominio di errore di rete.

Prerequisiti

Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.

Procedura

1 Creazione di un gruppo di data center locale con il tipo di provider di rete di NSX Data Center for vSphere

È possibile raggruppare da uno a sedici virtual data center (VDC) in un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita del dominio di errore.

2 Aggiunta di un punto di uscita attivo per un gruppo di data center locale con il tipo di provider di rete di NSX Data Center for vSphere

Per connettere a Internet i data center del gruppo di data center locale supportata da NSX Data Center for vSphere, è necessario aggiungere un punto di uscita attivo al dominio di errore di rete.

3 Aggiunta di un punto di uscita di standby per un gruppo di data center locale con il tipo di provider di rete di NSX Data Center for vSphere

Nelle configurazioni dei gruppi di data center locali, è possibile aggiungere un punto di uscita secondario, che funge da punto di uscita in stand-by per gli scenari di tolleranza degli errori.

Creazione di un gruppo di data center locale con il tipo di provider di rete di NSX Data Center for vSphere

È possibile raggruppare da uno a sedici virtual data center (VDC) in un gruppo di data center supportato da NSX Data Center for vSphere con una configurazione del punto di uscita del dominio di errore.

Prerequisiti

L'**amministratore di sistema** ha abilitato i virtual data center di destinazione per le reti inter-VDC.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

2 Fare clic su **Nuovo**.

3 Nella pagina **VDC di avvio**, selezionare un VDC per avviare il gruppo di VDC.

4 Immettere un nome e, facoltativamente, una descrizione per il nuovo gruppo di data center.

5 Per creare un gruppo che contenga solo virtual data center di un unico dominio di errore di rete, attivare l'opzione **Crea gruppo locale**.

6 Fare clic su **Avanti**.

- 7 Nella pagina **VDC partecipanti**, selezionare i data center aggiuntivi per il nuovo gruppo di data center e fare clic su **Avanti**.

La pagina **Data center** contiene un elenco dei VDC che l'**amministratore di sistema** ha abilitato per le reti tra virtual data center.

- 8 Rivedere i dettagli del gruppo di data center e fare clic su **Fine**.

Risultati

Il gruppo di virtual data center appena creato viene visualizzato nella vista **Gruppi di data center**.

Aggiunta di un punto di uscita attivo per un gruppo di data center locale con il tipo di provider di rete di NSX Data Center for vSphere

Per connettere a Internet i data center del gruppo di data center locale supportata da NSX Data Center for vSphere, è necessario aggiungere un punto di uscita attivo al dominio di errore di rete.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Fare clic su **Aggiungi punto di uscita**.

- 4 Dall'elenco dei gateway edge che appartengono ai virtual data center partecipanti, selezionare un gateway edge che funga da punto di uscita attivo per il gruppo di data center e fare clic su **Aggiungi**.

Risultati

Nel gateway edge che rappresenta il punto di uscita e il router universale del dominio di errore di rete, vengono configurati i percorsi BGP. La configurazione non influisce sulle route esistenti nel gateway edge.

Il punto di uscita attivo appena aggiunto viene visualizzato nel diagramma della topologia di rete. Una linea blu continua rappresenta il traffico dai virtual data center del dominio di errore di rete a Internet.

Operazioni successive

Per consentire la tolleranza di errore del punto di uscita, aggiungere un punto di uscita in standby per il gruppo di data center locale.

Aggiunta di un punto di uscita di standby per un gruppo di data center locale con il tipo di provider di rete di NSX Data Center for vSphere

Nelle configurazioni dei gruppi di data center locali, è possibile aggiungere un punto di uscita secondario, che funge da punto di uscita in stand-by per gli scenari di tolleranza degli errori.

Prerequisiti

Oltre al gateway edge che agisce come punto di uscita attivo, è necessario disporre di almeno un altro gateway edge in ogni virtual data center del gruppo di data center locale.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Fare clic su **Aggiungi punto di uscita in standby**.

Viene aperta la pagina **Aggiungi punto di uscita in standby** contenente un elenco dei gateway edge inutilizzati che appartengono ai virtual data center del gruppo. Il gateway edge utilizzato dal punto di uscita attivo in questo gruppo di virtual data center viene visualizzato in grigio.

- 4 Selezionare il gateway edge che si desidera agisca come punto di uscita in standby per questo gruppo di data center e fare clic su **Aggiungi**.

Risultati

Nel gateway edge che rappresenta il punto di uscita e il router universale del dominio di errore di rete, vengono configurati i percorsi BGP. La configurazione non influisce sulle route esistenti nel gateway edge.

Il punto di uscita appena aggiunto viene visualizzato nel diagramma della topologia di rete. Una riga blu tratteggiata rappresenta il traffico dai virtual data center partecipanti a Internet in scenari di tolleranza di errore.

Visualizzazione di un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

È possibile visualizzare i gruppi di data center nell'organizzazione e i dettagli sulla loro configurazione corrente.

Prerequisiti

Questa operazione richiede il ruolo di **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Visualizza gruppo di VDC** pubblicato nell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

Aggiunta di un virtual data center a un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

È possibile aggiungere un virtual data center a un gruppo di data center, ed estendere in questo modo le reti esistenti al nuovo virtual data center.

Prerequisiti

- Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.
- Il gruppo di data center deve contenere meno di quattro virtual data center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Fare clic su **Aggiungi data center**.

- 4 Nella pagina **Data center**, selezionare il data center da aggiungere al gruppo di data center e fare clic su **Fine**.

La pagina **Data center** contiene l'elenco dei virtual data center abilitati per i servizi di rete inter-VDC dall'amministratore di sistema.

Nota Un gruppo di data center può contenere fino a quattro virtual data center.

Rimozione di un virtual data center da un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

È possibile rimuovere un virtual data center da un gruppo di data center, annullando in tal modo l'estensione delle reti esistenti a tale virtual data center.

Prerequisiti

- Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.
- Il gruppo di data center deve contenere almeno tre virtual data center.
- Il virtual data center che si desidera rimuovere non deve fornire un punto di uscita al gruppo di data center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.
- 2 Fare clic sul gruppo di data center di destinazione.
Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.
- 3 Nell'angolo superiore destro della scheda del virtual data center di destinazione, fare clic sui tre puntini e quindi su **Rimuovi**.
- 4 Per confermare, fare clic su **Rimuovi**.

Risultati

Il virtual data center viene rimosso dal diagramma della topologia di rete del gruppo di data center.

Sincronizzazione di un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

Per applicare nuovamente le configurazioni di rete di un gruppo di data center e assicurarsi che tutti i virtual data center partecipanti siano attivi, è possibile sincronizzare il gruppo di data center.

Nota Durante il processo di sincronizzazione del gruppo di data center, il gruppo di data center diventa non disponibile per alcuni secondi, poiché il router universale esegue la sincronizzazione in NSX.

Prerequisiti

Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.
Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Fare clic su **Sincronizza gruppo di data center**.

- 4 Per confermare, fare clic su **OK**.

Scambio di punti di uscita in un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere e una configurazione di uscita comune

Dopo aver configurato un punto di uscita attivo e un punto di uscita in standby in un gruppo di data center con una configurazione di uscita comune, è possibile scambiare i ruoli dei punti di uscita. Il punto di uscita attivo può diventare un punto di uscita in standby e viceversa.

Prerequisiti

Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Fare clic su **Scambia punti di uscita**.

- 4 Per confermare, fare clic su **OK**.

Risultati

Il diagramma della topologia di rete viene aggiornato con le nuove ruote del traffico. Il traffico verso Internet viene ora reindirizzato al nuovo punto di uscita attivo.

Sostituzione del gateway edge di un punto di uscita di un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

È possibile sostituire il gateway edge che rappresenta un punto di uscita attivo o in standby in un gruppo di data center.

Prerequisiti

- Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.

- Il nuovo gateway edge non deve essere utilizzato da altri punti di uscita nel gruppo di data center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Se si sostituisce un punto di uscita da una configurazione di dominio di errore di rete, nel diagramma della topologia di rete, selezionare il dominio di errore di rete del punto di uscita di destinazione.

I domini di errore di rete sono rappresentati con linee continue e nomi di dominio nella parte inferiore del diagramma.

Il dominio di errore di rete selezionato è contrassegnato in blu.

- 4 Nell'angolo superiore destro della scheda del punto di uscita di destinazione, fare clic sui tre puntini e scegliere **Sostituisci**.

Viene aperta la pagina **Sostituisci punto di uscita** che include un elenco dei gateway edge appartenenti ai virtual data center partecipanti.

- 5 Selezionare il nuovo gateway edge e fare clic su **Sostituisci**.

Risultati

Le route BGP vengono rimosse dal vecchio gateway edge e configurate nel nuovo gateway edge che rappresenta il punto di uscita e il router universale del gruppo di virtual data center.

Il diagramma della topologia di rete viene aggiornato con il nome del nuovo gateway edge.

Rimozione di un punto di uscita da un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

Per disconnettere un gruppo di data center o un dominio di errore di rete da Internet, è possibile rimuoverne il punto di uscita.

Prerequisiti

- Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.
- Se si desidera rimuovere un punto di uscita attivo associato a un punto di uscita in standby, è necessario scambiare i punti di uscita o rimuovere il punto di uscita in standby.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Se si rimuove un punto di uscita da una configurazione di dominio di errore di rete, nel diagramma della topologia di rete selezionare il dominio di errore di rete del punto di uscita di destinazione.

I domini di errore di rete sono rappresentati con linee continue e nomi di dominio nella parte inferiore del diagramma.

Il dominio di errore di rete selezionato è contrassegnato in blu.

- 4 Nell'angolo superiore destro della scheda del punto di uscita di destinazione, fare clic sui tre puntini e quindi su **Elimina**.
- 5 Per confermare, fare clic su **OK**.

Risultati

Le route BGP vengono rimosse dal gateway edge che rappresenta il punto di uscita se non viene utilizzato da altri router universali.

Il punto di uscita viene rimosso dal diagramma della topologia di rete.

Sincronizzazione di route e punti di uscita di un gruppo di data center con il tipo di provider di rete di NSX Data Center for vSphere

La sincronizzazione delle route consente di applicare nuovamente la configurazione del routing dinamico a un gruppo di data center oppure a un dominio di errore di rete e ai relativi punti di uscita. È possibile assicurarsi che un punto di uscita sia connesso correttamente al gruppo di data center sincronizzando il punto di uscita.

Prerequisiti

- Questa operazione richiede il ruolo **Amministratore di sistema** o un ruolo con il diritto **Gruppo di VDC: Configura gruppo di VDC** pubblicato nell'organizzazione.
- È stato configurato un punto di uscita per il gruppo di data center o il dominio di errore di rete di destinazione.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete** e quindi fare clic sulla scheda **Gruppi di data center**.

Viene visualizzato l'elenco dei gruppi di data center.

- 2 Fare clic sul gruppo di data center di destinazione.

Viene aperta la vista **Topologia di rete** per questo gruppo di data center. Il diagramma della topologia di rete corrente include i VDC partecipanti con i rispettivi domini di errore di rete, gli eventuali punti di uscita configurati e le route del traffico.

- 3 Se si sincronizza un dominio di errore di rete in un gruppo di data center, nel diagramma della topologia di rete selezionare il dominio di errore di rete di destinazione.

I domini di errore di rete sono rappresentati con linee continue e nomi di dominio nella parte inferiore del diagramma.

Il dominio di errore di rete selezionato è contrassegnato in blu.

- 4 Per applicare nuovamente la configurazione del routing dinamico al gruppo o al dominio di errore di rete e ai relativi punti di uscita, fare clic su **Sincronizza route** e quindi su **OK**.
- 5 Per sincronizzare un punto di uscita con il relativo gruppo di data center, nell'angolo superiore destro della scheda del punto di uscita di destinazione, fare clic sui tre puntini, quindi su **Sincronizza** e su **OK**.

Gestione di reti di gruppi di data center supportate da NSX Data Center for vSphere

Dopo aver creato e configurato un gruppo di data center, è possibile creare e gestire reti di livello 2 del gruppo di VDC ai virtual data center partecipanti.

Aggiunta di una rete del gruppo di VDC supportata da NSX Data Center for vSphere

È possibile creare una rete del gruppo di VDC per tutti i virtual data center che fanno parte di un gruppo di data center.

È possibile aggiungere solo una rete di un gruppo di data center IPv4 supportata da NSX Data Center for vSphere.

Prerequisiti

Questa operazione richiede il ruolo **Amministratore organizzazione** predefinito o un ruolo con il diritto **Rete VDC dell'organizzazione: Modifica proprietà**.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Nella scheda **Reti**, fare clic su **Nuovo**.

- 3 Nella pagina **Ambito**, selezionare **Gruppo di data center**, selezionare un gruppo di data center supportato da NSX Data Center for vSphere in cui creare la rete e fare clic su **Avanti**.
- 4 Immettere un nome significativo per la rete.
- 5 Immettere le impostazioni CIDR (Classless Inter-Domain Routing) per la rete.
Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.
- 6 Immettere una descrizione della rete VDC dell'organizzazione.
- 7 Fare clic su **Avanti**.
- 8 Controllare le impostazioni e fare clic su **Fine**.

Risultati

È possibile visualizzare la rete del gruppo di data center appena creata nell'elenco di reti dell'organizzazione.

Il tipo di rete è elencato come inter-VDC.

Per ogni virtual data center del gruppo viene creata una rete di virtual data center dell'organizzazione con routing di tipo inter-VDC. È possibile visualizzare le reti del gruppo di VDC dei virtual data center partecipanti facendo clic sulla scheda di un virtual data center partecipante e quindi su **Reti**. Se una macchina virtuale o una vApp si connette a una di queste reti di virtual data center dell'organizzazione, si connette alla rete del gruppo di VDC.

Operazioni successive

È possibile assegnare pool di IP e indirizzi IP statici a ogni rete di virtual data center dell'organizzazione inter-VDC corrispondente. Vedere [Aggiunta di indirizzi IP al pool di IP di una rete di virtual data center dell'organizzazione](#).

Per le configurazioni DNS e DHCP delle macchine virtuali collegate a una rete del gruppo di VDC, è possibile utilizzare VMware Cloud Director OpenAPI. Per esaminare la documentazione di VMware Cloud Director OpenAPI, visitare la pagina https://Cloud_Director_IP_address_or_host_name/docs. Per visualizzare esempi di codice e testare le chiamate di VMware Cloud Director OpenAPI, passare alla pagina https://Cloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name.

Visualizzazione o modifica di una rete del gruppo di data center supportata da NSX Data Center for vSphere

È possibile visualizzare il nome, la descrizione e le impostazioni CIDR di una rete del gruppo di data center supportata da NSX Data Center for vSphere. È possibile modificare solo il nome e la descrizione di una rete del gruppo di data center supportata da NSX Data Center for vSphere.

Per informazioni sulla modifica dell'allocazione del pool di IP statici per una rete del gruppo di data center a livello di virtual data center, vedere [Aggiunta di indirizzi IP al pool di IP di una rete di virtual data center dell'organizzazione](#).

Prerequisiti

Verificare che sia stato assegnato il ruolo di **amministratore dell'organizzazione** predefinito o un ruolo che includa il diritto **Rete VDC dell'organizzazione: Visualizza proprietà** e **Rete VDC dell'organizzazione: Modifica proprietà**.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Fare clic sulla rete di destinazione per visualizzarne i dettagli.
- 3 Per modificare il nome e la descrizione delle reti, fare clic su **Modifica**.
- 4 Modificare i dettagli della rete e fare clic su **Salva**.

Sincronizzazione di una rete del gruppo di data center supportata da NSX Data Center for vSphere

Per garantire che tutti i virtual data center partecipanti possano accedere alla rete del gruppo di data center supportata da NSX Data Center for vSphere, è possibile sincronizzare la rete del gruppo di data center.

Prerequisiti

Questa operazione richiede il ruolo **Amministratore organizzazione** predefinito o un ruolo con il diritto **Rete VDC dell'organizzazione: Modifica proprietà**.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**.
- 2 Nella scheda Reti, selezionare il pulsante di opzione accanto al nome della rete di destinazione e fare clic su **Sincronizza**.
- 3 Per confermare, fare clic su **OK**.

Gestione dei servizi gateway edge NSX Data Center for vSphere

VMware Cloud Director fornisce le funzionalità di rete avanzate gestite dal software di virtualizzazione di rete NSX Data Center for vSphere che offre controlli di sicurezza avanzati, nonché funzionalità di scalabilità di rete e routing in un ambiente cloud.

Utilizzando queste funzionalità di rete, è possibile ottenere caratteristiche di sicurezza e isolamento senza precedenti nel virtual data center dell'organizzazione. Queste funzionalità offrono i seguenti vantaggi:

- Routing dinamico. Le funzionalità di NSX Data Center for vSphere nell'ambiente VMware Cloud Director supportano protocolli di routing come BGP (Border Gateway Protocol) e OSPF (Open Shortest Path First) per semplificare l'integrazione di rete tra i sistemi allo scopo di garantire continuità e ridondanza nella distribuzione di applicazioni ospitata nel cloud.

- Isolamento e sicurezza di rete con granularità fine. Le funzionalità di NSX Data Center for vSphere nell'ambiente VMware Cloud Director supportano l'uso di definizioni di regole basate sugli oggetti per fornire isolamento del traffico di rete con stato senza che siano necessarie più reti virtuali. Questo modello di sicurezza zero-trust impedisce agli intrusi di ottenere accesso completo alla rete se un'applicazione o una macchina virtuale risulta compromessa. La configurazione di rete è semplificata dall'utilizzo degli stessi criteri di sicurezza di rete per proteggere le applicazioni ovunque esse si trovino fisicamente nell'ambiente VMware Cloud Director e per estendere il modello di sicurezza zero-trust per la sicurezza portatile indipendentemente dalla posizione di distribuzione dell'applicazione.
- Le funzionalità aggiuntive offerte da NSX Data Center for vSphere sono supporto VPN per point-to-site (VPN IPsec) e connettività utente (SSL VPN-Plus) migliorati, bilanciamento del carico migliorato per HTTPS e scalabilità di rete estesa.

È possibile configurare due tipi di firewall, ovvero il firewall del gateway edge e il firewall distribuito. Per ulteriori informazioni sulle differenze tra questi firewall, vedere [Configurazione del firewall del tenant con NSX Data Center for vSphere](#).

È possibile accedere a queste funzionalità di rete avanzate utilizzando il portale tenant di VMware Cloud Director o il VMware Cloud Director Service Provider Admin Portal. Il gateway edge deve innanzitutto essere convertito in un gateway edge avanzato. Vedere [Conversione di un gateway edge di NSX Data Center for vSphere in un gateway edge avanzato](#).

Importante I gateway edge IPv6 supportano servizi limitati. I gateway edge IPv6 supportano i firewall edge, i firewall distribuiti e il routing statico.

Guida introduttiva alla rete avanzata di VMware Cloud Director con NSX Data Center for vSphere

È possibile utilizzare i servizi di rete avanzati di VMware Cloud Director per eseguire attività di gestione in un'organizzazione di un sistema VMware Cloud Director. È possibile gestire firewall distribuiti e altre funzionalità di rete avanzate fornite da NSX Data Center for vSphere e rese disponibili per l'organizzazione da un amministratore di sistema di VMware Cloud Director.

Gli utenti tipici della rete avanzata fornita da NSX Data Center for vSphere sono:

- VMware Cloud Director **Amministratori di sistema** che possono utilizzare il portale tenant per configurare il firewall distribuito e altre funzionalità dei servizi di rete avanzati per un'organizzazione.
- **Amministratori dell'organizzazione** che utilizzano il portale tenant per gestire il firewall distribuito e altre funzionalità dei servizi di rete avanzati che l'**amministratore di sistema** ha reso disponibili per l'organizzazione.

Configurazione del firewall del tenant con NSX Data Center for vSphere

Tramite il portale tenant, è possibile configurare le funzionalità del firewall fornite da NSX Data Center for vSphere nel virtual data center dell'organizzazione di VMware Cloud Director. È

possibile creare regole del firewall per firewall distribuiti allo scopo di fornire sicurezza tra le macchine virtuali del virtual data center di un'organizzazione e regole del firewall da applicare a un firewall del gateway edge per proteggere dal traffico di rete esterno le macchine virtuali del virtual data center di un'organizzazione.

Nota Il portale tenant offre la possibilità di configurare sia firewall del gateway edge sia firewall distribuiti.

La tecnologia del firewall logico di NSX Data Center for vSphere include due componenti per soddisfare diversi casi d'uso della distribuzione. Il firewall del gateway edge si occupa dell'applicazione del traffico verticale, mentre il firewall distribuito si occupa dei controlli di accesso orizzontale.

Differenze principali tra firewall del gateway edge e firewall distribuiti

Un firewall del gateway edge monitora il traffico verticale per fornire funzionalità di sicurezza del perimetro che includono firewall e Network Address Translation (NAT), oltre a funzionalità IPSec e VPN SSL tra siti.

Un firewall distribuito offre la possibilità di isolare e proteggere ciascuna macchina virtuale e applicazione fino al livello 2 (L2). La configurazione di firewall distribuiti consente di mettere efficacemente in quarantena qualsiasi compromissione della sicurezza di rete esterna o interna, isolando il traffico orizzontale tra macchine virtuali nello stesso segmento di rete. I criteri di protezione sono gestiti centralmente, ereditabili e nidificabili. In questo modo, gli amministratori di rete e della sicurezza possono gestirli scalarmente. Inoltre, una volta distribuiti, i criteri di protezione definiti seguono le applicazioni o le macchine virtuali quando vengono spostate tra virtual data center diversi.

Informazioni sulle regole del firewall

Come descritto nella documentazione del prodotto pertinente, in NSX Data Center for vSphere, le regole del firewall definite a livello centralizzato vengono definite pre-regole. È inoltre possibile aggiungere regole a livello di un gateway edge singolo, che vengono definite regole locali.

Ogni sessione di traffico viene verificata in base alla regola principale nella tabella del firewall prima di passare alle regole successive più in basso nella tabella. Viene applicata la prima regola nella tabella che corrisponde ai parametri del traffico. Le regole vengono visualizzate nell'ordine seguente:

- 1 Le pre-regole definite dall'utente hanno la priorità più alta e vengono applicate seguendo l'ordine dall'alto al basso con una precedenza a livello di NIC virtuale.
- 2 Regole con plumbing automatico (regole che abilitano il flusso del traffico di controllo per i servizi del gateway edge).
- 3 Regole locali definite a livello del gateway edge.
- 4 Regola del firewall distribuito predefinita

Per ulteriori informazioni su come il software NSX Data Center for vSphere applica le regole del firewall, vedere l'argomento relativo alla *modifica dell'ordine di una regola del firewall* nella documentazione di NSX Data Center for vSphere.

Firewall del gateway edge di NSX Data Center for vSphere

Il firewall per il gateway edge consente di soddisfare i requisiti di sicurezza chiave del perimetro, quali la creazione di DMZ in base a costrutti IP/VLAN, l'isolamento tra tenant in virtual data center con più tenant, Network Address Translation (NAT), VPN partner (extranet) e VPN SSL basate sull'utente.

La funzionalità del firewall del gateway edge nell'ambiente di VMware Cloud Director viene fornita da NSX Data Center for vSphere. In NSX Data Center for vSphere, questa funzionalità del firewall viene definita anche firewall edge. Il firewall del gateway edge monitora il traffico verticale per fornire funzionalità di sicurezza del perimetro che includono firewall e Network Address Translation (NAT), oltre a funzionalità IPSec e VPN SSL tra siti.

Per informazioni più dettagliate sulle funzionalità fornite dal firewall del gateway edge di NSX Data Center for vSphere, vedere la documentazione di NSX Data Center for vSphere.

Gestione di un firewall del gateway edge NSX Data Center for vSphere

Per proteggere il traffico da e verso un gateway edge, è possibile creare e gestire le regole del firewall in tale gateway edge.

Per informazioni sulla protezione del traffico tra le macchine virtuali in un virtual data center dell'organizzazione, vedere [Gestione di regole del firewall distribuito di NSX Data Center for vSphere tramite il portale tenant](#).

Le regole create nella schermata Firewall distribuito in cui è specificato un gateway edge avanzato nella colonna Applicato a non vengono visualizzate nella schermata Firewall di tale gateway edge avanzato.

Le regole del firewall del gateway edge per un gateway edge vengono visualizzate nella schermata **Firewall** e vengono applicate nell'ordine seguente:

- 1 Regole interne, note anche come regole con plumbing automatico. Queste regole abilitano il flusso del traffico di controllo per i servizi del gateway edge.
- 2 Regole definite dall'utente.
- 3 Regola predefinita.

Le impostazioni della regola predefinita vengono applicate al traffico che non corrisponde ad alcuna delle regole del firewall definite dall'utente. La regola predefinita viene visualizzata in fondo all'elenco delle regole nella schermata Firewall.

Nel portale tenant, utilizzare l'opzione **Abilita** nella schermata Regole firewall del gateway edge per attivare o disattivare un firewall del gateway edge.

Conversione di un gateway edge di NSX Data Center for vSphere in un gateway edge avanzato

Per utilizzare un gateway edge di NSX Data Center for vSphere nel portale tenant, è necessario convertirlo in un gateway edge avanzato. Una volta convertito il gateway edge in un gateway edge avanzato, è possibile utilizzare il portale tenant per configurare le funzionalità di routing statico e dinamico fornite da NSX Data Center for vSphere per i gateway edge avanzati.

Prerequisiti

È necessario che sia presente un gateway edge.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Selezionare il gateway edge da modificare.
- 3 Fare clic su **Converti in avanzato**.

Risultati

Il gateway edge viene convertito in un gateway edge avanzato.

Operazioni successive

Una volta effettuata la conversione in un gateway edge avanzato, è possibile configurare le impostazioni selezionando il gateway e facendo clic su **Servizi**.

Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere

Utilizzare la scheda **Firewall** del gateway edge per aggiungere regole del firewall per il gateway edge. È possibile aggiungere più interfacce NSX Edge e più gruppi di indirizzi IP come origine e destinazione per queste regole del firewall.

Se si specifica **interna** per un'origine o una destinazione di una regola, si indica il traffico per tutte le subnet nei gruppi di porte connessi al gateway edge NSX. Se si seleziona **Interna** come origine, la regola viene aggiornata automaticamente quando nel gateway NSX vengono configurate interfacce interne aggiuntive.

Nota Le regole del firewall gateway edge sulle interfacce interne non funzionano quando il gateway edge è configurato per il routing dinamico.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Se la schermata **Regole firewall** non è ancora visibile, fare clic sulla scheda **Firewall**.

- 3 Per aggiungere una regola sotto una regola esistente nella tabella delle regole del firewall, fare clic nella riga esistente e quindi fare clic sul pulsante **Crea**.

Sotto la regola selezionata verrà aggiunta una riga per la nuova regola a cui verranno assegnati qualsiasi destinazione, qualsiasi servizio e l'azione **Consenti** per impostazione predefinita. Quando la regola predefinita definita dal sistema rappresenta l'unica regola nella tabella del firewall, la nuova regola viene aggiunta sopra la regola predefinita.

- 4 Fare clic nella cella **Nome** e digitare un nome.
- 5 Fare clic nella cella **Origine** e utilizzare le icone ora visibili per selezionare un'origine da aggiungere alla regola:

Opzione	Descrizione
Fare clic sull'icona IP	Digitare il valore di origine che si desidera utilizzare. I valori validi sono un indirizzo IP, CIDR, un intervallo IP o la parola chiave qualsiasi . Il firewall del gateway edge supporta entrambi i formati IPv4 e IPv6.
Fare clic sull'icona +	<p>Utilizzare l'icona + per specificare l'origine come oggetto diverso rispetto a un indirizzo IP specifico:</p> <ul style="list-style-type: none"> ■ Utilizzare la finestra Seleziona oggetti per aggiungere oggetti che corrispondano alle proprie selezioni e fare clic su Mantieni per aggiungerli alla regola. ■ Per escludere un'origine dalla regola, aggiungerla alla regola utilizzando la finestra Seleziona oggetti e quindi selezionare l'icona dell'interruttore di esclusione per escludere tale origine dalla regola. <p>Quando si seleziona l'interruttore di esclusione nell'origine, la regola viene applicata al traffico proveniente da tutte le origini ad eccezione dell'origine esclusa. Quando non si seleziona l'interruttore di esclusione, la regola viene applicata al traffico proveniente dall'origine specificata nella finestra Seleziona oggetti.</p>

- 6 Fare clic nella cella **Destinazione** ed eseguire una delle seguenti opzioni:

Opzione	Descrizione
Fare clic sull'icona IP	Digitare il valore di destinazione che si desidera utilizzare. I valori validi sono un indirizzo IP, CIDR, un intervallo IP o la parola chiave qualsiasi . Il firewall del gateway edge supporta entrambi i formati IPv4 e IPv6.
Fare clic sull'icona +	<p>Utilizzare l'icona + per specificare l'origine come oggetto diverso rispetto a un indirizzo IP specifico:</p> <ul style="list-style-type: none"> ■ Utilizzare la finestra Seleziona oggetti per aggiungere oggetti che corrispondano alle proprie selezioni e fare clic su Mantieni per aggiungerli alla regola. ■ Per escludere un'origine dalla regola, aggiungerla alla regola utilizzando la finestra Seleziona oggetti e quindi selezionare l'icona dell'interruttore di esclusione per escludere tale origine dalla regola. <p>Quando si seleziona l'interruttore di esclusione nell'origine, la regola viene applicata al traffico proveniente da tutte le origini ad eccezione dell'origine esclusa. Quando non si seleziona l'interruttore di esclusione, la regola viene applicata al traffico proveniente dall'origine specificata nella finestra Seleziona oggetti.</p>

- 7 Fare clic nella cella **Servizio** della nuova regola e fare clic sull'icona **+** per specificare il servizio come una combinazione di porta e protocollo:
 - a Selezionare il protocollo del servizio.
 - b Digitare i numeri di porta per la porta di origine e quella di destinazione oppure specificare **qualsiasi**.
 - c Fare clic su **Mantieni**.
- 8 Nella cella **Azione** della nuova regola, configurare l'azione per la regola.

Opzione	Descrizione
Accetta	Consente il traffico da o per le origini, le destinazioni e i servizi specificati.
Nega	Blocca il traffico da o per le origini, le destinazioni e i servizi specificati.

- 9 Fare clic su **Salva modifiche**.

Il completamento dell'operazione di salvataggio può richiedere un minuto.

Modifica delle regole del firewall del gateway edge NSX Data Center for vSphere

È possibile modificare ed eliminare solo le regole del firewall definite dall'utente che sono state aggiunte a un gateway edge. Non è possibile modificare o eliminare una regola generata automaticamente o una regola predefinita. È possibile modificare solo l'impostazione dell'azione della regola predefinita. È possibile modificare l'ordine di priorità delle regole definite dall'utente.

Per informazioni dettagliate sulle impostazioni disponibili per le varie celle di una regola, vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#).

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Firewall**.
- 3 Consente di gestire le regole firewall.
 - Per disattivare una regola, fare clic sul segno di spunta verde nella relativa cella **N**. Il segno di spunta verde diventa un'icona di disattivazione di colore rosso. Se la regola è disattivata e si desidera attivarla, fare clic sull'icona di disattivazione rossa.
 - Per modificare il nome di una regola, fare doppio clic nella relativa cella **Nome** e digitare il nuovo nome.
 - Per modificare le impostazioni di una regola, ad esempio le impostazioni dell'origine o dell'azione, selezionare la cella appropriata e utilizzare i controlli visualizzati.
 - Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina** che si trova al di sopra della tabella delle regole.

- Per nascondere le regole generate dal sistema, utilizzare l'interruttore **Mostra solo regole definite dall'utente**.
- Per spostare una regola in alto o in basso nella tabella delle regole, selezionare la regola e fare clic sui pulsanti freccia giù e freccia su che si trovano al di sopra della tabella.

4 Fare clic su **Salva modifiche**.

Firewall distribuito di NSX Data Center for vSphere

Il firewall distribuito consente di segmentare le entità dei virtual data center dell'organizzazione, ad esempio le macchine virtuali, in base agli attributi e ai nomi delle macchine virtuali.

VMware Cloud Director supporta i servizi firewall distribuiti nei virtual data center dell'organizzazione supportati da NSX Data Center for vSphere. Come descritto nella documentazione di NSX Data Center for vSphere, il firewall distribuito è un firewall hypervisor integrato nel kernel che offre visibilità e controllo per le reti e i carichi di lavoro virtualizzati. È possibile creare criteri di controllo degli accessi in base a oggetti quali nomi di macchina virtuale e costrutti di rete come indirizzi IP o indirizzi di set di IP. Le regole del firewall vengono applicate a livello di vNIC di ogni macchina virtuale per garantire un controllo degli accessi coerente anche quando la macchina virtuale viene spostata in un nuovo host ESXi da vSphere vMotion. Questo firewall distribuito supporta un modello di sicurezza a micro-segmentazione in cui è possibile ispezionare il traffico orizzontale con elaborazione vicina alla velocità della linea.

Come descritto nella documentazione di NSX Data Center for vSphere, per i pacchetti di livello 2 (L2), il firewall distribuito crea una cache per l'incremento delle prestazioni. I pacchetti di livello 3 (L3) vengono elaborati nel seguente ordine:

- 1 Tutti i pacchetti vengono controllati in base a uno stato esistente.
 - 2 Quando viene rilevata una corrispondenza di stato, i pacchetti vengono elaborati.
 - 3 Quando non viene trovata una corrispondenza di stato, i pacchetti vengono elaborati in base alle regole finché non viene trovata una corrispondenza.
- Per i pacchetti TCP, viene impostato uno stato solo per i pacchetti con contrassegno SYN. Tuttavia, le regole che non specificano un protocollo (servizio ANY) possono corrispondere ai pacchetti TCP con qualsiasi combinazione di contrassegni.
 - Per i pacchetti UDP, vengono estratti dettagli quintupli dal pacchetto. Quando uno stato non è presente nella tabella di stato, viene creato un nuovo stato utilizzando i dettagli quintupli estratti. I pacchetti ricevuti successivamente vengono esaminati per trovare una corrispondenza con lo stato appena creato.
 - Per i pacchetti ICMP, per creare uno stato vengono utilizzati il tipo, il codice e la direzione del pacchetto ICMP.

Il firewall distribuito è utile anche per la creazione di regole basate sull'identità. Gli amministratori possono imporre il controllo degli accessi in base all'appartenenza al gruppo dell'utente, come definito nella Active Directory (AD) aziendale. Alcuni casi d'uso relativi all'utilizzo di regole del firewall basate sull'identità sono:

- Utenti che accedono alle applicazioni virtuali utilizzando un laptop o un dispositivo mobile in cui la Active Directory viene utilizzata per l'autenticazione dell'utente
- Utenti che accedono alle applicazioni virtuali utilizzando l'infrastruttura VDI in cui le macchine virtuali sono basate su Microsoft Windows

Per informazioni più dettagliate sulle funzionalità fornite dal firewall distribuito, vedere la documentazione di NSX Data Center for vSphere.

Abilitazione del firewall distribuito in un virtual data center dell'organizzazione supportato da NSX Data Center for vSphere

Prima di poter usare il portale tenant per utilizzare le funzionalità del firewall distribuito fornite da NSX Data Center for vSphere nel virtual data center di un'organizzazione, è necessario abilitare il firewall distribuito in tale virtual data center. Il firewall distribuito può essere abilitato nel virtual data center di un'organizzazione da un amministratore di sistema di VMware Cloud Director o da un utente a cui sia stato concesso il diritto **org_vdc_distributed_firewall_enable**.

L'abilitazione del firewall distribuito per il virtual data center di un'organizzazione viene effettuata utilizzando la schermata Firewall distribuito.

Prerequisiti

Verificare che all'organizzazione a cui appartiene il virtual data center siano stati assegnati i seguenti diritti:

- Firewall distribuito del vDC dell'organizzazione: abilitazione/disabilitazione
- Firewall distribuito del vDC dell'organizzazione: configurazione regole
- Firewall distribuito del vDC dell'organizzazione: visualizzazione regole

L'**amministratore di sistema** di VMware Cloud Director assegna i diritti a un'organizzazione. Il diritto Firewall distribuito del vDC dell'organizzazione: abilitazione/disabilitazione è necessario per attivare il firewall distribuito utilizzando l'interfaccia utente del portale tenant. Il diritto Firewall distribuito del vDC dell'organizzazione: visualizzazione regole è necessario per visualizzare le regole del firewall nel portale tenant e il diritto Firewall distribuito del vDC dell'organizzazione: configurazione regole è necessario per configurare le regole del firewall tramite il portale tenant.

Verificare di disporre di un ruolo cui sia concesso il diritto denominato Firewall distribuito del vDC dell'organizzazione: abilitazione/disabilitazione. Fra i ruoli predefiniti in un sistema VMware Cloud Director, solo il ruolo di amministratore di sistema dispone di tale diritto per impostazione predefinita.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.
- 2 Selezionare il virtual data center dell'organizzazione per cui si desidera configurare le regole del firewall distribuito.
- 3 Fare clic su **Configura servizi**.
- 4 Abilitare il firewall distribuito nella scheda **Firewall distribuito**.

Operazioni successive

Per una descrizione della regola predefinita del firewall distribuito, vedere [Gestione di regole del firewall distribuito di NSX Data Center for vSphere tramite il portale tenant](#).

Gestione di regole del firewall distribuito di NSX Data Center for vSphere tramite il portale tenant

Come descritto nella documentazione di NSX Data Center for vSphere, le impostazioni del firewall predefinito si applicano al traffico che non corrisponde ad alcuna delle regole del firewall definite dall'utente. In VMware Cloud Director Tenant Portal, la regola del firewall distribuito predefinita è etichettata come regola Consenti predefinita.

Prima di poter gestire le impostazioni del firewall distribuito tramite VMware Cloud Director Tenant Portal, è necessario abilitare la funzionalità del firewall distribuito in un virtual data center dell'organizzazione.

La regola del firewall distribuito predefinita è configurata per consentire il passaggio di tutto il traffico di livello 3 e di livello 2 attraverso il virtual data center dell'organizzazione. Questa impostazione è indicata dall'opzione Consenti impostata nella colonna Azione nell'interfaccia utente. La regola predefinita si trova sempre nella parte inferiore della tabella delle regole.

Importante Non è possibile eliminare o modificare le regole del firewall distribuito predefinito.

Aggiunta di una regola del firewall distribuito

Aggiungere innanzitutto una regola del firewall distribuito nell'ambito del virtual data center dell'organizzazione. È quindi possibile restringere l'ambito in cui si desidera applicare la regola. Il firewall distribuito consente di aggiungere più oggetti a livello di origine e destinazione per ogni regola. In questo modo, è possibile ridurre il numero totale di regole del firewall da aggiungere.

Per informazioni sui servizi e sui gruppi di servizi predefiniti che possono essere utilizzati in una regola, vedere [Visualizzazione dei servizi disponibili per le regole del firewall](#) e [Visualizzazione dei gruppi di servizi disponibili per le regole del firewall](#).

Prerequisiti

- [Abilitazione del firewall distribuito in un virtual data center dell'organizzazione supportato da NSX Data Center for vSphere](#)

- Se si desidera utilizzare un set di IP come origine o destinazione in una regola, [Creazione di un set di IP da utilizzare nelle regole del firewall e nella configurazione dell'inoltro DHCP](#).
- Se si desidera utilizzare un set di MAC come origine o destinazione in una regola, [Creazione di un set di MAC da utilizzare nelle regole del firewall](#).
- Se si desidera utilizzare un gruppo di sicurezza come origine o destinazione in una regola, [Creazione di un gruppo di sicurezza](#).

Procedura


- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.

- 2 Selezionare la rete VDC dei servizi di sicurezza per cui si desidera modificare le regole del firewall e fare clic su **Configura servizi**.

Verrà visualizzata la schermata Servizi di sicurezza.

- 3 Selezionare il tipo di regola che si desidera creare. È possibile creare una regola generale o una regola Ethernet.

Le regole di livello 3 (L3) vengono configurate nella scheda **Generale**. Le regole di livello 2 (L2) vengono configurate nella scheda **Ethernet**.

- 4 Per aggiungere una regola sotto una regola esistente nella tabella del firewall, fare clic nella riga esistente e quindi fare clic sul pulsante **Crea** ()

Sotto la regola selezionata verrà aggiunta una riga per la nuova regola a cui verranno assegnati qualsiasi destinazione, qualsiasi servizio e l'azione **Consenti** per impostazione predefinita. Se la regola Consenti assegnata dal sistema per impostazione predefinita rappresenta la sola regola nella tabella del firewall, la nuova regola viene aggiunta sopra la regola predefinita.

- 5 Fare clic nella cella **Nome** e digitare un nome.

- 6 Fare clic nella cella **Origine** e utilizzare le icone ora visibili per selezionare un'origine da aggiungere alla regola:

Azione	Descrizione
Fare clic sull'icona IP	Applicabile alle regole definite nella scheda Generale . Digitare il valore di origine che si desidera utilizzare. I valori validi sono un indirizzo IP, CIDR, un intervallo IP o la parola chiave qualsiasi . Il firewall distribuito supporta solo il formato IPv4.
Fare clic sull'icona +	Utilizzare l'icona + per specificare l'origine come oggetto diverso rispetto a un indirizzo IP specifico: <ul style="list-style-type: none"> ■ Utilizzare la finestra Seleziona oggetti per aggiungere oggetti che corrispondano alle proprie selezioni e fare clic su Mantieni per aggiungerli alla regola. ■ Per escludere un'origine dalla regola, aggiungerla alla regola utilizzando la finestra Seleziona oggetti e quindi selezionare l'icona dell'interruttore di esclusione per escludere tale origine dalla regola. <p>Quando si seleziona l'interruttore di esclusione nell'origine, la regola viene applicata al traffico proveniente da tutte le origini ad eccezione dell'origine esclusa. Quando non si seleziona l'interruttore di esclusione, la regola viene applicata al traffico proveniente dall'origine specificata nella finestra Seleziona oggetti.</p>

- 7 Fare clic nella cella **Destinazione** ed eseguire una delle seguenti azioni:

Azione	Descrizione
Fare clic sull'icona IP	Applicabile alle regole definite nella scheda Generale . Digitare il valore di destinazione che si desidera utilizzare. I valori validi sono un indirizzo IP, CIDR, un intervallo IP o la parola chiave qualsiasi . Il firewall distribuito supporta solo il formato IPv4.
Fare clic sull'icona +	Utilizzare l'icona + per specificare l'origine come oggetto diverso rispetto a un indirizzo IP specifico: <ul style="list-style-type: none"> ■ Utilizzare la finestra Seleziona oggetti per aggiungere oggetti che corrispondano alle proprie selezioni e fare clic su Mantieni per aggiungerli alla regola. ■ Per escludere un'origine dalla regola, aggiungerla alla regola utilizzando la finestra Seleziona oggetti e quindi selezionare l'icona dell'interruttore di esclusione per escludere tale origine dalla regola. <p>Quando si seleziona l'interruttore di esclusione nell'origine, la regola viene applicata al traffico proveniente da tutte le origini ad eccezione dell'origine esclusa. Quando non si seleziona l'interruttore di esclusione, la regola viene applicata al traffico proveniente dall'origine specificata nella finestra Seleziona oggetti.</p>

- 8 Fare clic nella cella **Servizio** della nuova regola ed eseguire una delle seguenti azioni:

Azione	Descrizione
Fare clic sull'icona IP	Per specificare il servizio come combinazione di porta e protocollo: <ul style="list-style-type: none"> a Selezionare il protocollo del servizio. b Digitare i numeri di porta per le porta di origine e quella di destinazione oppure specificare qualsiasi e fare clic su Mantieni.
Fare clic sull'icona +	Per selezionare un servizio o un gruppo di servizi predefinito oppure per definirne uno nuovo: <ul style="list-style-type: none"> a Selezionare uno o più oggetti e aggiungerli al filtro. b Fare clic su Mantieni.

- 9 Nella cella **Azione** della nuova regola, configurare l'azione per la regola.

Opzione	Descrizione
Consenti	Consente il traffico da o per le origini, le destinazioni e i servizi specificati.
Nega	Blocca il traffico da o per le origini, le destinazioni e i servizi specificati.

- 10 Nella cella **Direzione** della nuova regola, selezionare se la regola si applica al traffico in entrata, a quello in uscita oppure a entrambi.
- 11 Se si tratta di una regola nella scheda **Generale**, nella cella **Tipo di pacchetto** della nuova regola, selezionare un tipo di pacchetto, ovvero **Qualsiasi**, **IPv4** o **IPv6**.
- 12 Selezionare la cella **Applicato a** e utilizzare l'icona + per definire l'ambito dell'oggetto a cui la regola è applicabile.

Quando la regola contiene macchine virtuali nelle celle **Origine** e **Destinazione**, è necessario aggiungere la macchina virtuale di origine e quella di destinazione alla cella **Applicato a** della regola affinché la regola funzioni correttamente.

Importante I gruppi di indirizzi IP (set di IP), i gruppi di indirizzi MAC (set di MAC) e i gruppi di sicurezza che contengono set di IP o set di MAC non sono parametri di input validi.

- 13 Fare clic su **Salva modifiche**.

Modifica di una regola del firewall distribuito

In un ambiente VMware Cloud Director, per modificare una regola del firewall distribuito esistente di un virtual data center dell'organizzazione, utilizzare la schermata **Firewall distribuito**.

Per informazioni dettagliate sulle impostazioni disponibili per le varie celle di una regola, vedere [Aggiunta di una regola del firewall distribuito](#).

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.

- 2 Selezionare la rete VDC dei servizi di sicurezza per cui si desidera modificare le regole del firewall e fare clic su **Configura servizi**.

Verrà visualizzata la schermata Servizi di sicurezza.

- 3 Per gestire le regole del firewall distribuito, eseguire una delle seguenti azioni:

- Per disattivare una regola, fare clic sul segno di spunta verde nella relativa cella **N..**
Il segno di spunta verde diventa un'icona di disattivazione di colore rosso. Se la regola è disattivata e si desidera attivarla, fare clic sull'icona di disattivazione rossa.
- Per modificare il nome di una regola, fare doppio clic nella relativa cella **Nome** e digitare il nuovo nome.
- Per modificare le impostazioni di una regola, ad esempio le impostazioni dell'origine o dell'azione, selezionare la cella appropriata e utilizzare i controlli visualizzati.
- Per eliminare una regola, selezionarla e fare clic sul pulsante **Elimina** che si trova al di sopra della tabella delle regole.
- Per spostare una regola in alto o in basso nella tabella delle regole, selezionare la regola e fare clic sui pulsanti freccia giù e freccia su che si trovano al di sopra della tabella.

- 4 Fare clic su **Salva modifiche**.

Gestione del DHCP del gateway edge NSX Data Center for vSphere

È possibile configurare gateway edge per fornire servizi DHCP (Dynamic Host Configuration Protocol) alle macchine virtuali connesse alle reti di virtual data center dell'organizzazione associata.

Come descritto nella [documentazione di NSX](#), le funzionalità di un gateway edge NSX includono il pooling degli indirizzi IP, l'allocazione degli indirizzi IP statici di tipo uno-a-uno e la configurazione di un server DNS esterno. Il binding degli indirizzi IP statici è basato sull'ID dell'oggetto gestito e sull'ID dell'interfaccia della macchina virtuale client che invia la richiesta.

Il servizio DHCP per un gateway edge NSX:

- È in ascolto sull'interfaccia interna del gateway edge per l'individuazione del DHCP.
- Utilizza l'indirizzo IP dell'interfaccia interna del gateway edge come indirizzo del gateway predefinito per tutti i client.
- Utilizza i valori del broadcast e della subnet mask dell'interfaccia interna per la rete contenitore.

Nelle seguenti circostanze, è necessario riavviare il servizio DHCP nelle macchine virtuali client i cui indirizzi IP sono stati assegnati mediante DHCP:

- È stato modificato o eliminato un pool DHCP, il gateway predefinito o il server DNS.

- È stato modificato l'indirizzo IP interno dell'istanza del gateway edge.

Nota Se si modificano le impostazioni di DNS in un gateway edge con DHCP attivato, è possibile che il gateway edge smetta di fornire i servizi DHCP. In questo caso, utilizzare l'interruttore **Stato servizio DHCP** nella schermata Pool DHCP per disattivare il servizio DHCP, quindi attivarlo nuovamente nel gateway edge. Vedere [Aggiunta di un pool di IP DHCP](#).

Aggiunta di un pool di IP DHCP

È possibile configurare i pool di IP necessari per il servizio DHCP di un gateway edge NSX Data Center for vSphere. DHCP automatizza l'assegnazione di indirizzi IP alle macchine virtuali connesse alle reti dei virtual data center dell'organizzazione.

Come descritto nella documentazione *per l'amministratore NSX*, il servizio DHCP richiede un pool di indirizzi IP. Un pool di IP è un intervallo sequenziale di indirizzi IP all'interno della rete. Alle macchine virtuali protette da un gateway edge che non dispongono di un binding di indirizzo viene assegnato un indirizzo IP da questo pool. Poiché gli intervalli dei pool di IP non possono intersecarsi, un indirizzo IP può appartenere a un solo pool di IP.

Nota Affinché venga attivato lo stato del servizio DHCP, è necessario configurare almeno un pool di IP DHCP.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **DHCP > Pool**.
- 3 Se il servizio DHCP non è abilitato, attivare l'interruttore **Stato servizio DHCP**.

Nota Aggiungere almeno un pool di IP DHCP prima di salvare le modifiche apportate dopo l'attivazione dell'interruttore **Stato servizio DHCP**. Quando nella schermata non è elencato alcun pool di IP DHCP, se si attiva l'interruttore **Stato servizio DHCP** e quindi si salvano le modifiche, la schermata viene visualizzata con l'interruttore disattivato.

- 4 In Pool DHCP, fare clic sul pulsante **Crea** () , specificare i dettagli per il pool DHCP e fare clic su **Mantieni**.

Opzione	Descrizione
Intervallo IP	Digitare un intervallo di indirizzi IP.
Nome dominio	Nome di dominio del server DNS.
Configura DNS automaticamente	Attivare questo interruttore per utilizzare la configurazione del servizio DNS per il binding DNS di questo pool di IP. Se lo si abilita, i campi Server dei nomi principale e Server dei nomi secondario sono impostati su Automatico .

Opzione	Descrizione
Server dei nomi principale	Se non si abilita Configura DNS automaticamente , digitare l'indirizzo IP del server DNS primario. Questo indirizzo IP viene utilizzato per la risoluzione degli indirizzi da nome host a IP.
Server dei nomi secondario	Se non si abilita Configura DNS automaticamente , digitare l'indirizzo IP del server DNS secondario. Questo indirizzo IP viene utilizzato per la risoluzione degli indirizzi da nome host a IP.
Gateway predefinito	Digitare l'indirizzo del gateway predefinito. Se non si specifica l'indirizzo IP del gateway predefinito, l'interfaccia interna dell'istanza del gateway edge viene impostata come gateway predefinito.
Subnet mask	Digitare la subnet mask dell'interfaccia del gateway edge.
Il lease non ha scadenza	Abilitare questo interruttore per fare in modo che gli indirizzi IP assegnati all'esterno di questo pool rimangano per sempre associati alle rispettive macchine virtuali assegnate. Se si seleziona questa opzione, il campo Durata lease viene impostato su Infinito.
Durata lease (secondi)	Intervallo di tempo (in secondi) che indica la durata del lease degli indirizzi IP assegnati dal DHCP ai client. La durata del lease predefinita è un giorno (86400 secondi). Nota Se si seleziona Il lease non ha scadenza , non è possibile specificare una durata del lease.

5 Fare clic su **Salva modifiche**.

Risultati

VMware Cloud Director aggiorna il gateway edge per fornire servizi DHCP.

Aggiunta di associazioni DHCP


Se si dispone di servizi in esecuzione in una macchina virtuale e non si desidera modificare l'indirizzo IP, è possibile associare l'indirizzo MAC della macchina virtuale all'indirizzo IP. L'indirizzo IP di cui si effettua l'associazione non deve sovrapporsi a un pool di IP DHCP.

Prerequisiti

Si dispone degli indirizzi MAC per le macchine virtuali di cui si desidera configurare le associazioni.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.

- 2 Nella scheda **DHCP > Binding**, fare clic sul pulsante **Aggiungi** () , specificare i dettagli per il binding e fare clic su **Mantieni**.

Opzione	Descrizione
Indirizzo MAC	Digitare l'indirizzo MAC della macchina virtuale che si desidera associare all'indirizzo IP.
Nome host	Digitare il nome host che si desidera impostare per la macchina virtuale quando questa richiede un lease di DHCP.
Indirizzo IP	Digitare l'indirizzo IP che si desidera associare all'indirizzo MAC.
Subnet mask	Digitare la subnet mask dell'interfaccia del gateway edge.
Nome dominio	Digitare il nome di dominio del server DNS.
Configura DNS automaticamente	Abilitare questo interruttore per utilizzare la configurazione del servizio DNS per questa associazione di DNS. Se lo si abilita, i campi Server dei nomi principale e Server dei nomi secondario sono impostati su Automatico .
Server dei nomi principale	Se non si seleziona Configura DNS automaticamente , digitare l'indirizzo IP del server DNS primario. Questo indirizzo IP viene utilizzato per la risoluzione degli indirizzi da nome host a IP.
Server dei nomi secondario	Se non si seleziona Configura DNS automaticamente , digitare l'indirizzo IP del server DNS secondario. Questo indirizzo IP viene utilizzato per la risoluzione degli indirizzi da nome host a IP.
Gateway predefinito	Digitare l'indirizzo del gateway predefinito. Se non si specifica l'indirizzo IP del gateway predefinito, l'interfaccia interna dell'istanza del gateway edge viene impostata come gateway predefinito.
Il lease non ha scadenza	Abilitare questo interruttore per mantenere l'indirizzo IP associato a tale indirizzo MAC per sempre. Se si seleziona questa opzione, il campo Durata lease viene impostato su Infinito.
Durata lease (secondi)	Intervallo di tempo (in secondi) che indica la durata del lease degli indirizzi IP assegnati dal DHCP ai client. La durata del lease predefinita è un giorno (86400 secondi).
Nota Se si seleziona Il lease non ha scadenza , non è possibile specificare una durata del lease.	

- 3 Fare clic su **Salva modifiche**.

Configurazione dell'inoltro DHCP per i gateway edge NSX Data Center for vSphere

La funzionalità di inoltro DHCP fornita da NSX nell'ambiente di VMware Cloud Director consente di sfruttare l'infrastruttura DHCP esistente dall'interno dell'ambiente di VMware Cloud Director senza alcuna interruzione della gestione degli indirizzi IP nell'infrastruttura DHCP esistente. I messaggi DHCP vengono inoltrati dalle macchine virtuali ai server DHCP designati nell'infrastruttura DHCP

fisica. In questo modo, gli indirizzi IP controllati dal software NSX continuano a essere sincronizzati con gli indirizzi IP esistenti negli altri ambienti controllati tramite DHCP.

La configurazione di inoltro DHCP di un gateway edge può elencare diversi server DHCP. Le richieste vengono inviate a tutti i server elencati. Durante l'inoltro della richiesta DHCP da parte di una macchina virtuale, il gateway edge aggiunge l'indirizzo IP di un gateway alla richiesta. Il server DHCP esterno utilizza l'indirizzo di questo gateway per trovare un pool corrispondente e allocare un indirizzo IP per la richiesta. L'indirizzo del gateway deve appartenere a una subnet dell'interfaccia del gateway edge.

È possibile specificare un server DHCP diverso per ogni gateway edge e configurare più server DHCP in ogni gateway edge per fornire il supporto per più domini IP.

Nota

- L'inoltro DHCP non supporta spazi di indirizzi IP sovrapposti.
 - L'inoltro DHCP e il servizio DHCP non possono essere eseguiti contemporaneamente nella stessa vNIC. Se un agente di inoltro è configurato in una vNIC, non è possibile configurare un pool DHCP nelle subnet di tale vNIC. Per ulteriori dettagli, vedere *NSX Administration Guide*.
-

Come specificare una configurazione di inoltro DHCP per un gateway edge NSX Data Center for vSphere

Il software NSX nell'ambiente VMware Cloud Director consente al gateway edge di inoltrare i messaggi del DHCP ai server DHCP esterni al virtual data center dell'organizzazione di VMware Cloud Director. È possibile configurare la funzionalità di inoltro DHCP del gateway edge.

Come descritto nella documentazione *per l'amministratore NSX*, è possibile specificare i server DHCP utilizzando i seguenti elementi esistenti: un set di IP, un blocco di indirizzi IP, un dominio, o una loro combinazione. I messaggi DHCP vengono inoltrati a ogni server DHCP specificato.

È inoltre necessario configurare almeno un agente di inoltro DHCP. Un agente di inoltro DHCP è un'interfaccia nel gateway edge da cui le richieste DHCP vengono inoltrate ai server DHCP esterni.


Prerequisiti


Se si desidera utilizzare un set di IP per specificare un server DHCP, verificare che il set di IP sia disponibile come oggetto di raggruppamento per il gateway edge. Vedere [Creazione di un set di IP da utilizzare nelle regole del firewall e nella configurazione dell'inoltro DHCP](#).

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **DHCP > Inoltro**.

- 3 Utilizzare i campi nella schermata per specificare i server DHCP tramite indirizzi IP, nomi di dominio o set di IP.

Per selezionare uno dei set di IP esistenti, utilizzare il pulsante **Aggiungi** () per cercare i set di IP disponibili.

- 4 Configurare un agente di inoltro DHCP e aggiungerne la configurazione alla tabella nella schermata facendo clic sul pulsante **Aggiungi** () , selezionando un vNIC e l'indirizzo IP del gateway corrispondente, quindi facendo clic su **Mantieni**.

Per impostazione predefinita, l'indirizzo IP del gateway corrisponde all'indirizzo primario del vNIC selezionato. È possibile mantenere il valore predefinito o selezionare un indirizzo alternativo se è disponibile nel vNIC.

- 5 Fare clic su **Salva modifiche**.

Gestione di Network Address Translation in un gateway edge di NSX Data Center for vSphere

Il software NSX Data Center for vSphere nell'ambiente VMware Cloud Director consente ai gateway edge di fornire un servizio NAT. Grazie a questa funzionalità, le organizzazioni possono aumentare la sicurezza e risparmiare riducendo il numero di indirizzi IP pubblici che devono utilizzare.

Il servizio NAT del gateway edge offre la possibilità di assegnare un indirizzo pubblico a una macchina virtuale o a un gruppo di macchine virtuali in una rete privata. Per consentire ai gateway edge di fornire accesso ai servizi in esecuzione in macchine virtuali con indirizzo privato nel virtual data center dell'organizzazione, è necessario configurare regole NAT nei gateway edge. Nel caso più comune, è possibile associare un servizio NAT a un'interfaccia di uplink in un gateway edge nell'ambiente VMware Cloud Director in modo che gli indirizzi nelle reti di virtual data center dell'organizzazione non vengano esposti nella rete esterna.

La configurazione del servizio NAT è suddivisa in regola NAT di origine (SNAT) e regola NAT di destinazione (DNAT). Quando si configura una regola SNAT o DNAT in un gateway edge nell'ambiente di VMware Cloud Director, la regola viene sempre configurata dal punto di vista del virtual data center dell'organizzazione. In particolare, ciò significa che le regole vengono configurate nei modi seguenti:

- **SNAT:** il traffico passa da una macchina virtuale in una rete interna nel virtual data center dell'organizzazione (l'origine) tramite Internet alla rete esterna (la destinazione). Una regola SNAT traduce l'indirizzo IP di origine dei pacchetti in uscita di una rete del virtual data center dell'organizzazione inviati a una rete esterna o a un'altra rete del virtual data center dell'organizzazione.

- DNAT: il traffico passa da Internet (l'origine) a una macchina virtuale all'interno del virtual data center dell'organizzazione (la destinazione). Una regola DNAT converte l'indirizzo IP, e facoltativamente la porta, dei pacchetti ricevuti dalla rete di virtual data center dell'organizzazione provenienti da una rete esterna o da un'altra rete di virtual data center dell'organizzazione.

È possibile configurare regole NAT per creare uno spazio di indirizzi IP privati all'interno del virtual data center dell'organizzazione. Questa configurazione consente di portare uno spazio di indirizzi IP privati da un virtual data center dell'organizzazione a un altro. La configurazione delle regole NAT consente di utilizzare nel virtual data center di un'organizzazione gli stessi indirizzi IP privati delle macchine virtuali utilizzati in un altro virtual data center.

La funzionalità della regola NAT nell'ambiente VMware Cloud Director supporta:

- Creazione di subnet all'interno dello spazio di indirizzi IP privati
- Creazione di più spazi di indirizzi IP privati per un gateway edge
- Configurazione di più regole NAT in più interfacce del gateway edge

Importante Per rendere accessibili le macchine virtuali nella rete di un gateway edge, è necessario configurare sia regole del firewall sia regole NAT nel gateway edge. Per impostazione predefinita, i gateway edge vengono distribuiti con regole del firewall configurate per negare tutto il traffico di rete da e verso le macchine virtuali nelle reti dei gateway edge. NAT è inoltre disattivato per impostazione predefinita nei gateway edge per impedire che i gateway edge convertano gli indirizzi IP del traffico in entrata e in uscita, a meno che non si configuri NAT nei gateway edge. Il tentativo di eseguire il ping di una macchina virtuale in una rete dopo la configurazione di una regola NAT non riesce a meno che non si aggiunga una regola del firewall per consentire il traffico corrispondente.

Aggiunta di una regola SNAT o DNAT

È possibile creare una regola NAT di origine (SNAT) per modificare l'indirizzo IP di origine da pubblico a privato o viceversa. È possibile creare una regola NAT di destinazione (DNAT) per modificare l'indirizzo IP di destinazione da pubblico a privato o viceversa.

Durante la creazione di regole NAT, è possibile specificare gli indirizzi IP originali e convertiti utilizzando i seguenti formati:

- Indirizzo IP, ad esempio 192.0.2.0
- Intervallo di indirizzi IP, ad esempio 192.0.2.0-192.0.2.24
- Indirizzo IP/subnet mask, ad esempio 192.0.2.0/24
- any

Quando si configura una regola SNAT o DNAT in un gateway edge nell'ambiente di VMware Cloud Director, la regola viene sempre configurata dal punto di vista del virtual data center dell'organizzazione. Una regola SNAT converte l'indirizzo IP di origine dei pacchetti inviati da una rete di virtual data center dell'organizzazione a una rete esterna o a un'altra rete di virtual data center dell'organizzazione. Una regola DNAT converte l'indirizzo IP, e facoltativamente la porta, dei pacchetti ricevuti dalla rete di virtual data center dell'organizzazione provenienti da una rete esterna o da un'altra rete di virtual data center dell'organizzazione.

Prerequisiti

È necessario che gli indirizzi IP pubblici siano stati aggiunti all'interfaccia del gateway edge NSX Data Center for vSphere a cui si desidera aggiungere la regola. Per le regole DNAT, è necessario che all'interfaccia del gateway edge sia stato aggiunto l'indirizzo IP originale (pubblico), mentre per le regole SNAT, è necessario che all'interfaccia sia stato aggiunto l'indirizzo IP convertito (pubblico).

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic su **NAT** per visualizzare la schermata Regole NAT.
- 3 In base al tipo di regola NAT che si sta creando, fare clic su **REGOLA DNAT** o **REGOLA SNAT**.
- 4 Configurare una regola NAT di destinazione (dall'esterno verso l'interno).

Opzione	Descrizione
Applicato su	Selezionare l'interfaccia in cui si desidera applicare la regola.
IP/Intervallo originale	Digitare l'indirizzo IP richiesto oppure selezionare l'indirizzo IP allocato nell'elenco. Questo indirizzo deve essere l'indirizzo IP pubblico del gateway edge per il quale si sta configurando la regola DNAT. Nel pacchetto ispezionato, questo indirizzo o intervallo IP è quello visualizzato come indirizzo IP di destinazione del pacchetto. Questi indirizzi di destinazione dei pacchetti sono quelli convertiti dalla regola DNAT.
Protocollo	Selezionare il protocollo a cui applicare la regola. Per applicare la regola a tutti i protocolli, selezionare Qualsiasi .
Porta originale	(Facoltativo) Selezionare la porta o l'intervallo di porte che il traffico in entrata utilizza nel gateway edge per connettersi alla rete interna a cui sono connesse le macchine virtuali. Questa opzione non è disponibile quando il Protocollo è impostato su ICMP o Qualsiasi .
Tipo di ICMP	Quando si seleziona ICMP (un'utilità di segnalazione degli errori e di diagnostica utilizzata tra i dispositivi per comunicare le informazioni sugli errori) in Protocollo , selezionare Tipo di ICMP dal menu a discesa. I messaggi di ICMP vengono identificati dal campo del tipo. Per impostazione predefinita, il tipo di ICMP è impostato su Qualsiasi .

Opzione	Descrizione
IP/Intervallo convertito	Digitare l'indirizzo IP o un intervallo di indirizzi IP in cui verranno convertiti gli indirizzi di destinazione dei pacchetti in entrata. Si tratta degli indirizzi IP di una o più macchine virtuali per le quali si sta configurando la regola DNAT in modo che possano ricevere traffico dalla rete esterna.
Porta convertita	(Facoltativo) Selezionare la porta o l'intervallo di porte a cui si connette il traffico in entrata nelle macchine virtuali della rete interna. Si tratta delle porte in cui la regola DNAT esegue la conversione per i pacchetti in entrata per le macchine virtuali.
Indirizzo IP origine	Se si desidera che la regola venga applicata solo al traffico proveniente da un dominio specifico, immettere un indirizzo IP per questo dominio o un intervallo di indirizzi IP nel formato CIDR. Se si lascia vuota questa casella di testo, la regola DNAT viene applicata a tutti gli indirizzi IP presenti nella subnet locale.
Porta di origine	(Facoltativo) Immettere un numero di porta per l'origine.
Descrizione	(Facoltativo) Immettere una descrizione significativa per la regola DNAT.
Abilitato	Attivare questa opzione per attivare la regola.
Abilita registrazione	Attivare questa opzione per abilitare la registrazione della conversione degli indirizzi eseguita dalla regola.

5 Configurare una regola NAT di origine (dall'interno verso l'esterno).

Opzione	Descrizione
Applicato su	Selezionare l'interfaccia in cui si desidera applicare la regola.
IP di origine/Intervallo originale	Digitare l'indirizzo IP originale o l'intervallo di indirizzi IP da applicare a questa regola oppure selezionare l'indirizzo IP allocato nell'elenco. Si tratta degli indirizzi IP di una o più macchine virtuali per le quali si sta configurando la regola SNAT in modo che possano inviare traffico alla rete esterna.
IP di origine/Intervallo convertito	Digitare l'indirizzo IP richiesto. Questo indirizzo è sempre l'indirizzo IP pubblico del gateway per il quale si sta configurando la regola SNAT. Specifica l'indirizzo IP in cui gli indirizzi (le macchine virtuali) di origine nei pacchetti in uscita vengono convertiti quando inviano il traffico alla rete esterna.
Indirizzo IP destinazione	(Facoltativo) Se si desidera che la regola venga applicata solo per il traffico verso un dominio specifico, immettere un indirizzo IP per questo dominio o un intervallo di indirizzi IP in formato CIDR. Se si lascia vuota questa casella di testo, la regola SNAT viene applicata a tutte le destinazioni esterne alla subnet locale.
Porta di destinazione	(Facoltativo) Immettere un numero di porta per la destinazione.
Descrizione	(Facoltativo) Immettere una descrizione significativa per la regola SNAT.
Abilitato	Attivare questa opzione per attivare la regola.
Abilita registrazione	Attivare questa opzione per abilitare la registrazione della conversione degli indirizzi eseguita dalla regola.

- 6 Fare clic su **Mantieni** per aggiungere la regola alla tabella nella schermata.
- 7 Ripetere i passaggi per configurare regole aggiuntive.
- 8 Fare clic su **Salva modifiche** per salvare le regole nel sistema.

Operazioni successive

Aggiungere le regole del firewall del gateway edge corrispondente per la regola SNAT o DNAT appena configurata. Vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#).

Configurazione del routing avanzata per i gateway edge di NSX Data Center for vSphere

È possibile configurare il routing statico e dinamico nei gateway edge di NSX Data Center for vSphere.

Per abilitare il routing dinamico, configurare un gateway edge avanzato utilizzando il protocollo BGP (Border Gateway Protocol) o il protocollo OSPF (Open Shortest Path First).

Per informazioni dettagliate sulle funzionalità di routing offerte da NSX Data Center for vSphere, vedere la documentazione di NSX Data Center for vSphere.

È possibile specificare il routing statico e dinamico per ciascun gateway edge avanzato. La funzionalità di routing dinamico fornisce le informazioni di inoltro necessarie tra i domini di broadcast di livello 2. Ciò consente di ridurre i domini di broadcast di livello 2 e migliorare l'efficienza di rete e la scalabilità. NSX Data Center for vSphere estende questa capacità alle posizioni dei carichi di lavoro per l'instradamento orizzontale. Questa funzionalità consente una comunicazione tra macchine virtuali più diretta senza il costo o i tempi aggiuntivi necessari per estendere gli hop.

Come specificare le configurazioni di routing predefinite per il gateway edge NSX Data Center for vSphere

È possibile specificare le impostazioni predefinite per il routing statico e il routing dinamico per un gateway edge.

Nota Per rimuovere tutte le impostazioni di routing configurate, utilizzare il pulsante **Cancella configurazione globale** nella parte inferiore della schermata **Configurazione routing**. Questa azione consente di eliminare tutte le impostazioni attualmente specificate nelle schermate secondarie, quali impostazioni di routing predefinite, route statiche, OSPF, BGP e redistribuzione delle route.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.

2 Passare a **Routing > Configurazione routing**.**3** Per abilitare il routing ECMP (Equal Cost Multipath) per questo gateway edge, attivare l'interruttore **ECMP**.

Come descritto nella documentazione per l'*amministrazione di NSX*, ECMP è una strategia di routing che consente l'inoltro del pacchetto dell'hop successivo a una singola destinazione in più percorsi migliori. NSX determina questi percorsi migliori in modo statico, ovvero utilizzando le route statiche configurate, oppure attraverso il risultato di calcoli metrici di protocolli di routing dinamico, come OSPF o BGP. È possibile specificare più percorsi per le route statiche specificando più hop successivi nella schermata Route statiche.

Per ulteriori informazioni su ECMP e NSX, consultare gli argomenti sul routing contenuti in *NSX Troubleshooting Guide*.

4 Specificare le impostazioni per il gateway di routing predefinito.

- a Utilizzare l'elenco a discesa **Applicata su** per selezionare un'interfaccia da cui è possibile raggiungere l'hop successivo indirizzato alla rete di destinazione.

Per visualizzare informazioni dettagliate sull'interfaccia selezionata, fare clic sull'icona delle informazioni blu.

- b Digitare l'indirizzo IP del gateway.
- c Digitare il valore MTU.
- d (Facoltativo) Digitare una descrizione facoltativa.
- e Fare clic su **Salva modifiche**.

5 Specificare le impostazioni di routing dinamico predefinite.

Nota Se nell'ambiente in uso è configurato il servizio VPN IPsec, è consigliabile non utilizzare il routing dinamico.

- a Selezionare un ID router.

È possibile selezionare un ID router nell'elenco o utilizzare l'icona **+** per immetterne uno nuovo. L'ID router è il primo indirizzo IP di uplink del gateway edge che esegue il push delle route al kernel per il routing dinamico.

- b Configurare la registrazione attivando l'interruttore **Abilita registrazione** e selezionando il livello di registrazione.
- c Fare clic su **OK**.

6 Fare clic su **Salva modifiche**.**Operazioni successive**

Aggiungere route statiche. Vedere [Aggiunta di una route statica](#).

Configurare la redistribuzione di route. Vedere [Configurazione delle redistribuzioni di route](#).

Configurare il routing dinamico. Vedere gli argomenti seguenti:

- [Configurazione del protocollo BGP](#)
- [Configurazione del protocollo OSPF](#)

Aggiunta di una route statica


È possibile aggiungere una route statica per una subnet o un host di destinazione.

Se è abilitato ECMP nella configurazione del routing predefinito, è possibile specificare più hop successivi nelle route statiche. Vedere [Come specificare le configurazioni di routing predefinite per il gateway edge NSX Data Center for vSphere](#) per istruzioni sull'attivazione di ECMP.

Prerequisiti

Come descritto nella documentazione di NSX, l'indirizzo IP dell'hop successivo della route statica deve essere presente in una subnet associata a una delle interfacce del gateway edge NSX Data Center for vSphere. In caso contrario, la configurazione di tale route statica non riesce.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Routing > Route statiche**.
- 3 Fare clic sul pulsante **Crea** ().
- 4 Configurare le seguenti opzioni per la route statica:

Opzione	Descrizione
Rete	Digitare la rete con la notazione CIDR.
Hop successivo	Digitare l'indirizzo IP dell'hop successivo. L'indirizzo IP dell'hop successivo deve essere presente in una subnet associata a una delle interfacce del gateway edge. Se è abilitato ECMP, è possibile digitare più hop successivi.
MTU	Modificare il valore massimo di trasmissione per i pacchetti di dati. Il valore MTU non può essere maggiore del valore MTU impostato nell'interfaccia del gateway edge selezionato. È possibile visualizzare il valore MTU impostato nell'interfaccia del gateway edge per impostazione predefinita nella schermata Configurazione routing.
Interfaccia	Facoltativamente, selezionare l'interfaccia del gateway edge in cui si desidera aggiungere una route statica. Per impostazione predefinita, viene selezionata l'interfaccia che corrisponde all'indirizzo dell'hop successivo.
Descrizione	Facoltativamente, digitare una descrizione per la route statica.

- 5 Fare clic su **Salva modifiche**.

Operazioni successive

Configurare una regola NAT per la route statica. Vedere [Aggiunta di una regola SNAT o DNAT](#).

Aggiungere una regola del firewall per consentire al traffico di attraversare la route statica. Vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#).

Configurazione del protocollo OSPF

È possibile configurare il protocollo di routing OSPF (Open Short Path First) per le funzionalità di routing dinamico di un gateway edge NSX Data Center for vSphere. Un'applicazione comune di OSPF in un gateway edge in un ambiente VMware Cloud Director consiste nello scambio di informazioni di routing tra i gateway edge in VMware Cloud Director.

Il gateway edge NSX supporta OSPF, un protocollo IGP (Interior Gateway Protocol) che instrada i pacchetti IP solo all'interno di un singolo dominio di routing. Come descritto nella documentazione *per l'amministratore di NSX*, la configurazione OSPF in un gateway edge NSX consente al gateway edge di scoprire e annunciare route. Il gateway edge utilizza OSPF per raccogliere informazioni sullo stato del collegamento dai gateway edge disponibili e creare una mappa della topologia di rete. La topologia determina la tabella di routing presentata a livello di Internet, consentendo di prendere decisioni di routing in base all'indirizzo IP di destinazione presente nei pacchetti IP.

Di conseguenza, i criteri di routing OSPF forniscono un processo dinamico di bilanciamento del carico di traffico tra route con uguale costo. Una rete OSPF è suddivisa in aree di routing per ottimizzare il flusso del traffico e limitare le dimensioni delle tabelle di routing. Un'area è una raccolta logica di collegamenti, router e reti OSPF con la stessa identificazione di area. Le aree sono identificate da un ID area.

Prerequisiti


È necessario configurare un ID router. [Come specificare le configurazioni di routing predefinite per il gateway edge NSX Data Center for vSphere](#).

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Routing > OSPF**.
- 3 Se OSPF non è attualmente abilitato, utilizzare l'interruttore **OSPF abilitato** per abilitarlo.
- 4 Configurare le impostazioni di OSPF in base alle esigenze della propria organizzazione.

Opzione	Descrizione
Abilita riavvio normale	Specifica che l'inoltro dei pacchetti non deve essere interrotto quando i servizi OSPF vengono riavviati.
Abilita invio predefinito	Consente al gateway edge di annunciarsi come gateway predefinito ai propri peer OSPF.


- 5 (Facoltativo) È possibile fare clic su **Salva modifiche** o continuare con la configurazione delle definizioni di area e delle mappature di interfaccia.

- 6 Aggiungere una definizione di area OSPF facendo clic sul pulsante **Aggiungi** () , specificando nella finestra di dialogo i dettagli della mappatura, quindi facendo clic su **Mantieni**.

Nota Per impostazione predefinita, il sistema configura un'area NSSA (Not-So-Stubby Area) con ID area 51, che viene visualizzata automaticamente nella tabella delle definizioni di area nella schermata OSPF. È possibile modificare o eliminare l'area NSSA.

Opzione	Descrizione
ID area	Digitare un ID area sotto forma di indirizzo IP o numero decimale.
Tipo di area	<p>Selezionare Normale o NSSA.</p> <p>Le aree NSSA impediscono il sovraccarico degli annunci LSA (Link-State Advertisement) esterni ad AS nelle aree NSSA. Tali aree utilizzano il routing predefinito verso le destinazioni esterne. Di conseguenza, le aree NSSA devono essere posizionate in corrispondenza dell'edge di un dominio di routing OSPF. Un'area NSSA può importare route esterne nel dominio di routing OSPF, garantendo in tal modo il servizio di transito a piccoli domini di routing che non fanno parte del dominio di routing OSPF.</p>
Autenticazione area	<p>Selezionare il tipo di autenticazione per OSPF da eseguire a livello di area.</p> <p>Per tutti i gateway edge all'interno dell'area è necessario configurare la stessa autenticazione e la password corrispondente. Affinché l'autenticazione MD5 funzioni, il ricevitore e il trasmettitore devono avere la stessa chiave MD5.</p> <p>Le opzioni disponibili sono:</p> <ul style="list-style-type: none"> ■ Nessuno <p>Non è richiesta alcuna autenticazione.</p> ■ Password <p>Se si seleziona questa opzione, la password specificata nel campo Valore autenticazione area viene inclusa nel pacchetto trasmesso.</p> ■ MD5 <p>Se si seleziona questa opzione, l'autenticazione utilizza la crittografia MD5 (Message Digest tipo 5). Un checksum MD5 viene incluso nel pacchetto trasmesso. Digitare la chiave MD5 nel campo Valore autenticazione area.</p>

- 7 Fare clic su **Salva modifiche**, in modo che le definizioni di area appena configurate siano disponibili per la selezione quando si aggiungono mappature dell'interfaccia.

- 8 Aggiungere una mappatura dell'interfaccia facendo clic sul pulsante **Aggiungi** () , specificando nella finestra di dialogo i dettagli di mappatura, quindi facendo clic su **Mantieni**.

Queste mappature consentono di mappare le interfacce del gateway edge alle aree.

- a Nella finestra di dialogo, selezionare l'interfaccia che si desidera mappare a una definizione di area.

L'interfaccia specifica la rete esterna a cui sono connessi entrambi i gateway edge.

- b Selezionare l'ID area per l'area da mappare all'interfaccia selezionata.
- c (Facoltativo) Modificare i valori predefiniti delle impostazioni di OSPF in modo da personalizzarli per la mappatura di questa interfaccia.

Quando si configura una nuova mappatura, vengono visualizzati i valori predefiniti per queste impostazioni. Nella maggior parte dei casi, è consigliabile mantenere le impostazioni predefinite. Se si modificano le impostazioni, assicurarsi che i peer OSPF utilizzino le stesse impostazioni.

Opzione	Descrizione
Intervallo Hello	Intervallo (in secondi) tra i pacchetti Hello inviati nell'interfaccia.
Intervallo Dead	Intervallo (in secondi) durante il quale è necessario ricevere almeno un pacchetto di Hello da un router adiacente prima che questo venga dichiarato inattivo.
Priorità	Priorità dell'interfaccia. L'interfaccia con la priorità più alta è il router del gateway edge designato.
Costo	Overhead richiesto per inviare pacchetti attraverso l'interfaccia. Il costo di un'interfaccia è inversamente proporzionale alla larghezza di banda dell'interfaccia. Più grande è la larghezza di banda, minore sarà il costo.

- d Fare clic su **Mantieni**.

- 9 Fare clic su **Salva modifiche** nella schermata OSPF.

Operazioni successive

Configurare OSPF negli altri gateway edge con cui si desidera scambiare informazioni di routing.

Aggiungere una regola del firewall che consenta il traffico tra i gateway edge abilitati per OSPF.

Vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#).

Assicurarsi che la redistribuzione delle route e la configurazione del firewall consentano di annunciare le route corrette. Vedere [Configurazione delle redistribuzioni di route](#).

Configurazione del protocollo BGP

È possibile configurare il protocollo BGP (Border Gateway Protocol) per le funzionalità di routing dinamico di un gateway edge NSX Data Center for vSphere.

Come descritto in *NSX Administration Guide*, BGP prende decisioni relative al core routing utilizzando una tabella di prefissi o reti IP che indicano la raggiungibilità della rete tra più sistemi autonomi. Nel campo delle reti, il termine speaker BGP si riferisce a un dispositivo di rete che esegue BGP. Due speaker BGP stabiliscono una connessione prima che qualsiasi informazione di routing venga scambiata. Il termine router adiacente BGP si riferisce a uno speaker BGP che ha stabilito una connessione di questo tipo. Una volta stabilita la connessione, i dispositivi scambiano la route e sincronizzano le rispettive tabelle. Ogni dispositivo invia messaggi keep-alive per mantenere attiva questa relazione.

Procedura


- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Routing > BGP**.
- 3 Se BGP non è attualmente abilitato, utilizzare l'interruttore **Abilita BGP** per abilitarlo.
- 4 Configurare le impostazioni di BGP in base alle esigenze della propria organizzazione.

Opzione	Descrizione
Abilita riavvio normale	Specifica che l'inoltro dei pacchetti non deve essere interrotto quando vengono riavviati i servizi BGP.
Abilita invio predefinito	Consente al gateway edge di annunciarsi come gateway predefinito ai router adiacenti BGP.
AS locale	<p>Obbligatorio. Specificare il numero ID del sistema autonomo (AS) da utilizzare per la funzionalità AS locale del protocollo. Il valore specificato deve essere un numero globalmente univoco compreso tra 1 e 65534.</p> <p>Il sistema AS locale è una funzionalità di BGP. Il sistema assegna il numero AS locale al gateway edge che si sta configurando. Il gateway edge annuncia questo ID quando il gateway edge funge da peer con i router adiacenti BGP in altri sistemi autonomi. Il percorso dei sistemi autonomi che verrebbero attraversati da una route viene utilizzato come una metrica nell'algoritmo di routing dinamico quando si seleziona il percorso migliore verso una destinazione.</p>

- 5 È possibile fare clic su **Salva modifiche** o continuare a configurare le impostazioni per i router adiacenti BGP.

6 Aggiungere una configurazione di router adiacente BGP facendo clic sul pulsante **Aggiungi**



() , specificando nella finestra di dialogo i dettagli del router adiacente e facendo clic su **Mantieni**.

Opzione	Descrizione
Indirizzo IP	Digitare l'indirizzo IP di un router adiacente BGP per questo gateway edge.
AS remoto	Digitare un numero globalmente univoco compreso tra 1 e 65534 per il sistema autonomo a cui il router adiacente BGP appartiene. Questo numero AS remoto viene utilizzato nella voce del router adiacente BGP nella tabella dei router adiacenti BGP del sistema.
Peso	Il peso predefinito per la connessione del router adiacente. Modificare il valore in base alle esigenze della propria organizzazione.
Tempo keep-alive	Frequenza con cui il software invia messaggi keep-alive al proprio peer. La frequenza predefinita è 60 secondi. Impostare il valore appropriato in base alle esigenze della propria organizzazione.
Tempo hold-down	<p>L'intervallo per il quale il software dichiara inattivo un peer dopo che non ha ricevuto un messaggio keep-alive. Questo intervallo di tempo deve essere il triplo dell'intervallo di keep-alive. L'intervallo predefinito è 180 secondi. Impostare il valore appropriato in base alle esigenze della propria organizzazione.</p> <p>Una volta ottenuto il peering tra due router adiacenti BGP, il gateway edge avvia un timer di hold-down. Ogni messaggio keep-alive che riceve dal router adiacente comporta la reimpostazione del timer di hold-down su 0. Se il gateway edge non riesce a ricevere tre messaggi keep-alive consecutivi, in modo che il timer di hold-down raggiunga tre volte l'intervallo di keep-alive, il gateway edge considera inattivo il router adiacente ed elimina le route da tale router adiacente.</p>

Opzione	Descrizione
Password	<p>Se questo router adiacente BGP richiede l'autenticazione, digitare la password di autenticazione.</p> <p>Ogni segmento inviato tramite la connessione tra i router adiacenti viene verificato. È necessario configurare l'autenticazione MD5 con la stessa password su entrambi i router adiacenti BGP. In caso contrario, la connessione tra i router non verrà effettuata.</p>
Filtri BGP	<p>Utilizzare questa tabella per specificare il filtraggio della route utilizzando un elenco di prefissi da questo router adiacente BGP.</p> <p>Attenzione Una regola di tipo <code>blocca tutto</code> viene applicata alla fine dei filtri.</p> <p>Aggiungere un filtro alla tabella facendo clic sull'icona + e configurando le opzioni. Fare clic su Mantieni per salvare ciascun filtro.</p> <ul style="list-style-type: none"> ■ Selezionare la direzione per indicare se si sta filtrando il traffico diretto verso il router adiacente o proveniente dal router adiacente. ■ Selezionare l'azione per indicare se si sta consentendo o negando il traffico. ■ Immettere la rete che si desidera filtrare diretta al router adiacente o proveniente dal router adiacente. Immettere <code>ANY</code> o una rete nel formato CIDR. ■ Immettere il GE prefisso IP e il LE prefisso IP per poter utilizzare le parole chiave <code>le</code> e <code>ge</code> nell'elenco dei prefissi IP.

7 Fare clic su **Salva modifiche** per salvare le configurazioni nel sistema.

Operazioni successive

Configurare BGP negli altri gateway edge con cui si desidera scambiare informazioni di routing.



Aggiungere una regola del firewall che consenta il traffico proveniente dai gateway edge con BGP configurato o diretto verso i gateway edge con BGP configurato. Per ulteriori informazioni, vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#).

Configurazione delle redistribuzioni di route

Per impostazione predefinita, il router condivide le route solo con altri router che eseguono lo stesso protocollo. Dopo aver configurato un ambiente multi-protocollo, è necessario configurare la redistribuzione delle route per ottenere la condivisione delle route tra più protocolli. È possibile configurare la redistribuzione delle route per un gateway edge NSX Data Center for vSphere.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Routing > Redistribuzione route**.

- 3 Utilizzare gli interruttori dei protocolli per attivare i protocolli per cui si desidera abilitare la redistribuzione della route.
- 4 Aggiungere i prefissi IP alla tabella nella schermata.
 - a Fare clic sul pulsante **Aggiungi** ().
 - b Digitare il nome e l'indirizzo IP della rete nel formato CIDR.
 - c Fare clic su **Mantieni**.
- 5 Specificare i criteri di redistribuzione per ogni prefisso IP facendo clic sul pulsante **Aggiungi** () , specificando i criteri nella finestra di dialogo e facendo clic su **Mantieni**.

Le voci presenti nella tabella vengono elaborate in sequenza. Utilizzare la freccia su e la freccia giù per modificare la sequenza.

Opzione	Descrizione
Nome prefisso	Selezionare un prefisso IP specifico a cui applicare questi criteri o selezionare Qualsiasi per applicare i criteri a tutte le route della rete.
Protocollo learner	Selezionare il protocollo che dovrà individuare le route provenienti da altri protocolli in base a questi criteri di redistribuzione.
Consenti apprendimento da	Selezionare i tipi di rete da cui possono essere individuate route per il protocollo selezionato nell'elenco Protocollo learner .
Azione	Scegliere se consentire o negare la redistribuzione dai tipi di rete selezionati.

- 6 Fare clic su **Salva modifiche**.

Bilanciamento del carico con NSX Data Center for vSphere

Il bilanciamento del carico distribuisce le richieste di servizio in entrata tra più server in modo da rendere la distribuzione del carico trasparente per gli utenti. Il bilanciamento del carico fornisce elevata disponibilità all'applicazione e consente di ottimizzare l'utilizzo delle risorse, massimizzando la velocità effettiva, riducendo al minimo il tempo di risposta ed evitando il sovraccarico.

Informazioni sul bilanciamento del carico

Il bilanciamento del carico distribuisce le richieste di servizio in entrata tra più server in modo da rendere la distribuzione del carico trasparente per gli utenti. Il bilanciamento del carico consente di ottimizzare l'utilizzo delle risorse, massimizzando la velocità effettiva, riducendo al minimo il tempo di risposta ed evitando il sovraccarico.

Il bilanciamento del carico NSX supporta due motori di bilanciamento del carico. Il bilanciamento del carico di livello 4 è basato su pacchetti e fornisce un'elaborazione con percorso rapido. Il bilanciamento del carico di livello 7 è basato su socket e supporta strategie di gestione del traffico avanzate e attenuazione DDOS per i servizi back-end.

Il bilanciamento del carico per un gateway edge NSX Data Center for vSphere viene configurato nell'interfaccia esterna perché il gateway edge esegue il bilanciamento del carico del traffico in entrata dalla rete esterna. Quando si configurano server virtuali per il bilanciamento del carico, specificare uno degli indirizzi IP disponibili presenti nel VDC dell'organizzazione.

Concetti e strategie del bilanciamento del carico

Una strategia di bilanciamento del carico basato su pacchetti viene implementata a livello di TCP e UDP. Il bilanciamento del carico basato su pacchetti non interrompe la connessione e non invia l'intera richiesta al buffer. Dopo la modifica del pacchetto lo invia invece direttamente al server selezionato. Le sessioni TCP e UDP vengono gestite nel bilanciamento del carico in modo che i pacchetti di una singola sessione vengano indirizzati allo stesso server. È possibile selezionare Accelerazione abilitata sia nella configurazione globale sia nella configurazione del server virtuale appropriato per abilitare il bilanciamento del carico basato su pacchetti.

Una strategia di bilanciamento del carico basato su socket viene implementata oltre all'interfaccia del socket. Vengono stabilite due connessioni per una singola richiesta, ovvero una connessione verso il client e una verso il server. La connessione verso il server viene stabilita dopo la selezione del server. Per l'implementazione basata su socket HTTP, l'intera richiesta viene ricevuta prima di inviarla al server selezionato con modifica L7 facoltativa. Per l'implementazione basata su socket HTTPS, le informazioni di autenticazione vengono scambiate nella connessione verso il client o nella connessione verso il server. Il bilanciamento del carico basato su socket è la modalità predefinita per i server virtuali TCP, HTTP e HTTPS.

I concetti chiave del bilanciamento del carico NSX sono server virtuale, pool di server, membro del pool di server e monitor del servizio.

Server virtuale

Astrazione di un servizio di applicazioni, rappresentata da una combinazione univoca di IP, porta, protocollo e profilo di applicazione come TCP o UDP.

Pool di server

Gruppo di server back-end.

Membro del pool di server

Rappresenta il server back-end come membro di un pool.

Monitor del servizio

Definisce la modalità di verifica dello stato di integrità di un server back-end.

Profilo applicazione

Rappresenta TCP, UDP, persistenza e configurazione del certificato per una determinata applicazione.

Panoramica della configurazione

Si inizia impostando opzioni globali per il bilanciamento del carico. Si crea quindi un pool di server contenente membri del server back-end e si associa un monitor del servizio al pool per gestire e condividere i server back-end in modo efficiente.

Si crea quindi un profilo di applicazione per definire il comportamento comune dell'applicazione in un bilanciamento del carico, ad esempio SSL client, SSL server, X-Forwarded-For (XFF) o persistenza. La persistenza invia richieste successive con caratteristiche simili, ad esempio un indirizzo IP di origine o un cookie deve essere distribuito allo stesso membro del pool, senza eseguire l'algoritmo di bilanciamento del carico. Il profilo dell'applicazione può essere riutilizzato nei server virtuali.

Si crea quindi una regola dell'applicazione facoltativa per configurare impostazioni specifiche dell'applicazione per la gestione del traffico, ad esempio la corrispondenza di un determinato URL o nome host, in modo che richieste diverse possano essere gestite da pool diversi.

Successivamente si crea un monitor del servizio specifico dell'applicazione oppure è possibile utilizzare un monitor del servizio esistente se soddisfa le proprie esigenze.

Facoltativamente, è possibile creare una regola di applicazione per supportare le funzionalità avanzate dei server virtuali L7. Alcuni casi d'uso per le regole delle applicazioni includono passaggio di contenuti, modifica dell'intestazione, regole di sicurezza e protezione DOS.

Infine, si crea un server virtuale che connette il pool di server, il profilo dell'applicazione e tutte le eventuali regole delle applicazioni.

Quando il server virtuale riceve una richiesta, l'algoritmo di bilanciamento del carico valuta la configurazione del membro del pool e lo stato di runtime. L'algoritmo calcola quindi il pool appropriato per distribuire il traffico che include uno o più membri. La configurazione del membro del pool include impostazioni quali il volume, il numero massimo di connessioni e lo stato della condizione. Lo stato di runtime include informazioni sulle connessioni correnti, sul tempo di risposta e sullo stato di controllo di integrità. I metodi di calcolo possono essere Round Robin, Weighted Round Robin, Least Connection, Source IP Hash, Weighted Least Connection, URL, URI o intestazione HTTP.

Ogni pool viene monitorato dal monitor del servizio associato. Quando il bilanciamento del carico rileva un problema relativo a un membro del pool, viene contrassegnato come Non raggiungibile. Quando si sceglie un membro del pool dal pool di server, viene selezionato solo il server raggiungibile. Se il pool di server non è configurato con un monitor del servizio, tutti i membri del pool sono considerati raggiungibili.

Configurazione del servizio di bilanciamento del carico

I parametri della configurazione globale del bilanciamento del carico includono l'abilitazione complessiva, la selezione del motore di livello 4 o livello 7 e l'indicazione dei tipi di evento da registrare.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Bilanciamento del carico > Configurazione globale**.
- 3 Selezionare le opzioni che si desidera abilitare:

Opzione	Azione
Stato	<p>Abilitare il bilanciamento del carico facendo clic sull'icona di attivazione/disattivazione.</p> <p>Abilitare Accelerazione abilitata per configurare il bilanciamento del carico in modo che utilizzi il motore L4 più veloce anziché il motore L7. Poiché l'indirizzo VIP TCP L4 viene elaborato prima del firewall del gateway edge, non è necessaria alcuna regola per consentire il firewall.</p> <hr/> <p>Nota Gli indirizzi VIP L7 per HTTP e HTTPS vengono elaborati dopo il firewall. Se non si abilita l'accelerazione, è pertanto necessaria una regola del firewall del gateway edge per consentire l'accesso all'indirizzo VIP L7 per tali protocolli. Se si abilita l'accelerazione e il pool di server è in modalità non trasparente, viene aggiunta una regola SNAT. È pertanto necessario assicurarsi che il firewall sia abilitato nel gateway edge.</p>
Abilita registrazione	Abilitare la registrazione in modo che il bilanciamento del carico del gateway edge raccolga i registri del traffico.
Livello di registrazione	Scegliere il livello di gravità degli eventi da raccogliere nei registri.

- 4 Fare clic su **Salva modifiche**.

Operazioni successive

Configurare i profili di applicazione per il bilanciamento del carico. Vedere [Creazione di un profilo di applicazione](#).


Creazione di un profilo di applicazione

Un profilo di applicazione consente di definire il comportamento del bilanciamento del carico per un particolare tipo di traffico di rete. Dopo aver configurato un profilo, è possibile associarlo a un server virtuale. Il server virtuale elabora quindi il traffico in base ai valori specificati nel profilo. L'utilizzo di profili consente di ottimizzare il controllo della gestione del traffico di rete, rendendo le attività di gestione del traffico più semplici ed efficienti.

Quando si crea un profilo per il traffico HTTPS, sono consentiti i seguenti modelli di traffico HTTPS:

- Client -> HTTPS -> LB (termina SSL) -> HTTP -> server
- Client -> HTTPS -> LB (termina SSL) -> HTTPS -> server
- Client -> HTTPS-> LB (passthrough SSL) -> HTTPS -> server
- Client -> HTTP-> LB -> HTTP -> server

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Bilanciamento del carico > Profili di applicazione**.
- 3 Fare clic sul pulsante **Crea** ()
- 4 Immettere un nome per il profilo.
- 5 Configurare il profilo di applicazione.

Opzione	Descrizione
Tipo	Selezionare il tipo di protocollo utilizzato per inviare le richieste al server. L'elenco dei parametri obbligatori dipende dal protocollo selezionato. Non è possibile immettere parametri non applicabili al protocollo selezionato. Tutti gli altri parametri sono obbligatori.
Abilita passthrough SSL	Fare clic su questa opzione per abilitare il passthrough dell'autenticazione SSL nel server virtuale. In case contrario, l'autenticazione SSL viene eseguita all'indirizzo di destinazione.
URL di reindirizzamento HTTP	(HTTP e HTTPS) Immettere l'URL a cui deve essere reindirizzato il traffico che arriva all'indirizzo di destinazione.

Opzione	Descrizione
Salvataggio permanente	<p>Specificare un meccanismo di salvataggio permanente per il profilo.</p> <p>Il salvataggio permanente tiene traccia e archivia i dati della sessione, ad esempio il membro del pool specifico che ha gestito la richiesta di un client. Ciò garantisce che le richieste del client vengano indirizzate allo stesso membro del pool durante l'intera durata di una sessione o durante le sessioni successive. Le opzioni sono:</p> <ul style="list-style-type: none"> ■ IP origine <p>Il salvataggio permanente di IP origine tiene traccia delle sessioni in base all'indirizzo IP di origine. Quando un client richiede una connessione a un server virtuale che supporta il salvataggio permanente dell'affinità dell'indirizzo di origine, il bilanciamento del carico verifica se tale client si è connesso in precedenza. In questo caso, reindirizza il client allo stesso membro del pool.</p> ■ MSRDP <p>(Solo TCP) Il salvataggio permanente di Microsoft Remote Desktop Protocol (MSRDP) garantisce il salvataggio permanente delle sessioni tra client e server Windows in cui viene eseguito il servizio Microsoft Remote Desktop Protocol (RDP). È consigliabile abilitare il salvataggio permanente di MSRDP quando si crea un pool di bilanciamento del carico composto da membri che eseguono un sistema operativo guest Windows Server, in cui tutti i membri appartengono a un cluster Windows e partecipano a una directory di sessione Windows.</p> ■ ID sessione SSL <p>La persistenza di ID sessione SSL è disponibile quando si abilita il passthrough SSL. La persistenza di ID sessione SSL garantisce che le connessioni ripetute dello stesso client vengano inviate allo stesso server. La persistenza dell'ID sessione consente l'uso della ripresa della sessione SSL, che permette di risparmiare tempo di elaborazione sia per il client sia per il server.</p>
Nome cookie	<p>(HTTP e HTTPS) Se si specifica Cookie come meccanismo di persistenza, immettere il nome del cookie. Il salvataggio permanente di tipo Cookie utilizza un cookie per identificare in modo univoco la sessione la prima volta che un client accede al sito. Il bilanciamento del carico fa riferimento a questo cookie durante la connessione delle richieste successive nella sessione, in modo da indirizzarle tutte allo stesso server virtuale.</p>

Opzione	Descrizione
Modalità	<p>Selezionare la modalità di inserimento del cookie. Sono supportate le seguenti modalità:</p> <ul style="list-style-type: none"> ■ Inserisci <p>Il gateway edge invia un cookie. Se il server invia uno o più cookie, il client riceve un cookie supplementare (i cookie del server più il cookie del gateway edge). Se il server non invia alcun cookie, il client riceverà soltanto il cookie del gateway edge.</p> ■ Prefisso <p>Selezionare questa opzione se il client non supporta più di un cookie.</p> <p>Nota Tutti i browser accettano più cookie. Tuttavia, potrebbe essere presente un'applicazione proprietaria basata su un client proprietario che supporta un solo cookie. Il server Web invia il proprio cookie normalmente. Il gateway edge inserisce (come prefisso) le informazioni relative al proprio cookie nel valore del cookie del server. Queste informazioni aggiuntive sul cookie vengono rimosse quando il gateway edge le invia al server.</p> ■ Sessione app Per questa opzione, il server non invia un cookie. Invia invece le informazioni della sessione utente come URL. Ad esempio, <code>http://example.com/admin/UpdateUserServlet;jsessionid=0I24B9ASD7BSSD</code>, in cui <code>jsessionid</code> corrisponde all'informazione della sessione utente e viene utilizzato per la persistenza. Non è possibile consultare la tabella di salvataggio permanente di Sessione app per la risoluzione dei problemi.
Scade tra (secondi)	<p>Immettere un intervallo di tempo in secondi durante il quale il salvataggio permanente rimane attivo. Il valore deve essere un numero intero positivo compreso nell'intervallo da 1 a 86400.</p> <p>Nota Per il bilanciamento del carico L7 con salvataggio permanente dell'indirizzo IP di origine TCP, la voce salvataggio permanente scade se non vengono stabilite nuove connessioni TCP per un determinato periodo di tempo, anche se le connessioni esistenti sono ancora attive.</p>
Inserisci intestazione X-Forwarded-For HTTP	<p>(HTTP e HTTPS) Selezionare Inserisci intestazione X-Forwarded-For HTTP per identificare l'indirizzo IP di origine di un client che si connette a un server Web tramite il bilanciamento del carico.</p> <p>Nota L'utilizzo di questa intestazione non è supportato se è stato abilitato il passthrough SSL.</p>
Abilita SSL lato pool	<p>(Solo HTTPS) Selezionare Abilita SSL lato pool per definire il certificato, le autorità di certificazione o i CRL utilizzati per l'autenticazione del bilanciamento del carico sul lato server nella scheda Certificati pool.</p>

- 6 (Solo HTTPS) Configurare i certificati da utilizzare con il profilo di applicazione. Se i certificati necessari non esistono, è possibile crearli nella scheda **Certificati**.

Opzione	Descrizione
Certificati server virtuale	Selezionare il certificato, le autorità di certificazione o i CRL utilizzati per decrittografare il traffico HTTPS.
Certificati pool	Definire il certificato, le autorità di certificazione o i CRL utilizzati per l'autenticazione del bilanciamento del carico sul lato server. Nota Selezionare Abilita SSL lato pool per abilitare questa scheda.
Crittografia	Selezionare gli algoritmi di crittografia (o suite di crittografia) negoziati durante l'handshake SSL/TLS.
Autenticazione client	Specificare se l'autenticazione client deve essere ignorata o obbligatoria. Nota Se viene impostata su Obbligatoria , il client deve fornire un certificato dopo la richiesta. In caso contrario, l'handshake viene annullato.

- 7 Per salvare le modifiche, fare clic su **Mantieni**.


Operazioni successive

Aggiungere monitor del servizio per il bilanciamento del carico per definire i controlli di integrità per i diversi tipi di traffico di rete. Vedere [Creazione di un monitor del servizio](#).

Creazione di un monitor del servizio

È possibile creare un monitor del servizio per definire i parametri di controllo dell'integrità di un particolare tipo di traffico di rete. Quando si associa un monitor del servizio a un pool, i membri del pool vengono monitorati in base ai parametri di tale monitor.

Procedura

- Aprire i servizi gateway edge.
 - Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- Passare a **Bilanciamento del carico** > **Monitoraggio del servizio**.
- Fare clic sul pulsante **Crea** ()
- Immettere un nome per il monitor del servizio.
- (Facoltativo) Configurare le opzioni seguenti per il monitor del servizio:

Opzione	Descrizione
Intervallo	Immettere l'intervallo in cui un server deve essere monitorato utilizzando il Metodo specificato.
Timeout	Immettere il tempo massimo in secondi entro il quale si deve ricevere una risposta dal server.

Opzione	Descrizione
Tentativi massimi	Immettere il numero massimo di tentativi non riusciti consecutivi del Metodo di monitoraggio specificato dopo i quali il server viene dichiarato inattivo.
Tipo	Selezionare la modalità con cui si desidera inviare la richiesta di controllo dell'integrità al server, ovvero HTTP, HTTPS, TCP, ICMP o UDP. A seconda del tipo selezionato, le opzioni rimanenti nella finestra di dialogo Nuovo monitor del servizio sono attivate o disattivate.
Previsto	(HTTP e HTTPS) Immettere la stringa che il monitor prevede di trovare nella riga dello stato della risposta HTTP o HTTPS (ad esempio, HTTP/1.1).
Metodo	(HTTP e HTTPS) Selezionare il metodo da utilizzare per rilevare lo stato del server.
URL	(HTTP e HTTPS) Immettere l'URL da utilizzare nella richiesta dello stato del server. Nota Se si seleziona il metodo POST, è necessario specificare un valore per Invia .
Invia	(HTTP, HTTPS, UDP) Immettere i dati da inviare.
Ricevi	(HTTP, HTTPS e UDP) Immettere la stringa che deve essere presente nel contenuto della risposta. Nota Se non viene trovata una corrispondenza con Previsto , il monitor non tenta di trovare la corrispondenza con il contenuto di Ricevi .
Estensione	(TUTTO) Immettere i parametri avanzati del monitor, ad esempio coppie chiave = valore. Ad esempio, avviso=10 indica che se un server non risponde entro 10 secondi, il relativo stato viene impostato su avviso. Tutte le voci dell'estensione devono essere separate da un carattere di ritorno a capo. Ad esempio: <pre><extension>delay=2 critical=3 escape</extension></pre>

6 Per salvare le modifiche, fare clic su **Mantieni**.

Esempio: Estensioni supportate per ciascun protocollo

Tabella 5-4. Estensioni per i protocolli HTTP/HTTPS

Estensione del monitor	Descrizione
no-body	Non attende il corpo di un documento e arresta la lettura dopo l'intestazione HTTP/HTTPS. Nota Una richiesta HTTP GET o HTTP POST viene comunque inviata. Non si tratta di un metodo HEAD.
max-age= <i>SECONDS</i>	Avvisa quando un documento è più vecchio di <i>SECONDS</i> . Il numero può essere espresso nel formato 10m per i minuti, 10h per le ore o 10d per i giorni.
content-type= <i>STRING</i>	Specifica un tipo di multimedia con intestazione Content-Type nelle chiamate POST.

Tabella 5-4. Estensioni per i protocolli HTTP/HTTPS (continua)

Estensione del monitor	Descrizione
linespan	Consente alla stringa regex di estendersi su nuove righe (deve precedere -r o -R).
regex= <i>STRING</i> o ereg= <i>STRING</i>	Cerca il valore <i>STRING</i> regex nella pagina.
eregi= <i>STRING</i>	Cerca nella pagina il valore <i>STRING</i> regex senza distinzione tra maiuscole e minuscole.
invert-regex	Restituisce CRITICAL quando trova una corrispondenza e OK quando non la trova.
proxy-authorization= <i>AUTH_PAIR</i>	Specifica nome utente:password nei server proxy con autenticazione di base.
useragent= <i>STRING</i>	Invia la stringa nell'intestazione HTTP come <i>User Agent</i> .
header= <i>STRING</i>	Invia tutti gli altri tag nell'intestazione HTTP. Utilizzarla più volte per ulteriori intestazioni.
onredirect=ok warning critical follow sticky stickyport	Indica come gestire le pagine reindirizzate. <i>sticky</i> è simile a <i>follow</i> ma corrisponde all'indirizzo IP specificato. <i>stickyport</i> garantisce che la porta rimanga invariata.
pagesize= <i>INTEGER:INTEGER</i>	Specifica le dimensioni minima e massima della pagina espresse in byte.
warning=DOUBLE	Specifica il tempo di risposta in secondi trascorso il quale viene restituito uno stato di avviso.
critical=DOUBLE	Specifica il tempo di risposta in secondi trascorso il quale viene restituito uno stato critico.

Tabella 5-5. Estensioni solo per il protocollo HTTPS

Estensione del monitor	Descrizione
sni	Abilita il supporto dell'estensione del nome host SSL/TLS (SNI).
certificate= INTEGER	Specifica il numero minimo di giorni per cui un certificato deve essere valido. La porta predefinita è la 443. Quando viene utilizzata questa opzione, l'URL non viene controllato.
authorization= <i>AUTH_PAIR</i>	Specifica nome utente:password nei siti con autenticazione di base.

Tabella 5-6. Estensioni per il protocollo TCP

Estensione del monitor	Descrizione
escape	Consente l'utilizzo di \n, \r, \t o \ in una stringa send o quit. Deve precedere un'opzione send o quit. Per impostazione predefinita, non viene aggiunto alcun elemento alla stringa send e \r\n viene aggiunto alla fine della stringa quit.
all	Specifica tutte le stringhe previste che devono trovarsi in una risposta del server. Per impostazione predefinita, viene utilizzato any.
quit=STRING	Invia una stringa al server per chiudere correttamente la connessione.
refuse=ok warn crit	Accetta i rifiuti TCP con stato ok, warn o crit. Per impostazione predefinita, utilizza lo stato crit.
mismatch=ok warn crit	Accetta mancate corrispondenze della stringa prevista con stato ok, warn o crit. Per impostazione predefinita, utilizza lo stato warn.
jail	Nasconde l'output del socket TCP.
maxbytes=INTEGER	Chiude la connessione quando viene ricevuto un numero di byte superiore a quello specificato.
delay=INTEGER	Attende il numero di secondi specificato tra l'invio della stringa e il polling di una risposta.
certificate=INTEGER[,INTEGER]	Specifica il numero minimo di giorni per cui un certificato deve essere valido. Il primo valore è #days per avviso e il secondo valore è critico (se non specificato - 0).
ssl	Utilizza SSL per la connessione.
warning=DOUBLE	Specifica il tempo di risposta in secondi trascorso il quale viene restituito uno stato di avviso.
critical=DOUBLE	Specifica il tempo di risposta in secondi trascorso il quale viene restituito uno stato critico.


Operazioni successive

Aggiungere pool di server per il bilanciamento del carico. Vedere [Aggiunta di un pool di server per il bilanciamento del carico](#).

Aggiunta di un pool di server per il bilanciamento del carico


È possibile aggiungere un pool di server per gestire e condividere server backend in modo flessibile ed efficiente. Un pool gestisce i metodi di distribuzione del bilanciamento del carico e dispone di un monitor del servizio collegato per i parametri del controllo di integrità.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Bilanciamento del carico > Pool**.
- 3 Fare clic sul pulsante **Crea** ().
- 4 Digitare un nome e, facoltativamente, una descrizione per il pool del bilanciamento del carico.
- 5 Selezionare un metodo di bilanciamento per il servizio dal menu a discesa **Algoritmo**:

Opzione	Descrizione
ROUND ROBIN	Ciascun server viene utilizzato in sequenza, in base al volume assegnato. Quando il tempo di elaborazione del server è distribuito in modo uniforme, questo è l'algoritmo che garantisce le prestazioni migliori.
HASH IP	Seleziona un server in base all'hash dell'indirizzo IP di origine e destinazione di ciascun pacchetto.
LEASTCONN	Distribuisce le richieste dei client a più server, in base al numero di connessioni già aperte sul server. Le nuove connessioni vengono inviate al server con il minor numero di connessioni aperte.
URI	La parte sinistra dell'URI (prima del punto interrogativo) è elaborata e divisa per il volume totale dei server in esecuzione. Il risultato stabilisce quale server riceve la richiesta. Questa opzione garantisce che l'URI punti sempre allo stesso server, sempre che il server non sia disattivato.
HTTPHEADER	In ciascuna richiesta HTTP viene cercato il nome dell'intestazione HTTP. Nel nome dell'intestazione tra parentesi non viene fatta distinzione tra maiuscole e minuscole, in modo simile alla funzione ACL 'hdr()'. Se l'intestazione è assente o non contiene alcun valore, viene applicato l'algoritmo round robin. Il parametro dell'algoritmo HTTP HEADER ha un'unica opzione <code>headerName=<name></code> . Ad esempio, è possibile utilizzare host come parametro dell'algoritmo HTTP HEADER.
URL	Nella stringa di query di ciascuna richiesta HTTP GET viene cercato il parametro dell'URL specificato nell'argomento. Se il parametro è seguito da un segno di uguale (=) e un valore, il valore viene elaborato e diviso per il peso totale dei server in esecuzione. Il risultato stabilisce quale server riceve 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 server sia attivato o disattivato. Se non viene trovato alcun valore o parametro, viene applicato un algoritmo round robin. Il parametro dell'algoritmo dell'URL ha un'unica opzione <code>urlParam=<url></code> .

6 Aggiungere membri al pool.

- a Fare clic sul pulsante **Aggiungi** ().
- b Immettere il nome per il membro del pool.
- c Immettere l'indirizzo IP del membro del pool.
- d Inserire la porta in cui il membro riceverà il traffico dal bilanciamento del carico.
- e Inserire la porta di monitoraggio in cui il membro riceverà le richieste di monitoraggio dell'integrità.
- f Nella casella di testo **Peso**, specificare la percentuale di traffico che questo membro dovrà gestire. Deve essere un numero intero compreso nell'intervallo da 1 a 256.
- g (Facoltativo) Nella casella di testo **Connessioni massime**, digitare il numero massimo di connessioni simultanee che il membro è in grado di gestire.

Quando il numero di richieste in entrata supera il valore massimo, le richieste vengono messe in coda e il bilanciamento del carico attende che venga rilasciata una connessione.
- h (Facoltativo) Nella casella di testo **Connessioni minime**, digitare il numero minimo di connessioni simultanee che un membro deve sempre accettare.
- i Fare clic su **Mantieni** per aggiungere il nuovo membro al pool.

Il completamento dell'operazione può richiedere un minuto.

7 (Facoltativo) Per rendere gli indirizzi IP client visibili per i server back-end, selezionare **Trasparente**.

Quando l'opzione **Trasparente** non è selezionata (il valore predefinito), i server back-end interpretano l'indirizzo IP dell'origine del traffico come indirizzo IP interno del bilanciamento del carico.

Quando l'opzione **Trasparente** è selezionata, l'indirizzo IP di origine è l'indirizzo IP effettivo del client e il gateway edge deve essere impostato come gateway predefinito per garantire che i pacchetti restituiti passino attraverso il gateway edge.

8 Per salvare le modifiche, fare clic su **Mantieni**.


Operazioni successive

Aggiungere server virtuali per il bilanciamento del carico. Un server virtuale dispone di un indirizzo IP pubblico e gestisce tutte le richieste client in entrata. Vedere [Aggiunta di un server virtuale](#).

Aggiunta di una regola di applicazione

È possibile scrivere una regola di applicazione per modificare e gestire direttamente il traffico dell'applicazione IP.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Bilanciamento del carico** > **Regole di applicazione**.
- 3 Fare clic sul pulsante **Aggiungi** ().

+
- 4 Immettere il nome della regola di applicazione.
- 5 Immettere lo script della regola di applicazione.
 Per informazioni sulla sintassi della regola di applicazione, vedere <http://cbonte.github.io/haproxy-dconv/2.2/configuration.html>.
- 6 Per salvare le modifiche, fare clic su **Mantieni**.

Operazioni successive


Associare la nuova regola di applicazione a un server virtuale aggiunto per il bilanciamento del carico. Vedere [Aggiunta di un server virtuale](#).

Aggiunta di un server virtuale

Aggiungere un'interfaccia uplink o interna del gateway edge NSX Data Center for vSphere come server virtuale. Un server virtuale dispone di un indirizzo IP pubblico e gestisce tutte le richieste client in entrata.

Per impostazione predefinita, il bilanciamento del carico chiude la connessione TCP del server dopo ciascuna richiesta del client.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **Bilanciamento del carico** > **Server virtuali**.
- 3 Fare clic sul pulsante **Aggiungi** ().

+
- 4 Nella scheda **Generale**, configurare le seguenti opzioni per il server virtuale:

Opzione	Descrizione
Abilita server virtuale	Fare clic per abilitare il server virtuale.
Abilita accelerazione	Fare clic per abilitare l'accelerazione.
Profilo applicazione	Selezionare un profilo dell'applicazione da associare al server virtuale.
Nome	Digitare un nome per il server virtuale.

Opzione	Descrizione
Descrizione	Digitare una descrizione facoltativa per il server virtuale.
Indirizzo IP	Digitare o sfogliare per selezionare l'indirizzo IP su cui è in ascolto il bilanciamento del carico.
Protocollo	Selezionare il protocollo accettato dal server virtuale. È necessario selezionare lo stesso protocollo utilizzato dal Profilo applicazione selezionato.
Porta	Digitare il numero di porta su cui il bilanciamento del carico sta in ascolto.
Pool predefinito	Scegliere il pool di server che verrà utilizzato dal bilanciamento del carico.
Limite connessione	(Facoltativo) Digitare il numero massimo di connessioni simultanee che il server virtuale può elaborare.
Limite velocità di connessione (CPS)	(Facoltativo) Digitare il numero massimo di nuove richieste di connessione in entrata al secondo.

- 5 (Facoltativo) Per associare regole di applicazione al server virtuale, fare clic sulla scheda **Avanzate** e completare i passaggi seguenti:

- a Fare clic sul pulsante **Aggiungi** ()

Verranno visualizzate le regole di applicazione create per il bilanciamento del carico. Se necessario, aggiungere regole di applicazione per il bilanciamento del carico. Vedere [Aggiunta di una regola di applicazione](#).

- 6 Per salvare le modifiche, fare clic su **Mantieni**.

Operazioni successive

Creare una regola del firewall del gateway edge per consentire il traffico verso il nuovo server virtuale (l'indirizzo IP di destinazione). Vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#)

Configurazione dell'accesso sicuro tramite VPN in un gateway edge di NSX Data Center for vSphere

È possibile configurare le funzionalità VPN fornite dal software NSX Data Center for vSphere nei gateway edge di NSX Data Center for vSphere. È possibile configurare connessioni VPN al virtual data center dell'organizzazione utilizzando un tunnel SSL VPN-Plus, un tunnel VPN IPsec o un tunnel VPN L2.

Come descritto in *NSX Administration Guide*, il gateway edge NSX supporta i seguenti servizi VPN:

- SSL VPN-Plus, che consente agli utenti remoti di accedere alle applicazioni aziendali private.
- VPN IPsec, che offre la connettività da sito a sito tra un gateway edge NSX e siti remoti che dispongono di NSX oppure di router hardware o gateway VPN di terze parti.

- VPN L2, che permette l'estensione del virtual data center dell'organizzazione consentendo alle macchine virtuali di mantenere la connettività di rete utilizzando lo stesso indirizzo IP in aree geografiche diverse.

In un ambiente VMware Cloud Director, è possibile creare tunnel VPN tra:

- Reti del virtual data center dell'organizzazione nella stessa organizzazione
- Reti del virtual data center dell'organizzazione appartenenti a organizzazioni diverse
- La rete del virtual data center dell'organizzazione e una rete esterna

Nota VMware Cloud Director non supporta più tunnel VPN tra gli stessi due gateway edge. Se esiste già un tunnel tra due gateway edge e si desidera aggiungere un'altra subnet al tunnel, eliminare il tunnel VPN esistente e crearne uno nuovo che includa la nuova subnet.

Dopo avere configurato i tunnel VPN per un gateway edge, è possibile utilizzare un client VPN da una posizione remota per connettersi al virtual data center dell'organizzazione supportato da tale gateway edge.

Configurazione di SSL VPN-Plus

I servizi SSL VPN-Plus per un gateway edge NSX Data Center for vSphere dell'ambiente VMware Cloud Director consentono agli utenti remoti di connettersi in modo sicuro alle applicazioni e alle reti private dei virtual data center dell'organizzazione supportati da tale gateway edge. È possibile configurare vari servizi SSL VPN-Plus nel gateway edge.

Nell'ambiente VMware Cloud Director, la funzionalità SSL VPN-Plus del gateway edge supporta la modalità di accesso di rete. Gli utenti remoti devono installare un client SSL per rendere le connessioni protette e accedere alle reti e alle applicazioni dietro al gateway edge. Come parte della configurazione di SSL VPN-Plus del gateway edge, è necessario aggiungere i pacchetti di installazione per il sistema operativo e configurare determinati parametri. Vedere [Aggiunta di un pacchetto di installazione client SSL VPN-Plus](#) per informazioni dettagliate.

La configurazione di SSL VPN-Plus in un gateway edge è un processo con più passaggi.

Prerequisiti

Verificare che tutti i certificati SSL necessari per SSL VPN-Plus siano stati aggiunti alla schermata **Certificati**. Vedere [Gestione del certificato SSL in un gateway edge di NSX Data Center for vSphere](#).

Nota In un gateway edge, la porta 443 è la porta predefinita per il protocollo HTTPS. Per la funzionalità VPN SSL, la porta HTTPS del gateway edge deve essere accessibile dalle reti esterne. Il client VPN SSL richiede che la porta e l'indirizzo IP del gateway edge configurati nella schermata Impostazioni server nella scheda **VPN SSL plus** siano raggiungibili dal sistema client. Vedere [Configurazione delle impostazioni del server VPN SSL](#).

Procedura

1 Navigazione alla schermata SSL-VPN Plus

È possibile passare alla schermata SSL-VPN Plus per iniziare a configurare il servizio SSL-VPN Plus per un gateway edge NSX Data Center for vSphere.

2 Configurazione delle impostazioni del server VPN SSL

Queste impostazioni del server consentono di configurare il server VPN SSL e includono l'indirizzo IP e la porta su cui è in ascolto il servizio, l'elenco di crittografia del servizio e il relativo certificato di servizio. Durante la connessione al gateway edge NSX Data Center for vSphere, gli utenti remoti specificano lo stesso indirizzo IP e la porta impostati in queste impostazioni del server.

3 Creazione di un pool di IP per l'utilizzo con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere

Agli utenti remoti vengono assegnati indirizzi IP virtuali dai pool di IP statici configurati mediante la schermata **Pool di IP** nella scheda **VPN SSL plus**.

4 Aggiunta di una rete privata per l'uso con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere

Utilizzare la schermata Reti private nella scheda **VPN SSL plus** per configurare le reti private. Le reti private sono quelle a cui si desidera che i client VPN possano accedere quando gli utenti remoti si connettono utilizzando i propri client VPN e il tunnel VPN SSL. Le reti private attivate verranno installate nella tabella di routing del client VPN.

5 Configurazione di un servizio di autenticazione per SSL VPN-Plus in un gateway edge NSX Data Center for vSphere

Utilizzare la schermata **Autenticazione** nella scheda **VPN SSL plus** per configurare un server di autenticazione locale per il servizio VPN SSL del gateway edge e, facoltativamente, abilitare l'autenticazione del certificato client. Questo server di autenticazione viene utilizzato per eseguire l'autenticazione degli utenti che si connettono. Verrà eseguita l'autenticazione di tutti gli utenti configurati nel server di autenticazione locale.

6 Aggiunta di utenti SSL VPN-Plus al server di autenticazione SSL VPN-Plus locale

Utilizzare la schermata **Utenti** nella scheda **VPN SSL plus** per aggiungere account di utenti remoti al server di autenticazione locale per il servizio VPN SSL del gateway edge NSX Data Center for vSphere.

7 Aggiunta di un pacchetto di installazione client SSL VPN-Plus

Utilizzare la schermata **Pacchetti di installazione** nella scheda **VPN SSL plus** per creare pacchetti di installazione con nome del client VPN SSL plus per gli utenti remoti.

8 Modifica della configurazione del client SSL VPN-Plus

Utilizzare la schermata **Configurazione client** nella scheda **VPN SSL plus** per personalizzare la modalità di risposta del tunnel client VPN SSL quando l'utente remoto accede a VPN SSL.

9 Personalizzazione delle impostazioni generali di SSL VPN-Plus per un gateway edge NSX Data Center for vSphere

Per impostazione predefinita, il sistema configura alcune impostazioni di SSL VPN-Plus in un gateway edge nell'ambiente VMware Cloud Director. È possibile personalizzare queste impostazioni utilizzando la schermata **Impostazioni generali** nella scheda **VPN SSL plus** del portale tenant di VMware Cloud Director.

Navigazione alla schermata SSL-VPN Plus

È possibile passare alla schermata SSL-VPN Plus per iniziare a configurare il servizio SSL-VPN Plus per un gateway edge NSX Data Center for vSphere.

Procedura

- 1** Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2** Fare clic sulla scheda **VPN SSL plus**.

Operazioni successive

Nella schermata **Generale**, configurare le impostazioni di VPN SSL plus predefinite. Vedere [Personalizzazione delle impostazioni generali di SSL VPN-Plus per un gateway edge NSX Data Center for vSphere](#).

Configurazione delle impostazioni del server VPN SSL

Queste impostazioni del server consentono di configurare il server VPN SSL e includono l'indirizzo IP e la porta su cui è in ascolto il servizio, l'elenco di crittografia del servizio e il relativo certificato di servizio. Durante la connessione al gateway edge NSX Data Center for vSphere, gli utenti remoti specificano lo stesso indirizzo IP e la porta impostati in queste impostazioni del server.

Se il gateway edge è configurato con più reti a indirizzi IP sovrapposti nell'interfaccia esterna, l'indirizzo IP selezionato per il server VPN SSL può essere diverso da quello dell'interfaccia esterna predefinita del gateway edge.

Quando si configurano le impostazioni del server VPN SSL, è necessario scegliere quali algoritmi di crittografia utilizzare per il tunnel VPN SSL. È possibile scegliere uno o più tipi di crittografia. Scegliere attentamente i tipi di crittografia in base ai livelli di sicurezza delle selezioni.

Per impostazione predefinita, il sistema utilizza il certificato autofirmato predefinito che il sistema genera per ogni gateway edge come certificato di identità del server predefinito per il tunnel VPN SSL. Invece di questa impostazione predefinita, è possibile scegliere di utilizzare un certificato digitale aggiunto al sistema nella schermata **Certificati**.

Prerequisiti

- Verificare che siano soddisfatti i prerequisiti descritti in [Configurazione di SSL VPN-Plus](#).
- Se si sceglie di utilizzare un certificato di servizio diverso da quello predefinito, importare il certificato richiesto nel sistema. Vedere [Aggiunta di un certificato di servizio al gateway edge](#).
- [Navigazione alla schermata SSL-VPN Plus](#).

Procedura

- 1 Nella schermata **VPN SSL plus**, fare clic su **Impostazioni server**.
- 2 Fare clic su **Abilitato**.
- 3 Selezionare un indirizzo IP dal menu a discesa.
- 4 (Facoltativo) Immettere un numero di porta TCP.

Il numero di porta TCP viene utilizzato dal pacchetto di installazione del client SSL. Per impostazione predefinita, il sistema utilizza la porta 443, ovvero la porta predefinita per il traffico HTTPS/SSL. Anche se è obbligatorio un numero di porta, per le comunicazioni è possibile impostare qualsiasi porta TCP.

Nota Il client VPN SSL richiede che l'indirizzo IP e la porta configurati qui siano raggiungibili dai sistemi client degli utenti remoti. Se si modifica il numero di porta predefinito, assicurarsi che la combinazione di porta e indirizzo IP sia raggiungibile dai sistemi degli utenti finali.

- 5 Selezionare un metodo di crittografia nell'elenco dei pacchetti di crittografia.
- 6 Configurare il criterio di registrazione Syslog del servizio.

La registrazione è attivata per impostazione predefinita. È possibile modificare il livello dei messaggi da registrare o disattivare la registrazione.

- 7 (Facoltativo) Se si desidera utilizzare un certificato di servizio al posto del certificato autofirmato predefinito generato dal sistema, fare clic su **Modifica certificato server**, selezionare un certificato e fare clic su **OK**.
- 8 Fare clic su **Salva modifiche**.

Operazioni successive

Nota L'indirizzo IP del gateway edge e il numero di porta TCP impostati devono essere raggiungibili dagli utenti remoti. Aggiungere una regola del firewall del gateway edge che consenta di accedere all'indirizzo IP SSL VPN-Plus e alla porta configurata in questa procedura. Vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#).

Aggiungere un pool di IP, in modo che agli utenti remoti vengono assegnati gli indirizzi IP quando si connettono utilizzando SSL VPN-Plus. Vedere [Creazione di un pool di IP per l'utilizzo con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere](#).

Creazione di un pool di IP per l'utilizzo con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere

Agli utenti remoti vengono assegnati indirizzi IP virtuali dai pool di IP statici configurati mediante la schermata **Pool di IP** nella scheda **VPN SSL plus**.


Ogni pool di IP aggiunto a questa schermata risulta in una subnet di indirizzi IP configurata nel gateway edge. Gli intervalli di indirizzi IP utilizzati in questi pool di IP devono essere diversi da tutte le altre reti configurate nel gateway edge.

Nota Il VPN SSL assegna indirizzi IP agli utenti remoti dai pool di IP in base all'ordine con cui i pool di IP vengono visualizzati nella tabella della schermata. Dopo aver aggiunto i pool di IP alla tabella nella schermata, è possibile modificarne le posizioni nella tabella utilizzando la freccia su e la freccia giù.

Prerequisiti

- [Navigazione alla schermata SSL-VPN Plus.](#)
- [Configurazione delle impostazioni del server VPN SSL.](#)

Procedura

- 1 Nella scheda **VPN SSL plus**, fare clic su **Pool di IP**.
- 2 Fare clic sul pulsante **Crea** ()
- 3 Configurare le impostazioni del pool di IP.

Opzione	Azione
Intervallo IP	Immettere un intervallo di indirizzi IP per questo pool di IP, ad esempio 127.0.0.1-127.0.0.9.. Questi indirizzi IP verranno assegnati ai client VPN quando effettuano l'autenticazione e la connessione al tunnel VPN SSL.
Maschera di rete	Immettere la maschera di rete del pool di IP, ad esempio 255.255.255.0.

Opzione	Azione
Gateway	Immettere l'indirizzo IP che si desidera venga creato dal gateway edge e assegnarlo come indirizzo gateway per questo pool di IP. Quando viene creato il pool di IP, viene creata una scheda virtuale nella macchina virtuale del gateway edge e questo indirizzo IP viene configurato su tale interfaccia virtuale. Questo indirizzo IP può essere qualsiasi indirizzo IP all'interno della subnet che non sia compreso anche nell'intervallo indicato nel campo Intervallo IP .
Descrizione	(Facoltativo) Immettere una descrizione per questo pool di IP.
Stato	Selezionare se attivare o disattivare questo pool di IP.
DNS primario	(Facoltativo) Immettere il nome del server DNS primario che verrà utilizzato per la risoluzione dei nomi per questi indirizzi IP virtuali.
DNS secondario	(Facoltativo) Immettere il nome del server DNS secondario da utilizzare.
Suffisso DNS	(Facoltativo) Immettere il suffisso DNS per il dominio che ospita i sistemi client, per la risoluzione dei nomi host basati su dominio.
Server WINS	(Facoltativo) Immettere l'indirizzo del server WINS in base alle esigenze della propria organizzazione.

4 Fare clic su **Mantieni**.

Risultati

La configurazione del pool di IP viene aggiunta alla tabella nella schermata.

Operazioni successive

Aggiungere le reti private che si desidera rendere accessibili agli utenti remoti che si connettono tramite SSL VPN-Plus. Vedere [Aggiunta di una rete privata per l'uso con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere](#).

Aggiunta di una rete privata per l'uso con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere

Utilizzare la schermata Reti private nella scheda **VPN SSL plus** per configurare le reti private. Le reti private sono quelle a cui si desidera che i client VPN possano accedere quando gli utenti remoti si connettono utilizzando i propri client VPN e il tunnel VPN SSL. Le reti private attivate verranno installate nella tabella di routing del client VPN.

Le reti private rappresentano un elenco di tutte le reti IP raggiungibili dietro al gateway edge per cui si desidera crittografare, o escludere dalla crittografia, il traffico per un client VPN. Ogni rete privata che richiede l'accesso tramite un tunnel VPN SSL deve essere aggiunta come una voce separata. È possibile utilizzare tecniche di riepilogo della route per limitare il numero di voci.


- SSL VPN-Plus consente agli utenti remoti di accedere alle reti private in base all'ordine dall'alto verso il basso con cui i pool IP vengono visualizzati nella tabella nella schermata. Dopo aver aggiunto le reti private alla tabella nella schermata, è possibile modificarne le posizioni nella tabella utilizzando la freccia su e la freccia giù.

- Se si sceglie di attivare l'ottimizzazione TCP per una rete privata, alcune applicazioni come FTP in modalità attiva potrebbero non funzionare all'interno di tale subnet. Per aggiungere un server FTP configurato in modalità attiva, è necessario aggiungere un'altra rete privata per il server FTP e disattivare l'ottimizzazione di TCP per tale rete privata. Inoltre, la rete privata per il server FTP deve essere attivata e viene visualizzata nella tabella nella schermata sopra la rete privata ottimizzata per TCP.

Prerequisiti

- [Navigazione alla schermata SSL-VPN Plus.](#)
- [Creazione di un pool di IP per l'utilizzo con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere.](#)

Procedura

- 1 Nella scheda **VPN SSL plus**, fare clic su **Reti Private**.
- 2 Fare clic sul pulsante **Aggiungi** ().
- 3 Configurare le impostazioni della rete privata.

Opzione	Azione
Rete	Digitare l'indirizzo IP della rete privata in formato CIDR, ad esempio 192169.1.0/24 .
Descrizione	(Facoltativo) Digitare una descrizione per la rete.
Invia traffico	<p>Specificare in che modo si desidera che il client VPN invii il traffico della rete privata e di Internet.</p> <ul style="list-style-type: none"> ■ Tramite tunnel Il client VPN invia il traffico della rete privata e di Internet tramite il gateway edge attivato per SSL VPN-Plus. ■ Ignora tunnel Il client VPN ignora il gateway edge e invia il traffico direttamente al server privato.

Opzione	Azione
Abilita ottimizzazione TCP	<p>(Facoltativo) Per ottimizzare la velocità di Internet, quando si seleziona Tramite tunnel per l'invio del traffico, è necessario selezionare anche Abilita ottimizzazione TCP.</p> <p>Se si seleziona questa opzione, migliorano le prestazioni dei pacchetti TCP all'interno del tunnel VPN, ma non migliorano le prestazioni del traffico UDP. Il tunnel VPN SSL di accesso completo convenzionale invia dati TCP/IP in un secondo stack TCP/IP per la crittografia su Internet. Questo metodo convenzionale incapsula i dati a livello di applicazione in due flussi TCP separati. Quando si verifica una perdita di pacchetti, che può accadere anche in condizioni ottimali di Internet, si ha un effetto di peggioramento delle prestazioni denominato TCP-over-TCP meltdown. Quando si verifica il TCP-over-TCP meltdown, due strumenti TCP correggono lo stesso pacchetto di dati IP, influenzando sulla velocità della rete e causando timeout di connessione. Se si seleziona Abilita ottimizzazione TCP, è possibile eliminare il rischio che il problema TCP-over-TCP si verifichi.</p> <hr/> <p>Nota Quando si attiva l'ottimizzazione di TCP:</p> <ul style="list-style-type: none"> ■ È necessario immettere i numeri di porta per i quali ottimizzare il traffico di Internet. ■ Il server VPN SSL apre la connessione TCP per conto del client VPN. Quando il server SSL VPN apre la connessione TCP, viene applicata la prima regola del firewall edge generata automaticamente, che consente il passaggio di tutte le connessioni aperte dal gateway edge. Il traffico non ottimizzato viene valutato dalle regole normali del firewall edge. La regola TCP generata per impostazione predefinita consente qualsiasi connessione. <hr/>
Porte	<p>Quando si seleziona Tramite tunnel, digitare un intervallo di numeri di porta che si desidera rimangano aperti per consentire all'utente remoto di accedere ai server interni, ad esempio 20–21 per il traffico FTP e 80–81 per il traffico HTTP.</p> <p>Per offrire agli utenti l'accesso illimitato, lasciare vuoto questo campo.</p> <hr/>
Stato	Attivare o disattivare la rete privata.

4 Fare clic su **Mantieni**.

5 Fare clic su **Salva modifiche** per salvare la configurazione nel sistema.

Operazioni successive

Aggiungere un server di autenticazione. Vedere [Configurazione di un servizio di autenticazione per SSL VPN-Plus in un gateway edge NSX Data Center for vSphere](#).

Importante Aggiungere le regole del firewall corrispondenti per consentire il traffico di rete nelle reti private aggiunte in questa schermata. Vedere [Aggiunta di una regola del firewall del gateway edge NSX Data Center for vSphere](#).

Configurazione di un servizio di autenticazione per SSL VPN-Plus in un gateway edge NSX Data Center for vSphere

Utilizzare la schermata **Autenticazione** nella scheda **VPN SSL plus** per configurare un server di autenticazione locale per il servizio VPN SSL del gateway edge e, facoltativamente, abilitare l'autenticazione del certificato client. Questo server di autenticazione viene utilizzato per eseguire l'autenticazione degli utenti che si connettono. Verrà eseguita l'autenticazione di tutti gli utenti configurati nel server di autenticazione locale.

Nel gateway edge è possibile configurare un solo server di autenticazione SSL VPN-Plus locale. Se si fa clic su **+ Locale** e si specificano server di autenticazione aggiuntivi, quando si tenta di salvare la configurazione viene visualizzato un messaggio di errore.

Il tempo massimo per l'autenticazione tramite VPN SSL è tre (3) minuti. Il numero massimo è determinato dal timeout non di autenticazione, che è 3 minuti per impostazione predefinita e non è configurabile. Di conseguenza, se sono presenti più server di autenticazione nell'autorizzazione della catena e l'autenticazione dell'utente richiede più di 3 minuti, l'autenticazione dell'utente non viene eseguita.

Prerequisiti

- [Navigazione alla schermata SSL-VPN Plus.](#)
- [Aggiunta di una rete privata per l'uso con SSL VPN-Plus in un gateway edge NSX Data Center for vSphere.](#)
- Se si desidera abilitare l'autenticazione del certificato client, verificare che al gateway edge sia stato aggiunto un certificato CA. Vedere [Aggiunta di un certificato CA al gateway edge per la verifica di attendibilità dei certificati SSL.](#)

Procedura

- 1 Fare clic sulla scheda **VPN SSL plus** e su **Autenticazione**.
- 2 Fare clic su **Locale**.

3 Configurare le impostazioni del server di autenticazione.

a (Facoltativo) Abilitare e configurare il criterio della password.

Opzione	Descrizione
Abilita criterio password	Attivare l'applicazione delle impostazioni dei criteri della password configurate qui.
Lunghezza password	Immettere il numero minimo e massimo di caratteri consentito per la lunghezza della password.
N. minimo caratteri alfanumerici	(Facoltativo) Digitare il numero minimo di caratteri alfabetici necessari nella password.
N. minimo cifre	(Facoltativo) Digitare il numero minimo di caratteri numerici necessari nella password.
N. minimo caratteri speciali	(Facoltativo) Digitare il numero minimo di caratteri speciali, ad esempio e commerciale (&), hashtag (#), simbolo di percentuale (%) e così via, necessari nella password.
La password non deve contenere l'ID utente	(Facoltativo) Abilitare questa opzione per fare in modo che la password non contenga l'ID utente.
La password scade tra	(Facoltativo) Digitare il numero massimo di giorni di durata della password prima che l'utente debba cambiarla.
Notifica di scadenza tra	(Facoltativo) Digitare quanti giorni prima del valore dell'opzione La password scade tra si desidera che l'utente venga avvisato che la password sta per scadere.

b (Facoltativo) Abilitare e configurare i criteri di blocco dell'account.

Opzione	Descrizione
Abilita criterio di blocco account	Attivare l'applicazione delle impostazioni dei criteri di blocco dell'account configurate qui.
Numero tentativi successivi	Immettere il numero di volte che un utente può tentare di accedere al proprio account.
Durata tentativi successivi	Digitare il periodo in minuti trascorso il quale l'account dell'utente viene bloccato in seguito a tentativi di accesso non riusciti. Ad esempio, se si specifica 5 per Numero tentativi successivi e 1 minuto per Durata tentativi successivi , l'account dell'utente viene bloccato dopo 5 tentativi di accesso non riusciti effettuati entro 1 minuto.
Durata blocco	Immettere il periodo di tempo per cui l'account utente rimane bloccato. Una volta trascorso questo tempo, l'account viene sbloccato automaticamente.

c Nella sezione Stato, abilitare questo server di autenticazione.

- d (Facoltativo) Configurare l'autenticazione secondaria.

Opzioni	Descrizione
Usa questo server per l'autenticazione secondaria	(Facoltativo) Specificare se si desidera utilizzare il server come secondo livello di autenticazione.
Termina sessione se l'autenticazione non riesce	(Facoltativo) Specificare se si desidera terminare la sessione VPN quando l'autenticazione non riesce.

- e Fare clic su **Mantieni**.

- 4 (Facoltativo) Per abilitare l'autenticazione del certificato client, fare clic su **Modifica certificato**, attivare l'interruttore di abilitazione, selezionare il certificato CA da utilizzare e fare clic su **OK**.

Operazioni successive

Aggiungere utenti locali al server di autenticazione locale, in modo che possano connettersi con SSL VPN-Plus. Vedere [Aggiunta di utenti SSL VPN-Plus al server di autenticazione SSL VPN-Plus locale](#).

Creare un pacchetto di installazione contenente il client SSL in modo che gli utenti remoti possano installarlo nei loro sistemi locali. Vedere [Aggiunta di un pacchetto di installazione client SSL VPN-Plus](#).

Aggiunta di utenti SSL VPN-Plus al server di autenticazione SSL VPN-Plus locale

Utilizzare la schermata **Utenti** nella scheda **VPN SSL plus** per aggiungere account di utenti remoti al server di autenticazione locale per il servizio VPN SSL del gateway edge NSX Data Center for vSphere.

Nota Se non è già stato configurato un server di autenticazione locale, l'aggiunta di un utente nella schermata **Utenti** consente di aggiungere automaticamente un server di autenticazione locale con valori predefiniti. È quindi possibile utilizzare il pulsante di modifica nella schermata **Autenticazione** per visualizzare e modificare i valori predefiniti. Per informazioni sull'utilizzo della schermata **Autenticazione**, vedere [Configurazione di un servizio di autenticazione per SSL VPN-Plus in un gateway edge NSX Data Center for vSphere](#).

Prerequisiti

[Navigazione alla schermata SSL-VPN Plus.](#)

Procedura

- 1 Nella scheda **VPN SSL plus**, fare clic su **Utenti**.
- 2 Fare clic sul pulsante **Crea** ().

3 Configurare le opzioni seguenti per l'utente.

Opzione	Descrizione
ID utente	Immettere l'ID utente.
Password	Immettere una password per l'utente.
Ridigita password	Reimmettere la password.
Nome	(Facoltativo) Immettere il nome dell'utente.
Cognome	(Facoltativo) Immettere il cognome dell'utente.
Descrizione	(Facoltativo) Immettere una descrizione per l'utente.
Abilitato	Specificare se l'utente è attivato o disattivato.
Password senza scadenza	(Facoltativo) Specificare se si desidera mantenere per sempre la stessa password per questo utente.
Consenti modifica password	(Facoltativo) Specificare se si desidera consentire all'utente di modificare la password.
Modifica password al prossimo accesso	(Facoltativo) Specificare se si desidera che questo utente modifichi la password al prossimo accesso.

4 Fare clic su **Mantieni**.

5 Ripetere i passaggi per aggiungere ulteriori utenti.

Operazioni successive

Aggiungere utenti locali al server di autenticazione locale, in modo che possano connettersi con SSL VPN-Plus. Vedere [Aggiunta di utenti SSL VPN-Plus al server di autenticazione SSL VPN-Plus locale](#).

Creare un pacchetto di installazione contenente il client SSL in modo che gli utenti remoti possano installarlo nei loro sistemi locali. Vedere [Aggiunta di un pacchetto di installazione client SSL VPN-Plus](#).

Aggiunta di un pacchetto di installazione client SSL VPN-Plus

Utilizzare la schermata Pacchetti di installazione nella scheda **VPN SSL plus** per creare pacchetti di installazione con nome del client VPN SSL plus per gli utenti remoti.


È possibile aggiungere un pacchetto di installazione client SSL VPN-Plus al gateway edge NSX Data Center for vSphere. Ai nuovi utenti viene richiesto di scaricare e installare il pacchetto al momento del loro primo accesso alla connessione VPN. Quando vengono aggiunti, questi pacchetti di installazione client sono quindi scaricabili dal nome di dominio completo dell'interfaccia pubblica del gateway edge.


È possibile creare pacchetti di installazione eseguibili nei sistemi operativi Windows, Linux e Mac. Se sono necessari parametri di installazione diversi per i client VPN SSL, creare un pacchetto di installazione per ogni configurazione.

Prerequisiti

Navigazione alla schermata SSL-VPN Plus

Procedura

- 1 Nella scheda **VPN SSL plus** nel portale tenant, fare clic su **Pacchetti di installazione**.
- 2 Fare clic sul pulsante **Aggiungi** ()
- 3 Configurare le impostazioni del pacchetto di installazione.

Opzione	Descrizione
Nome profilo	Immettere un nome profilo per il pacchetto di installazione. Il nome viene visualizzato per consentire all'utente remoto di identificare questa connessione VPN SSL nel gateway edge.
Gateway	Immettere l'indirizzo IP o il nome di dominio completo (FQDN) dell'interfaccia pubblica del gateway edge. L'indirizzo IP o il nome di dominio completo immesso è associato al client VPN SSL. Quando il client viene installato nel sistema locale dell'utente remoto, questo indirizzo IP o nome di dominio completo viene visualizzato in tale client VPN SSL. Per associare altre interfacce di uplink del gateway edge a questo client VPN SSL, fare clic sul pulsante Aggiungi () per aggiungere righe e digitare gli indirizzi IP o FQDN, e le porte, di ciascuna interfaccia.
Porta	(Facoltativo) Per modificare il valore della porta rispetto a quello predefinito visualizzato, fare doppio clic sul valore e digitarne uno nuovo.
Windows Linux Mac	Selezionare i sistemi operativi per i quali si desidera creare i pacchetti di installazione.
Descrizione	(Facoltativo) Digitare una descrizione per l'utente.
Abilitato	Specificare se questo pacchetto è attivato o disattivato.

- 4 Selezionare i parametri di installazione per Windows.

Opzione	Descrizione
Avvia client all'accesso	Avvia il client VPN SSL quando l'utente remoto accede al proprio sistema locale.
Consenti memorizzazione password	Consente al client di ricordare la password dell'utente.
Abilita installazione in modalità invisibile all'utente	Nasconde i comandi di installazione degli utenti remoti.
Nascondi scheda di rete client SSL	Nasconde la scheda SSL VPN-Plus VMware installata nel computer dell'utente remoto insieme al pacchetto di installazione del client VPN SSL.
Nascondi icona nell'area di notifica del client	Nasconde l'icona di notifica VPN SSL che indica se la connessione VPN è attiva o meno.
Crea icona sul desktop	Crea un'icona sul desktop dell'utente per richiamare il client SSL.

Opzione	Descrizione
Abilita funzionamento in modalità invisibile all'utente	Nasconde la finestra che indica il completamento dell'installazione.
Convalida certificato di sicurezza server	Il client VPN SSL convalida il certificato del server VPN SSL prima di stabilire una connessione sicura.

5 Fare clic su **Mantieni**.

Operazioni successive

Modificare la configurazione del client. Vedere [Modifica della configurazione del client SSL VPN-Plus](#).

Modifica della configurazione del client SSL VPN-Plus

Utilizzare la schermata **Configurazione client** nella scheda **VPN SSL plus** per personalizzare la modalità di risposta del tunnel client VPN SSL quando l'utente remoto accede a VPN SSL.

Prerequisiti

[Navigazione alla schermata SSL-VPN Plus](#)

Procedura

- 1 Nella scheda **VPN SSL plus**, fare clic su **Configurazione client**.
- 2 Selezionare la **Modalità tunneling**.
 - In modalità tunnel diviso, solo il traffico VPN attraversa il gateway edge.
 - In modalità tunnel completo il gateway edge diventa il gateway predefinito dell'utente remoto e tutto il traffico, ad esempio VPN, locale e Internet, attraversa il gateway edge.
- 3 Se si seleziona la modalità tunnel completo, immettere l'indirizzo IP per il gateway predefinito utilizzato dai client degli utenti remoti e, facoltativamente, scegliere se impedire che il traffico della subnet locale passi attraverso il tunnel VPN.
- 4 (Facoltativo) Disattivare la riconnessione automatica.

L'opzione **Abilita riconnessione automatica** è attivata per impostazione predefinita. Se la riconnessione automatica è attivata, il client VPN SSL riconnette automaticamente gli utenti quando vengono disconnessi.
- 5 (Facoltativo) Facoltativamente, fare in modo che il client informi gli utenti remoti quando è disponibile un aggiornamento del client.

Questa opzione è disattivata per impostazione predefinita. Se si attiva questa opzione, gli utenti remoti possono scegliere di installare l'aggiornamento.
- 6 Fare clic su **Salva modifiche**.

Personalizzazione delle impostazioni generali di SSL VPN-Plus per un gateway edge NSX Data Center for vSphere

Per impostazione predefinita, il sistema configura alcune impostazioni di SSL VPN-Plus in un gateway edge nell'ambiente VMware Cloud Director. È possibile personalizzare queste impostazioni utilizzando la schermata **Impostazioni generali** nella scheda **VPN SSL plus** del portale tenant di VMware Cloud Director.

Prerequisiti

[Navigazione alla schermata SSL-VPN Plus.](#)

Procedura

- 1 Nella scheda **VPN SSL plus**, fare clic su **Impostazioni generali**.
- 2 Modificare le impostazioni generali in base alle esigenze della propria organizzazione.

Opzione	Descrizione
Impedisci accessi multipli con lo stesso nome utente	Consente di limitare un utente remoto a una singola sessione di login attiva con lo stesso nome utente.
Compressione	Attivare per consentire la compressione dei dati intelligente basata su TCP e migliorare la velocità di trasferimento dati.
Abilita registrazione	Attivare per mantenere un registro del traffico che attraversa il gateway VPN SSL. La registrazione è abilitata per impostazione predefinita.
Forza tastiera virtuale	Attivare per fare in modo che gli utenti remoti possano utilizzare solo una tastiera virtuale (sullo schermo) per immettere le informazioni di accesso.
Scegli in modo casuale i tasti della tastiera virtuale	Attivare per fare in modo che la tastiera virtuale utilizzi una disposizione dei tasti casuale.
Timeout inattività sessione	Immettere il timeout di inattività della sessione in minuti. Se in una sessione utente non è presente alcuna attività per il periodo di tempo specificato, la sessione viene disconnessa. Il valore predefinito di sistema è 10 minuti.
Notifica utente	Digitare il messaggio che gli utenti remoti visualizzeranno dopo avere eseguito il login.
Abilita accesso URL pubblico	Attivare per consentire agli utenti remoti di accedere a siti non esplicitamente configurati per l'accesso di utenti remoti.
Abilita timeout forzato	Consente di disconnettere gli utenti remoti al termine del periodo di tempo specificato nel campo Timeout forzato .
Timeout forzato	Digitare il periodo di timeout in minuti. Questo campo viene visualizzato quando è attivato l'interruttore Abilita timeout forzato .

- 3 Fare clic su **Salva modifiche**.

Configurazione di VPN IPsec

I gateway edge NSX Data Center for vSphere in un ambiente VMware Cloud Director supportano il protocollo IPsec (Internet Protocol Security) da sito a sito per proteggere i tunnel VPN tra reti di virtual data center dell'organizzazione o tra una rete di virtual data center dell'organizzazione e un indirizzo IP esterno. È possibile configurare il servizio VPN IPsec in un gateway edge.

La configurazione di una connessione VPN IPsec da una rete remota al virtual data center dell'organizzazione è lo scenario più comune. Il software NSX offre al gateway edge funzionalità VPN IPsec, incluso il supporto per l'autenticazione del certificato, la modalità con chiave precondivisa e il traffico unicast IP tra se stesso e i router VPN remoti. È inoltre possibile configurare più subnet per la connessione tramite tunnel IPsec alla rete interna dietro un gateway edge. Quando si configurano più subnet per la connessione tramite tunnel IPsec alla rete interna, tali subnet e la rete interna dietro al gateway edge non devono includere intervalli di indirizzi che si sovrappongono.

Nota Se il peer locale e remoto attraverso un tunnel IPsec includono indirizzi IP che si sovrappongono, l'inoltro del traffico attraverso il tunnel potrebbe non essere coerente in base alla presenza di route connesse locali e route con plumbing automatico.

Sono supportati i seguenti algoritmi VPN IPsec:

- AES (AES128-CBC)
- AES256 (AES256-CBC)
- DES triplo (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (gruppo Diffie-Hellman 2)
- DH-5 (gruppo Diffie-Hellman 5)
- DH-14 (gruppo Diffie-Hellman 14)

Nota I protocolli di routing dinamico non sono supportati con VPN IPsec. Quando si configura un tunnel VPN IPsec tra un gateway edge del virtual data center dell'organizzazione e un gateway VPN fisico in un sito remoto, non è possibile configurare il routing dinamico per tale connessione. L'indirizzo IP di tale sito remoto non può essere individuato tramite il routing dinamico nell'uplink del gateway edge.

Come descritto nell'argomento *Panoramica di VPN IPsec* nella *Guida per l'amministratore di NSX*, il numero massimo di tunnel supportato in un gateway edge è determinato dalle sue dimensioni configurate: Compact, Large, X-Large, Quad Large.

Per visualizzare le dimensioni della configurazione del gateway edge, passare al gateway edge e fare clic sul nome del gateway edge.

La configurazione di VPN IPsec in un gateway edge è un processo che include più passaggi.

Nota Se è presente un firewall tra gli endpoint del tunnel, dopo aver configurato il servizio VPN IPsec, aggiornare le regole del firewall per consentire le porte UDP e i protocolli IP seguenti:

- ID protocollo IP 50 (ESP)
- ID protocollo IP 51 (AH)
- Porta UDP 500 (IKE)
- Porta UDP 4500

Procedura

1 [Passaggio alla schermata VPN IPsec](#)

Nella schermata **VPN IPsec**, è possibile iniziare a configurare il servizio VPN IPsec per un gateway edge NSX Data Center for vSphere.

2 [Configurazione delle connessioni al sito VPN IPsec per il gateway edge NSX Data Center for vSphere](#)

Utilizzare la schermata **Siti VPN IPsec** nel portale tenant di VMware Cloud Director per configurare le impostazioni necessarie per creare una connessione VPN IPsec tra il virtual data center dell'organizzazione e un altro sito utilizzando le funzionalità VPN IPsec del gateway edge.

3 [Abilitazione del servizio VPN IPsec in un gateway edge NSX Data Center for vSphere](#)

Quando è configurata almeno una connessione VPN IPsec, è possibile abilitare il servizio VPN IPsec nel gateway edge.

4 [Come specificare le impostazioni VPN IPsec globali](#)

Utilizzare la schermata **Configurazione globale** per configurare le impostazioni di autenticazione di VPN IPsec a livello di un gateway edge. In questa schermata, è possibile impostare una chiave precondivisa globale e abilitare l'autenticazione del certificato.

Passaggio alla schermata VPN IPsec

Nella schermata **VPN IPsec**, è possibile iniziare a configurare il servizio VPN IPsec per un gateway edge NSX Data Center for vSphere.

Procedura

1 Aprire i servizi gateway edge.

- a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
- b Selezionare il gateway edge da modificare e fare clic su **Servizi**.

2 Passare a **VPN > VPN IPsec**.

Operazioni successive

Utilizzare la schermata **Siti VPN IPsec** per configurare una connessione VPN IPsec. Per poter abilitare il servizio VPN IPsec nel gateway edge, è necessario configurare almeno una connessione. Vedere [Configurazione delle connessioni al sito VPN IPsec per il gateway edge NSX Data Center for vSphere](#).

Configurazione delle connessioni al sito VPN IPsec per il gateway edge NSX Data Center for vSphere

Utilizzare la schermata **Siti VPN IPsec** nel portale tenant di VMware Cloud Director per configurare le impostazioni necessarie per creare una connessione VPN IPsec tra il virtual data center dell'organizzazione e un altro sito utilizzando le funzionalità VPN IPsec del gateway edge.

Quando si configura una connessione VPN IPsec tra siti, la connessione viene configurata dal punto di vista della posizione corrente. La configurazione della connessione richiede la comprensione dei concetti nel contesto dell'ambiente VMware Cloud Director in modo da configurare la connessione VPN in modo corretto.


- Le subnet peer e locale specificano le reti a cui la VPN si connette. Quando si specificano queste subnet nelle configurazioni per i siti VPN IPsec, immettere un intervallo di rete e non un indirizzo IP specifico. Utilizzare il formato CIDR, ad esempio **192.168.99.0/24**.
- L'ID peer è un identificatore che identifica in modo univoco il dispositivo remoto che termina la connessione VPN. In genere si tratta dell'indirizzo IP pubblico del dispositivo remoto. Per i peer che utilizzano l'autenticazione del certificato, questo ID deve essere il nome distinto impostato nel certificato del peer. Per i peer PSK, l'ID può essere qualsiasi stringa. Una procedura consigliata per NSX consiste nell'utilizzare come ID peer l'indirizzo IP pubblico del dispositivo remoto o il nome di dominio completo. Se l'indirizzo IP del peer proviene da un'altra rete di virtual data center dell'organizzazione, immettere l'indirizzo IP nativo del peer. Se NAT è configurato per il peer, immettere l'indirizzo IP privato del peer.
- L'endpoint peer specifica l'indirizzo IP pubblico del dispositivo remoto a cui ci si sta connettendo. L'endpoint peer potrebbe avere un indirizzo diverso dall'ID peer se il gateway del peer non è accessibile direttamente da Internet ma si connette tramite un altro dispositivo. Se NAT è configurato per il peer, immettere l'indirizzo IP pubblico che i dispositivi utilizzano per NAT.
- L'ID locale specifica l'indirizzo IP pubblico del gateway edge del virtual data center dell'organizzazione. È possibile immettere un indirizzo IP o un nome host insieme al firewall del gateway edge.
- L'endpoint locale specifica la rete nel virtual data center dell'organizzazione in cui il gateway edge trasmette. La rete esterna del gateway edge è in genere l'endpoint locale.

Prerequisiti

- [Passaggio alla schermata VPN IPsec](#).
- [Configurazione di VPN IPsec](#).

- Se si desidera utilizzare un certificato globale come metodo di autenticazione, verificare che l'autenticazione del certificato sia abilitata nella schermata **Configurazione globale**. Vedere [Come specificare le impostazioni VPN IPsec globali](#).

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Nella scheda **VPN IPsec**, fare clic su **Siti VPN IPsec**.
- 3 Fare clic sul pulsante **Aggiungi** ().
- 4 Configurare le impostazioni di connessione di VPN IPsec.

Opzione	Azione
Abilitato	Abilitare la connessione tra i due endpoint VPN.
Abilita PFS (Perfect Forward Secrecy)	<p>Abilitare questa opzione per fare in modo che il sistema generi chiavi pubbliche univoche per tutte le sessioni VPN IPsec avviate dagli utenti. L'abilitazione di PFS assicura che il sistema non crei un collegamento tra la chiave privata del gateway edge e la chiave di ciascuna sessione.</p> <p>La compromissione della chiave di una sessione influirà solo sui dati scambiati in tale sessione protetta da quella chiave specifica. La compromissione della chiave privata del server non può essere utilizzata per decrittografare le sessioni archiviate o le sessioni future.</p> <p>Quando PFS è abilitato, nelle connessioni VPN IPsec a questo gateway edge si verifica un leggero overhead di elaborazione.</p> <p>Importante Le chiavi di sessione univoche non devono essere utilizzate per ricavare altre chiavi aggiuntive. Inoltre, affinché il tunnel VPN IPsec funzioni è necessario che entrambi i lati supportino PFS.</p>
Nome	(Facoltativo) Immettere un nome per la connessione.
ID locale	<p>Immettere l'indirizzo IP esterno dell'istanza del gateway edge, che è l'indirizzo IP pubblico del gateway edge.</p> <p>L'indirizzo IP è quello utilizzato per l>ID peer nella configurazione VPN IPsec nel sito remoto.</p>
Endpoint locale	<p>Immettere la rete corrispondente all'endpoint locale per questa connessione. L'endpoint locale specifica la rete nel virtual data center dell'organizzazione in cui il gateway edge trasmette. La rete esterna è in genere l'endpoint locale.</p> <p>Se si aggiunge un tunnel da IP a IP mediante una chiave precondivisa, l>ID locale e l'IP dell'endpoint locale possono coincidere.</p>
Subnet locali	<p>Immettere le reti da condividere tra i siti e utilizzare una virgola come separatore per immettere più subnet.</p> <p>Immettere un intervallo di rete (non un indirizzo IP specifico) inserendo l'indirizzo IP in formato CIDR. Ad esempio, 192.168.99.0/24.</p>

Opzione	Azione
ID peer	<p>Immettere un ID peer per identificare in modo univoco il sito peer.</p> <p>L'ID peer è un identificatore che identifica in modo univoco il dispositivo remoto che termina la connessione VPN. In genere si tratta dell'indirizzo IP pubblico del dispositivo remoto.</p> <p>Per i peer che utilizzano l'autenticazione del certificato, l'ID deve essere il nome distinto nel certificato del peer. Per i peer PSK, l'ID può essere qualsiasi stringa. Una procedura consigliata di NSX consiste nell'utilizzare come ID peer l'indirizzo IP pubblico o il nome di dominio completo del dispositivo remoto.</p> <p>Se l'indirizzo IP del peer proviene da un'altra rete di virtual data center dell'organizzazione, immettere l'indirizzo IP nativo del peer. Se NAT è configurato per il peer, immettere l'indirizzo IP privato del peer.</p>
Endpoint peer	<p>Immettere l'indirizzo IP o il nome di dominio completo del sito peer, che è l'indirizzo pubblico del dispositivo remoto a cui ci si sta connettendo.</p> <p>Nota Quando NAT è configurato per il peer, immettere l'indirizzo IP pubblico che il dispositivo utilizza per il NAT.</p>
Subnet peer	<p>Immettere la rete remota a cui la VPN si connette e utilizzare una virgola come separatore per immettere più subnet.</p> <p>Immettere un intervallo di rete (non un indirizzo IP specifico) inserendo l'indirizzo IP in formato CIDR. Ad esempio, 192.168.99.0/24.</p>
Algoritmo di crittografia	<p>Selezionare il tipo di algoritmo di crittografia dal menu a discesa.</p> <p>Nota Il tipo di crittografia selezionato deve corrispondere al tipo di crittografia configurato nel dispositivo VPN del sito remoto.</p>
Autenticazione	<p>Selezionare un'autenticazione: Le opzioni sono:</p> <ul style="list-style-type: none"> ■ PSK <p>PSK (Pre Shared Key) indica che per l'autenticazione è necessario utilizzare la chiave segreta condivisa tra il gateway edge e il sito peer.</p> ■ Certificato <p>L'autenticazione Certificato indica che per l'autenticazione è necessario utilizzare il certificato definito a livello globale. Questa opzione non è disponibile a meno che non sia stato configurato il certificato globale nella schermata Configurazione globale della scheda VPN IPsec.</p>
Modifica chiave condivisa	<p>(Facoltativo) Quando si aggiornano le impostazioni di una connessione esistente, è possibile abilitare questa opzione per rendere disponibile il campo Chiave precondisa in modo da poter aggiornare la chiave condivisa.</p>
Chiave precondisa	<p>Se si seleziona PSK come tipo di autenticazione, digitare una stringa alfanumerica segreta che può essere una stringa con una lunghezza massima di 128 byte.</p> <p>Nota La chiave condivisa deve corrispondere alla chiave configurata nel dispositivo VPN del sito remoto. Una procedura consigliata consiste nel configurare una chiave condivisa quando siti anonimi si conatteranno al servizio VPN.</p>
Mostra chiave condivisa	<p>(Facoltativo) Abilitare questa opzione per rendere la chiave condivisa visibile nella schermata.</p>

Opzione	Azione
Gruppo Diffie-Hellman	<p>Selezionare lo schema di crittografia che consente al sito peer e a questo gateway edge di stabilire un segreto condiviso in un canale di comunicazione non protetto.</p> <hr/> <p>Nota Il valore di Gruppo Diffie-Hellman deve corrispondere a quello configurato nel dispositivo VPN del sito remoto.</p> <hr/>
Estensione	<p>(Facoltativo) Digitare una delle seguenti opzioni:</p> <ul style="list-style-type: none"> ■ <code>securelocaltrafficbyip=IPAddress</code> per reindirizzare il traffico locale del gateway edge attraverso il tunnel VPN IPsec. <p>Questo è il valore predefinito.</p> <ul style="list-style-type: none"> ■ <code>passthroughSubnets= PeerSubnet/IPAddress</code> per supportare le subnet che si sovrappongono. <hr/>

5 Fare clic su **Mantieni**.

6 Fare clic su **Salva modifiche**.

Operazioni successive

Configurare la connessione per il sito remoto. È necessario configurare la connessione VPN IPsec in entrambi i lati della connessione, ovvero nel virtual data center dell'organizzazione e nel sito peer.

Abilitare il servizio VPN IPsec in questo gateway edge. Se è configurata almeno una connessione VPN IPsec, è possibile abilitare il servizio. Vedere [Abilitazione del servizio VPN IPsec in un gateway edge NSX Data Center for vSphere](#).

Abilitazione del servizio VPN IPsec in un gateway edge NSX Data Center for vSphere

Quando è configurata almeno una connessione VPN IPsec, è possibile abilitare il servizio VPN IPsec nel gateway edge.

Prerequisiti

- [Passaggio alla schermata VPN IPsec](#).
- Verificare che per il gateway edge sia configurata almeno una connessione VPN IPsec. Vedere la procedura descritta in [Configurazione delle connessioni al sito VPN IPsec per il gateway edge NSX Data Center for vSphere](#).

Procedura

- 1 Nella scheda **VPN IPsec**, fare clic su **Stato di attivazione**.
- 2 Fare clic su **Stato servizio VPN IPsec** per abilitare il servizio VPN IPsec.
- 3 Fare clic su **Salva modifiche**.

Risultati

Il servizio VPN IPsec del gateway edge è attivo.

Come specificare le impostazioni VPN IPsec globali

Utilizzare la schermata **Configurazione globale** per configurare le impostazioni di autenticazione di VPN IPsec a livello di un gateway edge. In questa schermata, è possibile impostare una chiave precondivisa globale e abilitare l'autenticazione del certificato.

Una chiave precondivisa globale viene utilizzata per i siti il cui endpoint peer è impostato su **qualsiasi**.

Prerequisiti

- Se si desidera abilitare l'autenticazione del certificato, verificare di disporre di almeno un certificato di servizio e dei certificati corrispondenti firmati dall'autorità di certificazione nella schermata **Certificati**. I certificati autofirmati non possono essere utilizzati per le reti VPN IPsec. Vedere [Aggiunta di un certificato di servizio al gateway edge](#).
- [Passaggio alla schermata VPN IPsec](#).

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Nella scheda **VPN IPsec**, fare clic su **Configurazione globale**.
- 3 (Facoltativo) Impostare una chiave precondivisa globale:
 - a Abilitare l'opzione **Modifica chiave condivisa**.
 - b Inserire una chiave precondivisa.

La chiave precondivisa globale (PSK) è condivisa da tutti i siti il cui endpoint peer è impostato su **any**. Se è già stata impostata una chiave PSK globale, la modifica della chiave PSK in un valore vuoto e il relativo salvataggio non avranno alcun effetto sull'impostazione esistente.
 - c (Facoltativo) Facoltativamente, abilitare **Mostra chiave condivisa** per rendere la chiave precondivisa visibile.
 - d Fare clic su **Salva modifiche**.
- 4 Configurare l'autenticazione del certificato:
 - a Attivare l'opzione **Abilita autenticazione certificato**.
 - b Selezionare i certificati di servizio, i certificati dell'autorità di certificazione e gli elenchi CRL appropriati.
 - c Fare clic su **Salva modifiche**.

Operazioni successive

Facoltativamente, è possibile abilitare la registrazione per il servizio VPN IPsec del gateway edge. Vedere [Statistiche e registri per un gateway edge di NSX Data Center for vSphere](#).

Configurazione di VPN L2

I gateway edge NSX Data Center for vSphere in un ambiente VMware Cloud Director supportano VPN L2. VPN L2 permette l'estensione del virtual data center dell'organizzazione consentendo alle macchine virtuali di mantenere la connettività di rete mantenendo lo stesso indirizzo IP in aree geografiche diverse. È possibile configurare il servizio VPN L2 in un gateway edge.

NSX Data Center for vSphere offre le funzionalità VPN L2 di un gateway edge. VPN L2 consente di configurare un tunnel tra due siti. Le macchine virtuali rimangono nella stessa subnet nonostante vengano trasferite tra questi siti e ciò consente di estendere il virtual data center dell'organizzazione estendendone la rete tramite VPN L2. Un gateway edge in un sito può fornire tutti i servizi alle macchine virtuali nell'altro sito.

Per creare il tunnel VPN L2, è necessario configurare un server VPN L2 e un client VPN L2. Come descritto nella *Guida per l'amministratore di NSX*, il server VPN L2 è il gateway edge di destinazione e il client VPN L2 è il gateway edge di origine. Dopo aver configurato le impostazioni VPN L2 in ciascun gateway edge, è quindi necessario abilitare il servizio VPN L2 sia nel server che nel client.

Nota Nei gateway edge deve essere presente una rete di virtual data center dell'organizzazione instradata creata come interfaccia secondaria.

Passaggio alla schermata VPN L2

Per iniziare la configurazione del servizio VPN L2 per un gateway edge NSX Data Center for vSphere, è necessario passare alla schermata **VPN L2**.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Passare a **VPN > VPN L2**.

Operazioni successive

Configurare il server VPN L2. Vedere [Configurazione del gateway edge NSX Data Center for vSphere come server VPN L2](#).

Configurazione del gateway edge NSX Data Center for vSphere come server VPN L2

Il server VPN L2 è l'edge NSX di destinazione a cui il client VPN L2 sta per connettersi.

Come descritto in *NSX Administration Guide*, è possibile connettere più siti peer a questo server VPN L2.

Nota La modifica delle impostazioni di configurazione del sito comporta la disconnessione del gateway edge e la riconnessione di tutte le connessioni esistenti.


Prerequisiti

- Verificare che il gateway edge disponga di una rete di virtual data center dell'organizzazione instradata configurata come interfaccia secondaria nel gateway edge.
- [Passaggio alla schermata VPN L2.](#)
- Se si desidera associare un certificato di servizio alla connessione VPN L2, verificare che il certificato del server sia già stato caricato nel gateway edge. Vedere [Aggiunta di un certificato di servizio al gateway edge](#).
- Per poter abilitare il servizio VPN L2, è necessario disporre dell'IP listener del server, della porta del listener, dell'algoritmo di crittografia e di almeno un sito peer configurato.

Procedura

- 1 Nella scheda **VPN L2**, selezionare **Server** per la modalità VPN L2.
- 2 Nella scheda **Globale server**, configurare i dettagli di configurazione globale del server VPN L2.

Opzione	Azione
IP listener	Selezionare l'indirizzo IP primario o secondario di un'interfaccia esterna del gateway edge.
Porta listener	Modificare il valore visualizzato in base alle esigenze della propria organizzazione. La porta predefinita per il servizio VPN L2 è la 443.
Algoritmo di crittografia	Selezionare l'algoritmo di crittografia per la comunicazione tra il server e il client.
Dettagli certificato servizio	Fare clic su Modifica certificato server per selezionare il certificato da associare al server VPN L2. Nella finestra Modifica certificato server , attivare Convalida certificato server , selezionare un certificato server nell'elenco e fare clic su OK .

- 3 Per configurare i siti peer, fare clic sulla scheda **Siti server**.
- 4 Fare clic sul pulsante **Aggiungi** ().
- 5 Configurare le impostazioni per un sito peer VPN L2.

Opzione	Azione
Abilitato	Abilitare questo sito peer.
Nome	Immettere un nome univoco per il sito peer.

Opzione	Azione
Descrizione	(Facoltativo) Digitare una descrizione.
ID utente	Immettere il nome utente e la password con cui eseguire l'autenticazione del sito peer.
Password	
Conferma password	
Interfacce estese	Selezionare almeno un'interfaccia secondaria da estendere con il client. Le interfacce secondarie disponibili per la selezione sono le reti di virtual data center dell'organizzazione configurate come interfacce secondarie nel gateway edge.
Indirizzo gateway ottimizzazione in uscita	(Facoltativo) Se il gateway predefinito per le macchine virtuali è lo stesso per i due siti, immettere gli indirizzi IP del gateway delle interfacce secondarie per cui si desidera che il traffico venga instradato o bloccato localmente attraverso il tunnel VPN L2.

6 Fare clic su **Mantieni**.

7 Fare clic su **Salva modifiche**.

Operazioni successive

Abilitare il servizio VPN L2 in questo gateway edge. Vedere [Abilitazione del servizio VPN L2 in un gateway edge NSX Data Center for vSphere](#).

Configurazione di un gateway edge NSX Data Center for vSphere come client VPN L2

Il client VPN L2 è l'istanza di NSX Edge di origine che avvia la comunicazione con l'istanza di NSX Edge di destinazione, ovvero il server VPN L2.

Prerequisiti

- [Passaggio alla schermata VPN L2](#).
- Se il client VPN L2 si connette a un server VPN L2 che utilizza un certificato del server, verificare che il certificato CA corrispondente sia caricato nel gateway edge per abilitare la convalida del certificato del server per il client VPN L2. Vedere [Aggiunta di un certificato CA al gateway edge per la verifica di attendibilità dei certificati SSL](#).

Procedura

- 1 Nella scheda **VPN L2**, selezionare **Client** per la modalità VPN L2.
- 2 Nella scheda **Globale client**, configurare i dettagli di configurazione globale del client VPN L2.

Opzione	Descrizione
Indirizzo server	Immettere l'indirizzo IP del server VPN L2 a cui questo client dovrà connettersi.
Porta server	Immettere la porta del server VPN L2 a cui il client dovrà connettersi. La porta predefinita è 443.
Algoritmo di crittografia	Selezionare l'algoritmo di crittografia per la comunicazione con il server.

Opzione	Descrizione
Interfacce estese	Selezionare le interfacce secondarie da estendere al server. Le interfacce secondarie disponibili per la selezione sono le reti di virtual data center dell'organizzazione configurate come interfacce secondarie nel gateway edge.
Indirizzo gateway ottimizzazione in uscita	(Facoltativo) Se il gateway predefinito per le macchine virtuali è lo stesso tra i due siti, digitare gli indirizzi IP del gateway delle interfacce secondarie o gli indirizzi IP per i quali il traffico non deve passare attraverso il tunnel.
Dettagli utente	Immettere l'ID utente e la password per l'autenticazione nel server.

3 Fare clic su **Salva modifiche**.

4 (Facoltativo) Per configurare le opzioni avanzate, fare clic sulla scheda **Avanzato client**.

5 Se questo client edge VPN L2 non dispone di accesso diretto a Internet e deve raggiungere l'edge server VPN L2 tramite un server proxy, specificare le impostazioni del proxy.

Opzione	Descrizione
Abilita proxy sicuro	Selezionare per abilitare il proxy sicuro.
Indirizzo	Immettere l'indirizzo IP del server proxy.
Porta	Immettere la porta del server proxy.
Nome utente	Immettere le credenziali di autenticazione del server proxy.
Password	

6 Per abilitare la convalida del certificato del server, fare clic su **Modifica certificato CA** e selezionare il certificato CA appropriato.

7 Fare clic su **Salva modifiche**.

Operazioni successive

Abilitare il servizio VPN L2 in questo gateway edge. Vedere [Abilitazione del servizio VPN L2 in un gateway edge NSX Data Center for vSphere](#).

Abilitazione del servizio VPN L2 in un gateway edge NSX Data Center for vSphere

Quando si configurano le impostazioni di VPN L2 richieste, è possibile abilitare il servizio VPN L2 nel gateway edge.

Nota Se in questo gateway edge è già configurata la funzionalità HA, assicurarsi che nel gateway edge siano configurate più interfacce interne. Se è presente solo un'interfaccia ed è già stata utilizzata dalla funzionalità HA, non sarà possibile eseguire la configurazione di VPN L2 nella stessa interfaccia interna.

Prerequisiti

- Se questo gateway edge è un server VPN L2, ovvero l'NSX Edge di destinazione, verificare che siano configurate le impostazioni del server VPN L2 richieste e almeno un sito peer VPN L2. Vedere la procedura descritta in [Configurazione del gateway edge NSX Data Center for vSphere come server VPN L2](#).
- Se questo gateway edge è un client VPN L2, ovvero l'NSX Edge di origine, verificare che siano configurate le impostazioni del client VPN L2. Vedere la procedura descritta in [Configurazione di un gateway edge NSX Data Center for vSphere come client VPN L2](#).
- [Passaggio alla schermata VPN L2](#).

Procedura

- 1 Nella scheda **VPN L2**, fare clic sull'interruttore **Abilita**.
- 2 Fare clic su **Salva modifiche**.

Risultati

Il servizio VPN L2 del gateway edge viene attivato.

Operazioni successive

Creare regole firewall o NAT sul lato firewall della connessione a Internet in modo da abilitare il server VPN L2 per la connessione al client VPN L2.

Rimozione della configurazione del servizio VPN L2 da un gateway edge NSX Data Center for vSphere

È possibile rimuovere la configurazione del servizio VPN L2 esistente del gateway edge. Questa azione disattiva anche il servizio VPN L2 nel gateway edge.

Prerequisiti

[Passaggio alla schermata VPN L2](#)

Procedura

- 1 Scorrere fino alla parte inferiore della schermata VPN L2 e fare clic su **Elimina configurazione**.
- 2 Per confermare l'eliminazione, fare clic su **OK**.

Risultati

Il servizio VPN L2 viene disattivato e i dettagli relativi alla configurazione vengono rimossi dal gateway edge.

Gestione del certificato SSL in un gateway edge di NSX Data Center for vSphere

Il software NSX Data Center for vSphere nell'ambiente VMware Cloud Director consente di utilizzare certificati SSL (Secure Sockets Layer) con i tunnel SSL VPN-Plus e VPN IPsec configurati per i gateway edge.

I gateway edge nell'ambiente VMware Cloud Director supportano certificati autofirmati, certificati firmati da un'autorità di certificazione e certificati generati e firmati da un'autorità di certificazione. È possibile generare richieste di firma del certificato (CSR), importare certificati, gestire i certificati importati e creare elenchi di revoca dei certificati (CRL).

Informazioni sull'utilizzo di certificati con il virtual data center dell'organizzazione

Nel virtual data center dell'organizzazione di VMware Cloud Director è possibile gestire i certificati per le seguenti aree di rete.

- Tunnel VPN IPsec tra la rete di un virtual data center dell'organizzazione e una rete remota.
- Connessioni SSL VPN-Plus tra utenti remoti di reti private e risorse Web nel virtual data center dell'organizzazione.
- Un tunnel VPN L2 tra due gateway edge NSX Data Center for vSphere.
- I server virtuali e i server pool configurati per il bilanciamento del carico nel virtual data center dell'organizzazione.

Come utilizzare i certificati client

È possibile creare un certificato client tramite un comando CAI o una chiamata REST. È quindi possibile distribuire questo certificato agli utenti remoti, che possono installare il certificato nel proprio browser Web.

Il vantaggio principale offerto dall'implementazione di certificati client è che un certificato client di riferimento per ciascun utente remoto può essere memorizzato e confrontato con il certificato client presentato dall'utente remoto. Per impedire connessioni future da parte di un determinato utente, è possibile eliminare il certificato di riferimento dall'elenco dei certificati client del server di sicurezza. Se si elimina il certificato, le connessioni da tale utente vengono rifiutate.

Generazione di una richiesta di firma del certificato per un gateway edge

Per poter ordinare un certificato firmato da un'autorità di certificazione o creare un certificato autofirmato, è necessario generare una richiesta di firma del certificato (CSR) per il gateway edge.

Una richiesta CSR è un file codificato che è necessario generare in un gateway NSX Edge che richiede un certificato SSL. L'utilizzo di una richiesta CSR standardizza il modo in cui le società inviano le chiavi pubbliche insieme alle informazioni che identificano i nomi di tali società e i nomi dei domini.

È possibile generare la richiesta CSR con un file di chiave privata corrispondente che deve rimanere nel gateway edge. La richiesta CSR contiene la chiave pubblica corrispondente e altre informazioni quali il nome, la posizione e il nome di dominio dell'organizzazione.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Certificati**.
- 3 Nella scheda **Certificati** fare clic su **CSR**.
- 4 Configurare le opzioni seguenti per la richiesta CSR:

Opzione	Descrizione
Nome comune	Immettere il nome di dominio completo per l'organizzazione per cui il certificato verrà utilizzato (ad esempio, <code>www.example.com</code>). Non includere i prefissi <code>http://</code> o <code>https://</code> nel nome comune.
Unità organizzativa	Utilizzare questo campo per distinguere le divisioni all'interno dell'organizzazione di VMware Cloud Director a cui questo certificato è associato. Ad esempio, Ufficio tecnico o Vendite.
Nome organizzazione	Immettere il nome con cui la società è legalmente registrata. L'organizzazione elencata deve essere l'entità che registra legalmente il nome di dominio indicato nella richiesta di certificato.
Località	Immettere la città o la località in cui l'azienda è legalmente registrata.
Nome stato o provincia	Immettere il nome completo (senza abbreviazioni) di stato, provincia, regione o territorio in cui l'azienda è legalmente registrata.
Codice paese	Immettere il nome del paese in cui l'azienda è legalmente registrata.
Algoritmo chiave privata	Digitare il tipo di chiave, RSA o DSA, per il certificato. In genere si utilizza RSA. Il tipo di chiave definisce l'algoritmo di crittografia per le comunicazioni tra host. Nota SSL VPN-Plus supporta solo certificati RSA.
Dimensione chiave	Immettere le dimensioni della chiave in bit. Il valore minimo è 2048 bit.
Descrizione	(Facoltativo) Immettere una descrizione per il certificato.

- 5 Fare clic su **Mantieni**.

Il sistema genera la richiesta CSR e aggiunge una nuova voce con tipo CSR all'elenco nella schermata.

Risultati

Quando si seleziona una voce con tipo CSR nell'elenco nella schermata, vengono visualizzati i dettagli della richiesta CSR. È possibile copiare i dati in formato PEM visualizzati della richiesta CSR e inoltrarli a un'autorità di certificazione (CA) per ottenere un certificato firmato da tale autorità.

Operazioni successive

Utilizzare la richiesta CSR per creare un certificato di servizio utilizzando una di queste due opzioni:

- Trasmettere la richiesta CSR a un'autorità di certificazione per ottenere un certificato firmato da tale autorità. Quando l'autorità di certificazione invia il certificato firmato, importarlo nel sistema. Vedere [Importazione del certificato firmato dall'autorità di certificazione corrispondente alla richiesta CSR generata per un gateway edge](#).
- Utilizzare la richiesta CSR per creare un certificato autofirmato. Vedere [Configurazione di un certificato di servizio autofirmato](#).

Importazione del certificato firmato dall'autorità di certificazione corrispondente alla richiesta CSR generata per un gateway edge

Dopo avere generato un richiesta di firma del certificato (CSR) e avere ottenuto il certificato firmato dall'autorità di certificazione in base a tale richiesta CSR, è possibile importare il certificato firmato dall'autorità di certificazione per consentirne l'utilizzo da parte del gateway edge.

Prerequisiti

Verificare di aver ottenuto il certificato firmato dall'autorità di certificazione corrispondente alla richiesta CSR. Se la chiave privata presente nel certificato firmato dall'autorità di certificazione non corrisponde a quella nella richiesta CSR selezionata, il processo di importazione non riesce.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Certificati**.
- 3 Nella tabella nella schermata, selezionare la richiesta CSR per cui si sta importando il certificato firmato dall'autorità di certificazione.
- 4 Importare il certificato firmato.
 - a Fare clic su **Certificato firmato generato per CSR**.
 - b Fornire i dati PEM del certificato firmato dall'autorità di certificazione.
 - Se i dati si trovano in un file PEM in un sistema accessibile, fare clic sul pulsante **Carica** per cercare il file e selezionarlo.
 - Se è possibile copiare e incollare i dati PEM, incollarli nel campo **Certificato firmato (formato PEM)**.

Includere le righe -----BEGIN CERTIFICATE----- e -----END CERTIFICATE-----.

- c (Facoltativo) Digitare una descrizione.
- d Fare clic su **Mantieni**.

Nota Se la chiave privata presente nel certificato firmato dall'autorità di certificazione non corrisponde a quella nella richiesta CSR selezionata nella schermata **Certificati**, il processo di importazione non riesce.

Risultati

Il certificato firmato dall'autorità di certificazione con tipo **Certificato di servizio** viene visualizzato nell'elenco nella schermata.

Operazioni successive

Collegare il certificato firmato dall'autorità di certificazione al tunnel SSL VPN-Plus o VPN IPsec in base alle esigenze. Vedere [Configurazione delle impostazioni del server VPN SSL](#) e [Come specificare le impostazioni VPN IPsec globali](#).

Configurazione di un certificato di servizio autofirmato

È possibile configurare certificati di servizio autofirmati con i gateway edge, per utilizzarli nelle funzionalità relative alla VPN. È possibile creare, installare e gestire certificati autofirmati.

Se il certificato di servizio è disponibile nella schermata **Certificati**, è possibile selezionarlo quando si configurano le impostazioni relative alla VPN del gateway edge. La VPN presenta il certificato di servizio specificato ai client che accedono alla VPN.

Prerequisiti

Verificare che almeno una richiesta CSR sia disponibile nella schermata **Certificati** per il gateway edge. Vedere [Generazione di una richiesta di firma del certificato per un gateway edge](#).

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Certificati**.
- 3 Nell'elenco, selezionare la richiesta di firma del certificato (CSR) che si desidera utilizzare per questo certificato autofirmato e fare clic su **CSR autofirmato**.
- 4 Digitare il numero di giorni per cui il certificato autofirmato è valido.
- 5 Fare clic su **Mantieni**.

Il sistema genera il certificato autofirmato e aggiunge una nuova voce con tipo **Certificato di servizio** all'elenco nella schermata.

Risultati

Il certificato autofirmato è disponibile nel gateway edge. Nell'elenco nella schermata, quando si seleziona una voce con tipo Certificato di servizio, i dettagli vengono visualizzati nella schermata.

Aggiunta di un certificato CA al gateway edge per la verifica di attendibilità dei certificati SSL

L'aggiunta di un certificato CA a un gateway edge consente la verifica di attendibilità dei certificati SSL presentati al gateway edge per l'autenticazione, in genere i certificati client utilizzati nelle connessioni VPN al gateway edge.

Il certificato root della società o dell'organizzazione viene in genere aggiunto come certificato CA. Un utilizzo tipico è per VPN SSL, quando si esegue l'autenticazione dei client VPN utilizzando i certificati. I certificati client possono essere distribuiti ai client VPN e quando i client VPN si connettono, i certificati client vengono convalidati in base al certificato CA.

Nota Quando si aggiunge un certificato CA, in genere si configura un elenco di revoche di certificati (Certificate Revocation List, CRL) pertinente. L'elenco CRL protegge dai client che presentano certificati revocati. Vedere [Aggiunta di un elenco di revoche di certificati a un gateway edge](#).

Prerequisiti

Verificare che i dati del certificato CA siano in formato PEM. Nell'interfaccia utente, è possibile incollare i dati PEM del certificato CA o selezionare un file che contenga i dati e sia disponibile in rete dal sistema locale.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Certificati**.
- 3 Fare clic su **Certificato CA**.
- 4 Fornire i dati del certificato CA.
 - Se i dati si trovano in un file PEM in un sistema accessibile, fare clic sul pulsante **Carica** per cercare il file e selezionarlo.
 - Se è possibile copiare e incollare i dati PEM, incollarli nel campo **Certificato CA (formato PEM)**.
 Includere le righe `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----`.
- 5 (Facoltativo) Digitare una descrizione.
- 6 Fare clic su **Mantieni**.

Risultati

Il certificato CA con tipo Certificato CA viene visualizzato nell'elenco nella schermata. È ora possibile specificare questo certificato CA quando si configurano le impostazioni relative alla rete VPN del gateway edge.

Aggiunta di un elenco di revoche di certificati a un gateway edge

Un elenco di revoche di certificati (CRL) è un elenco di certificati digitali che l'autorità di certificazione (CA) emittente afferma di avere revocato, così che i sistemi possano essere aggiornati in modo che non considerino attendibili gli utenti che presentano i certificati revocati. È possibile aggiungere CRL al gateway edge.

Come descritto nella *Guida per l'amministratore di NSX*, l'elenco CRL contiene i seguenti elementi:

- I certificati revocati e i motivi della revoca
- Le date di rilascio dei certificati
- Le entità che hanno emesso i certificati
- Una data proposta per la versione successiva

Quando un utente potenziale tenta di accedere a un server, il server consente o nega l'accesso in base alla voce CRL per tale utente specifico.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Certificati**.
- 3 Fare clic su **CRL**.
- 4 Fornire i dati del CRL.
 - Se i dati si trovano in un file PEM in un sistema accessibile, fare clic sul pulsante **Carica** per cercare il file e selezionarlo.
 - Se è possibile copiare e incollare i dati PEM, incollarli nel campo **CRL (formato PEM)**.
Includere le righe -----BEGIN X509 CRL----- e -----END X509 CRL-----.
- 5 (Facoltativo) Digitare una descrizione.
- 6 Fare clic su **Mantieni**.

Risultati

L'elenco CRL viene visualizzato nell'elenco nella schermata.

Aggiunta di un certificato di servizio al gateway edge

L'aggiunta di certificati di servizio a un gateway edge rende tali certificati disponibili per l'uso nelle impostazioni relative alla VPN del gateway edge. È possibile aggiungere un certificato di servizio nella schermata **Certificati**.

Prerequisiti

Verificare di disporre del certificato di servizio e della relativa chiave privata in formato PEM.

Nell'interfaccia utente, è possibile incollare i dati PEM o selezionare un file che contenga i dati e sia disponibile in rete dal sistema locale.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Certificati**.
- 3 Fare clic su **Certificato di servizio**.
- 4 Immettere i dati in formato PEM del certificato di servizio.
 - Se i dati si trovano in un file PEM in un sistema accessibile, fare clic sul pulsante **Carica** per cercare il file e selezionarlo.
 - Se è possibile copiare e incollare i dati PEM, incollarli nel campo **Certificato di servizio (formato PEM)**.
Includere le righe **-----BEGIN CERTIFICATE-----** e **-----END CERTIFICATE-----**.
- 5 Immettere i dati in formato PEM della chiave privata del certificato.

Quando è attivata la modalità FIPS, le dimensioni delle chiavi RSA devono essere maggiori o uguali a 2048 bit.

 - Se i dati si trovano in un file PEM in un sistema accessibile, fare clic sul pulsante **Carica** per cercare il file e selezionarlo.
 - Se è possibile copiare e incollare i dati PEM, incollarli nel campo **Chiave privata (formato PEM)**.
Includere le righe **-----BEGIN RSA PRIVATE KEY-----** e **-----END RSA PRIVATE KEY-----**.
- 6 Immettere una passphrase della chiave privata e confermarla.
- 7 (Facoltativo) Immettere una descrizione.
- 8 Fare clic su **Mantieni**.

Risultati

Il certificato con tipo Certificato di servizio viene visualizzato nell'elenco nella schermata. È ora possibile selezionare questo certificato di servizio quando si configurano le impostazioni relative alla VPN del gateway edge.

Raggruppamento personalizzato di oggetti per i gateway edge di NSX Data Center for vSphere

Il software NSX Data Center for vSphere nell'ambiente VMware Cloud Director fornisce una funzionalità che consente di definire set e gruppi di entità specifiche, che possono quindi essere utilizzati quando si specificano altre configurazioni correlate alla rete, ad esempio nelle regole del firewall.

Creazione di un set di IP da utilizzare nelle regole del firewall e nella configurazione dell'inoltro DHCP

Un set di IP è un gruppo di indirizzi IP che è possibile creare a livello di virtual data center dell'organizzazione. È possibile utilizzare un set di IP come origine o destinazione in una regola del firewall o in una configurazione di inoltro DHCP.

È possibile creare un set di IP utilizzando la pagina **Raggruppamento di oggetti** del portale tenant di VMware Cloud Director. La pagina **Raggruppamento di oggetti** è disponibile sia nella schermata Servizi sia nella schermata Gateway edge.

Procedura

- 1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Apri tramite i servizi del gateway edge	<ol style="list-style-type: none"> a Passare a Rete > Edge. b Selezionare il gateway edge da modificare e fare clic su Configura servizi. c Fare clic su Raggruppamento di oggetti.
Apri tramite i servizi di sicurezza	<ol style="list-style-type: none"> a Passare a Rete > Sicurezza. b Selezionare il servizio di sicurezza da modificare e fare clic su Configura servizi. c Fare clic su Raggruppamento di oggetti.

- 2 Fare clic sulla scheda **Set di IP**.

Nella schermata vengono visualizzati i set di IP che sono già stati definiti.

- 3 Per aggiungere un set di IP, fare clic sul pulsante **Crea** ()

- 4 Immettere un nome e, facoltativamente, una descrizione per il set di IP, nonché gli indirizzi IP da includere nel set.

- 5 (Facoltativo) Se si specifica il set di IP utilizzando la pagina **Raggruppamento di oggetti** nella schermata Servizi, utilizzare il pulsante di opzione **Ereditarietà** per abilitare l'ereditarietà e consentire la visibilità a livello degli ambiti sottostanti.

L'ereditarietà è abilitata per impostazione predefinita.

- 6 Per salvare questo set di IP, fare clic su **Mantieni**.

Risultati

Il nuovo set di IP è disponibile per essere selezionato come origine o destinazione nelle regole del firewall o nelle configurazioni dell'inoltro DHCP.

Creazione di un set di MAC da utilizzare nelle regole del firewall

Un set di MAC è un gruppo di indirizzi MAC che è possibile creare a livello del virtual data center di un'organizzazione. È possibile utilizzare un set di MAC come origine o destinazione in una regola del firewall.

È possibile creare un set di MAC utilizzando la pagina **Raggruppamento di oggetti** del portale tenant di VMware Cloud Director. La pagina Raggruppamento di oggetti è disponibile sia nella schermata **Servizi** sia nella schermata **Gateway edge**.


Procedura

- 1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Apri tramite i servizi del gateway edge	a Passare a Rete > Edge .
	b Selezionare il gateway edge da modificare e fare clic su Configura servizi .
	c Fare clic su Raggruppamento di oggetti .
Apri tramite i servizi di sicurezza	a Passare a Rete > Sicurezza .
	b Selezionare il servizio di sicurezza da modificare e fare clic su Configura servizi .
	c Fare clic su Raggruppamento di oggetti .

- 2 Fare clic sulla scheda **Set di MAC**.

Nella schermata vengono visualizzati i set di MAC che sono già stati definiti.

- 3 Per aggiungere un set di MAC, fare clic sul pulsante **Crea** ()
- 4 Immettere un nome per il set, una descrizione facoltativa e gli indirizzi MAC da includere nel set.
- 5 (Facoltativo) Se si specifica il set di MAC utilizzando la pagina **Raggruppamento di oggetti** nella schermata **Servizi**, utilizzare l'interruttore **Ereditarietà** per abilitare l'ereditarietà e consentire la visibilità negli ambiti sottostanti.

L'ereditarietà è abilitata per impostazione predefinita.

- 6 Per salvare il set di MAC, fare clic su **Mantieni**.

Risultati

Il nuovo set di MAC è disponibile per essere selezionato come origine o destinazione nelle regole del firewall.

Visualizzazione dei servizi disponibili per le regole del firewall

È possibile visualizzare l'elenco dei servizi che possono essere utilizzati nelle regole del firewall. In questo contesto, un servizio è una combinazione di protocollo e porta.

È possibile visualizzare i gruppi di servizi disponibili utilizzando la pagina Raggruppamento di oggetti del portale tenant di VMware Cloud Director. La pagina Raggruppamento di oggetti è disponibile sia nella schermata Servizi sia nella schermata Gateway edge.

Non è possibile aggiungere nuovi servizi all'elenco utilizzando il portale tenant. L'insieme di servizi che è possibile utilizzare viene gestito dall'amministratore di sistema di VMware Cloud Director.

Procedura

1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Apri tramite i servizi del gateway edge	a Passare a Rete > Edge .
	b Selezionare il gateway edge da modificare e fare clic su Configura servizi .
	c Fare clic su Raggruppamento di oggetti .
Apri tramite i servizi di sicurezza	a Passare a Rete > Sicurezza .
	b Selezionare il servizio di sicurezza da modificare e fare clic su Configura servizi .
	c Fare clic su Raggruppamento di oggetti .

2 Fare clic sulla scheda **Servizi**.

Risultati

La schermata include i servizi disponibili.

Visualizzazione dei gruppi di servizi disponibili per le regole del firewall

È possibile visualizzare l'elenco dei gruppi di servizi che possono essere utilizzati nelle regole del firewall. In questo contesto, un servizio è una combinazione di protocollo e porta e un gruppo di servizi è un gruppo che include servizi o altri gruppi di servizi.

È possibile visualizzare i gruppi di servizi disponibili utilizzando la pagina Raggruppamento di oggetti del portale tenant di VMware Cloud Director. La pagina Raggruppamento di oggetti è disponibile sia nella schermata Servizi sia nella schermata Gateway edge.

Non è possibile creare nuovi gruppi di servizi tramite il portale tenant. L'insieme di gruppi di servizi che è possibile utilizzare viene gestito dall'amministratore di sistema di VMware Cloud Director.

Procedura**1** Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Apri tramite i servizi del gateway edge	a Passare a Rete > Edge .
	b Selezionare il gateway edge da modificare e fare clic su Configura servizi .
	c Fare clic su Raggruppamento di oggetti .
Apri tramite i servizi di sicurezza	a Passare a Rete > Sicurezza .
	b Selezionare il servizio di sicurezza da modificare e fare clic su Configura servizi .
	c Fare clic su Raggruppamento di oggetti .

2 Fare clic sulla scheda **Gruppi di servizi**.**Risultati**

La schermata include i gruppi di servizi disponibili. Nella colonna Descrizione sono visualizzati i servizi raggruppati in ciascun gruppo di servizi.

Statistiche e registri per un gateway edge di NSX Data Center for vSphere

È possibile visualizzare le statistiche e i registri per un gateway edge di NSX Data Center for vSphere.

Visualizzazione delle statistiche

È possibile visualizzare le statistiche nella schermata **Servizi gateway edge**.

Procedura**1** Aprire i servizi gateway edge.

- a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
- b Selezionare il gateway edge da modificare e fare clic su **Servizi**.

2 Fare clic sulla scheda **Statistiche**.

3 Esaminare le schede in base al tipo di statistiche desiderate.

Opzione	Descrizione
Connessioni	La schermata Connessioni fornisce la visibilità operativa. In questa schermata vengono visualizzati i grafici del flusso del traffico tra le interfacce del gateway edge selezionato e per il firewall. Selezionare il periodo in base a cui si desidera visualizzare le statistiche.
VPN IPsec	Nella schermata VPN IPsec vengono visualizzati lo stato e le statistiche della rete VPN IPsec, nonché lo stato e le statistiche di ciascun tunnel.
VPN L2	Nella schermata VPN L2 vengono visualizzati lo stato e le statistiche della rete VPN L2.

Abilitazione della registrazione

È possibile abilitare la registrazione per un gateway edge. Oltre ad abilitare la registrazione per le funzionalità per cui si desidera raccogliere i dati del registro, per completare la configurazione è necessario disporre di un server syslog per ricevere i dati del registro raccolti. Quando si configura un server syslog nella schermata Impostazioni edge, è possibile accedere ai dati registrati da tale server.

Prerequisiti

- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare che il proprio ruolo includa il diritto **Configura registrazione sistema**.

Procedura

1 Aprire i servizi gateway edge.

- Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
- Selezionare il gateway edge da modificare e fare clic su **Servizi**.

2 Nella scheda **Impostazioni edge** fare clic sul pulsante **Modifica server syslog**.

È possibile personalizzare il server syslog per i registri correlati alla rete del gateway edge per i servizi in cui è abilitata la registrazione.

Se l'amministratore di sistema di VMware Cloud Director ha già configurato un server syslog per l'ambiente VMware Cloud Director il sistema utilizza tale server per impostazione predefinita e il relativo indirizzo IP viene visualizzato nella schermata **Impostazioni edge**.

3 Abilitare la registrazione per funzionalità.

- Nella scheda **NAT** fare clic sul pulsante **Regola DNAT** e attivare l'opzione **Abilita registrazione**.
Consente di registrare la conversione degli indirizzi.
- Nella scheda **NAT** fare clic sul pulsante **Regola SNAT** e attivare l'opzione **Abilita registrazione**.

Consente di registrare la conversione degli indirizzi.

- Nella scheda **Routing** fare clic su **Configurazione routing** e in Configurazione routing dinamico attivare l'opzione **Abilita registrazione**.

Consente di registrare le attività di routing dinamico. Dal menu a discesa **Livello di registrazione** è possibile selezionare il limite inferiore del livello dello stato del messaggio da registrare.

- Nella scheda **Bilanciamento del carico** fare clic su **Configurazione globale** e attivare l'opzione **Abilita registrazione**.

Consente di registrare il flusso del traffico per il bilanciamento del carico. Dal menu a discesa **Livello di registrazione** è possibile selezionare il limite inferiore del livello dello stato del messaggio da registrare.

- Nella scheda **VPN** passare a **VPN IPsec > Impostazioni di registrazione** e attivare l'opzione **Abilita registrazione**.

Consente di registrare il flusso del traffico tra la subnet locale e la subnet peer. Dal menu a discesa **Livello di registrazione** è possibile selezionare il limite inferiore del livello dello stato del messaggio da registrare.

- Nella scheda **VPN SSL plus** fare clic su **Impostazioni generali** e attivare l'opzione **Abilita registrazione**.

Consente di mantenere un registro del traffico che passa attraverso il gateway VPN SSL.

- Nella scheda **VPN SSL plus** fare clic su **Impostazioni server** e attivare l'opzione **Abilita registrazione**.

Consente di registrare le attività eseguite nel server VPN SSL per syslog. Dal menu a discesa **Livello di registrazione** è possibile selezionare il limite inferiore del livello dello stato del messaggio da registrare.

Abilitazione dell'accesso a un gateway edge di NSX Data Center for vSphere dalla riga di comando SSH

È possibile abilitare l'accesso dalla riga di comando SSH a un gateway edge.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore fare clic su **Rete** e su **Gateway edge**.
 - b Selezionare il gateway edge da modificare e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Impostazioni edge**.

3 Configurare le impostazioni di SSH.

Opzione	Descrizione
Nome utente	Immettere le credenziali per l'accesso SSH a questo gateway edge.
Password	Per impostazione predefinita, il nome utente SSH è admin .
Ridigita password	
Scadenza password	Immettere la durata della password, in giorni.
Banner di accesso	Immettere il testo che sarà visualizzato dagli utenti quando avviano una connessione SSH al gateway edge.

4 Attivare l'interruttore **Abilitato**.

Operazioni successive

Configurare il NAT o le regole del firewall appropriate per consentire l'accesso SSH a questo gateway edge.

Utilizzo dei tag di sicurezza per i gateway edge di NSX Data Center for vSphere

I tag di sicurezza sono etichette che è possibile associare a una macchina virtuale o a un gruppo di macchine virtuali. I tag di sicurezza sono progettati per essere utilizzati con i gruppi di sicurezza. Una volta creati, i tag di sicurezza possono essere associati a un gruppo di sicurezza utilizzabile nelle regole del firewall. È possibile creare, modificare o assegnare un tag di sicurezza definito dall'utente, nonché visualizzare le macchine virtuali o i gruppi di sicurezza a cui è applicato un determinato tag di sicurezza.

I tag di sicurezza vengono generalmente utilizzati per raggruppare dinamicamente oggetti per semplificare le regole del firewall. Ad esempio, è possibile creare tag di sicurezza diversi in base al tipo di attività che verrà eseguita in una determinata macchina virtuale. È possibile creare un tag di sicurezza per i server di database e un altro per i server di posta elettronica. È quindi necessario applicare il tag appropriato alle macchine virtuali che ospitano i server di database o i server di posta elettronica. In seguito, è possibile assegnare il tag a un gruppo di sicurezza e scrivere una regola del firewall in base a tale gruppo, applicando impostazioni di sicurezza diverse a seconda che sulla macchina virtuale sia in esecuzione un server di database o un server di posta elettronica. Successivamente, se si modifica la funzionalità della macchina virtuale, è possibile rimuovere la macchina virtuale dal tag di sicurezza, anziché modificare la regola del firewall.


Creazione e assegnazione di tag di sicurezza

È possibile creare un tag di sicurezza e assegnarlo a una macchina virtuale o a un gruppo di macchine virtuali.

Creare un tag di sicurezza e assegnarlo a una macchina virtuale o a un gruppo di macchine virtuali.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.
- 2 Selezionare un servizio di sicurezza e fare clic su **Configura servizi**.
- 3 Fare clic sulla scheda **Tag di sicurezza**.

- 4 Fare clic sul pulsante **Crea** () e immettere un nome per il tag di sicurezza.
- 5 (Facoltativo) Immettere una descrizione per il tag di sicurezza.
- 6 (Facoltativo) Assegnare il tag di sicurezza a una macchina virtuale o a un gruppo di macchine virtuali.

Nel menu a discesa **Sfoglia oggetti di tipo** l'opzione **Macchine virtuali** è selezionata per impostazione predefinita.

- a Selezionare una macchina virtuale nel pannello sinistro.
- b Assegnare il tag di sicurezza alla macchina virtuale selezionata facendo clic sulla freccia destra.

La macchina virtuale viene spostata nel pannello destro e le viene assegnato il tag di sicurezza.

- 7 Una volta completata l'assegnazione del tag alle macchine virtuali selezionate, fare clic su **Mantieni**.

Risultati

Il tag di sicurezza viene creato e viene quindi assegnato alle macchine virtuali selezionate, se si sceglie questa opzione.

Operazioni successive

I tag di sicurezza sono progettati per l'utilizzo con un gruppo di sicurezza. Per ulteriori informazioni sulla creazione di gruppi di sicurezza, vedere [Creazione di un gruppo di sicurezza](#).

Modifica dell'assegnazione del tag di sicurezza

Dopo avere creato un tag di sicurezza, è possibile assegnarlo manualmente alle macchine virtuali. È inoltre possibile modificare un tag di sicurezza per rimuoverlo dalle macchine virtuali a cui è stato assegnato.

Se sono stati creati tag di sicurezza, è possibile assegnarli alle macchine virtuali. È possibile utilizzare i tag di sicurezza per raggruppare macchine virtuali per la scrittura di regole del firewall. Ad esempio, è possibile assegnare un tag di sicurezza a un gruppo di macchine virtuali con dati estremamente sensibili.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.
- 2 Selezionare un servizio di sicurezza e fare clic su **Configura servizi**.
- 3 Fare clic sulla scheda **Tag di sicurezza**.
- 4 Nell'elenco dei tag di sicurezza selezionare il tag di sicurezza che si desidera modificare e fare clic sul pulsante **Modifica**.
- 5 Selezionare le macchine virtuali dal pannello a sinistra e assegnare il tag di sicurezza facendo clic sulla freccia a destra.

Alle macchine virtuali nel pannello a destra viene assegnato il tag di sicurezza.
- 6 Selezionare le macchine virtuali nel pannello a destra e rimuovere il tag da tali macchine facendo clic sulla freccia a sinistra.

Alle macchine virtuali nel pannello a sinistra non è assegnato il tag di sicurezza.
- 7 Una volta terminate le modifiche, fare clic su **Mantieni**.

Risultati

Il tag di sicurezza viene assegnato alle macchine virtuali selezionate.

Operazioni successive

I tag di sicurezza sono progettati per l'utilizzo con un gruppo di sicurezza. Per ulteriori informazioni sulla creazione di gruppi di sicurezza, vedere [Creazione di un gruppo di sicurezza](#).

Visualizzazione dei tag di sicurezza applicati

È possibile visualizzare i tag di sicurezza applicati alle macchine virtuali nell'ambiente in uso. È inoltre possibile visualizzare i tag di sicurezza che vengono applicati ai gruppi di sicurezza nell'ambiente in uso.

Prerequisiti

È necessario che un tag di sicurezza sia stato creato e applicato a una macchina virtuale o a un gruppo di sicurezza.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.
- 2 Selezionare un servizio di sicurezza e fare clic su **Configura servizi**.

3 I tag assegnati possono essere visualizzati nella scheda **Tag di sicurezza**.

- a Nella scheda **Tag di sicurezza**, selezionare il tag di sicurezza di cui si desidera visualizzare le assegnazioni e fare clic sull'icona **Modifica**.
- b Nella sezione **Assegna/annulla assegnazione macchine virtuali** è disponibile l'elenco delle macchine virtuali assegnate al tag di sicurezza.
- c Fare clic su **Ignora**.

4 Visualizzare i tag assegnati nella scheda **Gruppi di sicurezza**.

- a Selezionare la scheda **Raggruppamento di oggetti** e fare clic su **Gruppi di sicurezza**.
- b Selezionare un gruppo di sicurezza.
- c Nell'elenco in **Includi membri** è possibile vedere il tag di sicurezza assegnato a un gruppo di sicurezza.

Risultati

È possibile visualizzare i tag di sicurezza esistenti e le macchine virtuali e i gruppi di sicurezza associati. In questo modo è possibile definire una strategia per la creazione di regole del firewall in base ai tag e ai gruppi di sicurezza.

Modifica di un tag di sicurezza

È possibile modificare i tag di sicurezza definiti dall'utente.

Se si modifica l'ambiente o la funzione di una macchina virtuale, è consigliabile utilizzare un tag di sicurezza diverso, per fare in modo che le regole del firewall siano appropriate per la nuova configurazione della macchina. Ad esempio, se si dispone di una macchina virtuale in cui non si archiviano più dati sensibili, è consigliabile assegnarle un tag di sicurezza diverso in modo che le regole firewall che vengono applicate ai dati sensibili non vengano più applicate a tale macchina virtuale.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.
- 2 Selezionare un servizio di sicurezza e fare clic su **Configura servizi**.
- 3 Fare clic sulla scheda **Tag di sicurezza**.
- 4 Nell'elenco dei tag di sicurezza, selezionare il tag di sicurezza che si desidera modificare.
- 5 Fare clic sul pulsante **Modifica**.
- 6 Modificare il nome e la descrizione del tag di sicurezza.
- 7 Assegnare il tag o rimuovere l'assegnazione per le macchine virtuali selezionate.
- 8 Per salvare le modifiche, fare clic su **Mantieni**.

Operazioni successive

Se si modifica un tag di sicurezza, potrebbe essere necessario modificare anche un gruppo di sicurezza o le regole del firewall associati. Per ulteriori informazioni sui gruppi di sicurezza, vedere [Utilizzo dei gruppi di sicurezza per i gateway edge di NSX Data Center for vSphere](#).

Eliminazione di un tag di sicurezza

È possibile eliminare un tag di sicurezza definito dall'utente.

È consigliabile eliminare un tag di sicurezza se la funzione o l'ambiente della macchina virtuale cambia. Ad esempio, se è presente un tag di sicurezza per i database Oracle, ma si decide di utilizzare un server database diverso, è possibile rimuovere il tag di sicurezza in modo che le regole del firewall relative ai database Oracle non vengano più applicate alla macchina virtuale.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e in **Reti** selezionare **Sicurezza**.
- 2 Selezionare un servizio di sicurezza e fare clic su **Configura servizi**.
- 3 Fare clic sulla scheda **Tag di sicurezza**.
- 4 Nell'elenco dei tag di sicurezza, selezionare il tag di sicurezza che si desidera eliminare.
- 5 Fare clic sul pulsante **Elimina**.
- 6 Per confermare l'eliminazione, fare clic su **OK**.

Risultati

Il tag di sicurezza viene eliminato.

Operazioni successive

Se si elimina un tag di sicurezza, potrebbe essere necessario modificare anche un gruppo di sicurezza o le regole firewall associati. Per ulteriori informazioni sui gruppi di sicurezza, vedere [Utilizzo dei gruppi di sicurezza per i gateway edge di NSX Data Center for vSphere](#).

Utilizzo dei gruppi di sicurezza per i gateway edge di NSX Data Center for vSphere

Un gruppo di sicurezza è una raccolta di asset o un raggruppamento di oggetti, ad esempio macchine virtuali, reti di virtual data center dell'organizzazione o tag di sicurezza.

I gruppi di sicurezza possono avere criteri di appartenenza dinamica basati su tag di sicurezza, nome della macchina virtuale, nome del sistema operativo guest della macchina virtuale o nome host guest della macchina virtuale. Ad esempio, tutte le macchine virtuali con tag di sicurezza "Web" verranno automaticamente aggiunte a un gruppo di sicurezza specifico destinato ai server Web. Una volta creato un gruppo di sicurezza, a tale gruppo viene applicato un criterio di sicurezza.

Creazione di un gruppo di sicurezza

È possibile creare gruppi di sicurezza definiti dall'utente.

Prerequisiti

Se si desidera utilizzare tag di sicurezza con gruppi di sicurezza, [Creazione e assegnazione di tag di sicurezza](#).

Procedura

- 1 Aprire i servizi di sicurezza.

- a Passare a **Rete > Sicurezza**.
- b Selezionare il VDC dell'organizzazione a cui si desidera applicare le impostazioni di sicurezza e fare clic su **Configura servizi**.

Nel portale tenant viene aperta la schermata Servizi di sicurezza.

- 2 Passare a **Raggruppamento di oggetti > Gruppi di sicurezza**


Viene aperta la pagina **Gruppi di sicurezza**.

- 3 Fare clic sul pulsante **Crea** ()

- 4 Immettere un nome e, facoltativamente, una descrizione per il gruppo di sicurezza.

Poiché la descrizione viene visualizzata nell'elenco dei gruppi di sicurezza, se si aggiunge una descrizione significativa, è possibile individuare più facilmente il gruppo di sicurezza.

- 5 (Facoltativo) Aggiungere un set di membri dinamici.

- a Fare clic sul pulsante **Aggiungi** () in Set di membri dinamici.
- b Selezionare se si desidera che venga soddisfatto **Qualsiasi** criterio o **Tutti** i criteri nell'istruzione.
- c Immettere il primo oggetto per cui deve essere trovata una corrispondenza.
Le opzioni sono **Tag di sicurezza**, **Nome sistema operativo guest macchina virtuale**, **Nome macchina virtuale** e **Nome host guest macchina virtuale**.
- d Selezionare un operatore, ad esempio **Contiene**, **Inizia con** o **Termina con**.
- e Immettere un valore.
- f (Facoltativo) Per aggiungere un'altra istruzione, utilizzare un operatore booleano **AND** o **OR**.

6 (Facoltativo) Includere i membri.

- a Dal menu a discesa **Sfoglia oggetti di tipo** selezionare il tipo di oggetti, ad esempio **Macchine virtuali, Reti VDC dell'organizzazione, Set di IP, Set di MAC o Tag di sicurezza.**
- b Per includere un oggetto nell'elenco Includi membri, selezionare l'oggetto nel pannello sinistro e spostarlo nel pannello destro facendo clic sulla freccia destra.

7 (Facoltativo) Escludere i membri.

- a Dal menu a discesa **Sfoglia oggetti di tipo** selezionare il tipo di oggetti, ad esempio **Macchine virtuali, Reti VDC dell'organizzazione, Set di IP, Set di MAC o Tag di sicurezza.**
- b Per includere un oggetto nell'elenco Escludi membri, selezionare l'oggetto nel pannello sinistro e spostarlo nel pannello destro facendo clic sulla freccia destra.

8 Per salvare le modifiche, fare clic su **Mantieni.**

Risultati

Il gruppo di sicurezza può ora essere utilizzato nelle regole, ad esempio le regole del firewall.

Modifica di un gruppo di sicurezza

È possibile modificare i gruppi di sicurezza definiti dall'utente.

Procedura

1 Aprire i servizi di sicurezza.

- a Passare a **Rete > Sicurezza.**
- b Selezionare il VDC dell'organizzazione a cui si desidera applicare le impostazioni di sicurezza e fare clic su **Configura servizi.**

Nel portale tenant viene aperta la schermata Servizi di sicurezza.

2 Passare a **Raggruppamento di oggetti > Gruppi di sicurezza**

Viene aperta la pagina **Gruppi di sicurezza.**

3 Selezionare il gruppo di sicurezza che si desidera modificare.

I dettagli del gruppo di sicurezza vengono visualizzati al di sotto dell'elenco dei gruppi di sicurezza.

4 (Facoltativo) Modificare il nome e la descrizione del gruppo di sicurezza.

5 (Facoltativo) Aggiungere un set di membri dinamici.

- a Fare clic sul pulsante **Aggiungi** in **Set di membri dinamici.**
- b Selezionare se si desidera che venga soddisfatto **Qualsiasi** criterio o **Tutti** i criteri nell'istruzione.

- c Immettere il primo oggetto per cui deve essere trovata una corrispondenza.
Le opzioni sono **Tag di sicurezza**, **Nome sistema operativo guest macchina virtuale**, **Nome macchina virtuale** e **Nome host guest macchina virtuale**.
 - d Selezionare un operatore, ad esempio **Contiene**, **Inizia con** o **Termina con**.
 - e Immettere un valore.
 - f (Facoltativo) Per aggiungere un'altra istruzione, utilizzare un operatore booleano **AND** o **OR**.
- 6 (Facoltativo) Modificare un set di membri dinamici facendo clic sull'icona **Modifica** accanto al set di membri che si desidera modificare.
 - a Applicare le modifiche necessarie al set di membri dinamici.
 - b Fare clic su **OK**.
 - 7 (Facoltativo) Eliminare un set di membri dinamici facendo clic sull'icona **Elimina** accanto al set di membri che si desidera eliminare.
 - 8 (Facoltativo) Modificare l'elenco dei membri inclusi facendo clic sull'icona **Modifica** accanto all'elenco Includi membri.
 - a Dal menu a discesa **Sfoggia oggetti di tipo** selezionare il tipo di oggetti, ad esempio **Macchine virtuali**, **Reti VDC dell'organizzazione**, **Set di IP**, **Set di MAC** o **Tag di sicurezza**.
 - b Per includere un oggetto nell'elenco Includi membri, selezionare l'oggetto nel pannello sinistro e spostarlo nel pannello destro facendo clic sulla freccia destra.
 - c Per escludere un oggetto dall'elenco Includi membri, selezionare l'oggetto nel pannello destro e spostarlo nel pannello sinistro facendo clic sulla freccia sinistra.
 - 9 (Facoltativo) Modificare l'elenco dei membri esclusi facendo clic sull'icona **Modifica** accanto all'elenco Escludi membri.
 - a Dal menu a discesa **Sfoggia oggetti di tipo** selezionare il tipo di oggetti, ad esempio **Macchine virtuali**, **Reti VDC dell'organizzazione**, **Set di IP**, **Set di MAC** o **Tag di sicurezza**.
 - b Per includere un oggetto nell'elenco Escludi membri, selezionare l'oggetto nel pannello sinistro e spostarlo nel pannello destro facendo clic sulla freccia destra.
 - c Per escludere un oggetto dall'elenco Escludi membri, selezionare l'oggetto nel pannello destro e spostarlo nel pannello sinistro facendo clic sulla freccia sinistra.
 - 10 Fare clic su **Salva modifiche**.

Le modifiche apportate al gruppo di sicurezza vengono salvate.

Eliminazione di un gruppo di sicurezza

È possibile eliminare un gruppo di sicurezza definito dall'utente.

Procedura

- 1 Aprire i servizi di sicurezza.
 - a Passare a **Rete > Sicurezza**.
 - b Selezionare il VDC dell'organizzazione a cui si desidera applicare le impostazioni di sicurezza e fare clic su **Configura servizi**.

Nel portale tenant viene aperta la schermata Servizi di sicurezza.

- 2 Passare a **Raggruppamento di oggetti > Gruppi di sicurezza**

Viene aperta la pagina **Gruppi di sicurezza**.

- 3 Selezionare il gruppo di sicurezza che si desidera eliminare.
- 4 Fare clic sul pulsante **Elimina**.
- 5 Per confermare l'eliminazione, fare clic su **OK**.

Risultati

Il gruppo di sicurezza viene eliminato.

Gestione dei gateway edge NSX-T Data Center

Un gateway edge di NSX-T Data Center fornisce una rete VDC dell'organizzazione instradata o una rete di gruppi di data center con connettività a reti esterne e proprietà di gestione IP. Può inoltre fornire servizi quali firewall, Network Address Translation (NAT), VPN IPSec, inoltre DNS e DHCP, abilitato per impostazione predefinita.

Reti esterne dedicate

Per fornire una topologia di rete completamente instradata in un virtual data center, l'**amministratore di sistema** può dedicare una rete esterna a un gateway edge NSX-T Data Center specifico.

In questa configurazione, è presente una relazione one-to-one tra la rete esterna e il gateway edge NSX-T Data Center e nessun altro gateway edge può connettersi alla rete esterna.

Un router logico di livello 0 NSX-T Data Center o un gateway VRF associato a una rete esterna dedicata fa parte dello stack di rete del tenant. La rete esterna è considerata parte del dominio di routing della rete di VMware Cloud Director.

Una rete esterna dedicata fornisce servizi di routing del gateway edge aggiuntivi, come la gestione della comunicazione della route e la configurazione di BGP (Border Gateway Protocol).

È possibile decidere quale delle reti collegate al gateway edge comunicare alla rete esterna. Ciò rende possibile una combinazione di reti di virtual data center dell'organizzazione con instradamento NAT e completamente instradate.

Aggiunta di un set di IP a un gateway edge di NSX-T Data Center

Per creare regole del firewall e aggiungerle a un gateway edge di NSX-T Data Center, è innanzitutto necessario creare set di IP. I set di IP sono gruppi di oggetti a cui si applicano le regole del firewall. La combinazione di più oggetti in set di IP consente di ridurre il numero totale di regole del firewall da creare.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge NSX-T.
- 3 In **Sicurezza**, fare clic sulla scheda **Set di IP**, quindi fare clic su **Nuovo**.
- 4 Immettere un nome e, facoltativamente, una descrizione per il set di IP.
- 5 Immettere un indirizzo IP o un intervallo di indirizzi IP per le macchine virtuali incluse nel set di IP e fare clic su **Aggiungi**.
- 6 Per salvare il gruppo di firewall, fare clic su **Salva**.

Risultati

Un set di IP è stato creato e aggiunto al gateway edge NSX-T.

Operazioni successive

[Aggiunta di una regola del firewall del gateway edge NSX-T Data Center](#)

Aggiunta di una regola del firewall del gateway edge NSX-T Data Center

Per controllare il traffico di rete in entrata e in uscita da e verso un gateway edge NSX-T Data Center, è possibile creare regole del firewall.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 Se la schermata **Firewall** non è già visualizzata nella sezione Servizi, fare clic sulla scheda **Firewall**.
- 4 Fare clic su **Modifica regole**.
- 5 Fare clic sul pulsante **Nuova in cima**.

Viene aggiunta una riga per la nuova regola sopra la regola selezionata.

6 Configurare la regola del firewall.

Opzione	Descrizione
Nome	Immettere un nome per la regola.
Stato	Per abilitare la regola al momento della creazione, attivare l'interruttore Stato .
Applicazioni	(Opzionale) Per selezionare un profilo di porta specifico a cui applicare la regola, attivare l'interruttore Applicazioni e fare clic su Salva .
Origine	<p>Scegliere un'opzione e fare clic su Mantieni.</p> <ul style="list-style-type: none"> ■ Per consentire o impedire il traffico da qualsiasi indirizzo di origine, attivare Qualsiasi origine. ■ Per consentire o negare il traffico proveniente da gruppi di firewall specifici, selezionare i gruppi di firewall nell'elenco.
Destinazione	<p>Scegliere un'opzione e fare clic su Mantieni.</p> <ul style="list-style-type: none"> ■ Per consentire o negare il traffico verso qualsiasi indirizzo di destinazione, attivare Qualsiasi destinazione. ■ Per consentire o negare il traffico verso gruppi di firewall specifici, selezionare i gruppi di firewall nell'elenco.
Azione	<p>Dal menu a discesa Azione, selezionare un'opzione.</p> <ul style="list-style-type: none"> ■ Selezionare Accetta per consentire il traffico da o verso le origini, le destinazioni e i servizi specificati. ■ Selezionare Nega per bloccare il traffico da o verso le origini, le destinazioni e i servizi specificati senza informare il client bloccato. ■ Selezionare Rifiuta per bloccare il traffico da o verso le origini, le destinazioni e i servizi specificati informando il client bloccato che il traffico è stato rifiutato.
Protocollo IP	Selezionare se applicare la regola al traffico IPv4 o IPv6.
Direzione	<p>Selezionare la direzione del traffico a cui applicare la regola.</p> <p>Nota In VMware Cloud Director 10.2.1 e versioni successive, questa opzione non è più disponibile.</p>
Abilita registrazione.	Per registrare la conversione degli indirizzi da parte di questa regola, attivare l'interruttore Abilita registrazione .

7 Fare clic su **Salva**.

8 Per configurare regole aggiuntive, ripetere questi passaggi.

Risultati

Dopo che sono state create, le regole del firewall vengono visualizzate nell'elenco delle regole del firewall del gateway edge. È possibile spostare verso l'alto o verso il basso, modificare o eliminare qualsiasi regola in base alle proprie esigenze.

Aggiunta di una regola SNAT o DNAT a un gateway edge NSX-T

Per modificare l'indirizzo IP di origine da un indirizzo IP privato a uno pubblico, creare una regola NAT (SNAT) di origine. Per modificare l'indirizzo IP di destinazione da un indirizzo IP pubblico a uno privato, creare una regola NAT di destinazione (DNAT).

Quando si configura una regola SNAT o DNAT in un gateway edge nell'ambiente di VMware Cloud Director, la regola viene sempre configurata dal punto di vista del VDC dell'organizzazione.

Una regola SNAT converte l'indirizzo IP di origine dei pacchetti inviati da una rete VDC dell'organizzazione a una rete esterna o a un'altra rete VDC dell'organizzazione.

Una regola NO SNAT impedisce la conversione dell'indirizzo IP interno dei pacchetti inviati da un VDC dell'organizzazione a una rete esterna o a un'altra rete VDC dell'organizzazione.

Una regola DNAT converte l'indirizzo IP e, facoltativamente, la porta dei pacchetti ricevuti da una rete VDC dell'organizzazione provenienti da una rete esterna o da un'altra rete VDC dell'organizzazione.

Una regola NO DNAT impedisce la conversione dell'indirizzo IP esterno dei pacchetti ricevuti da un VDC dell'organizzazione da una rete esterna o da un'altra rete VDC dell'organizzazione.

VMware Cloud Director supporta la ridistribuzione automatica della route quando si utilizzano i servizi NAT in un gateway edge NSX-T Data Center.

Importante Se si utilizzano cluster Tanzu Kubernetes, prendere nota della regola SNAT di sistema creata nel gateway edge per evitare di creare una regola in conflitto.

Prerequisiti

È necessario che gli indirizzi IP pubblici siano stati aggiunti all'interfaccia del gateway edge a cui si desidera aggiungere la regola.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge e, in **Servizi**, fare clic su **NAT**.
- 3 Per aggiungere una regola, fare clic su **Nuovo**.
- 4 Configurare una regola SNAT o NO SNAT (dall'interno verso l'esterno).

Opzione	Descrizione
Nome	Immettere un nome significativo per la regola.
Descrizione	(Facoltativo) Immettere una descrizione per la regola.
Tipo di interfaccia	Dal menu a discesa, selezionare SNAT o NO SNAT.

Opzione	Descrizione
IP esterno	<p>In base al tipo di regola che si sta creando, scegliere una delle opzioni.</p> <ul style="list-style-type: none"> ■ Se si crea una regola SNAT, immettere l'indirizzo IP pubblico del gateway edge per il quale si sta configurando la regola SNAT. ■ Se si crea una regola NO SNAT, lasciare vuota la casella di testo.
IP interno	Immettere l'indirizzo IP o un elenco di indirizzi IP delle macchine virtuali per cui si sta configurando la regola SNAT in modo che possano inviare il traffico alla rete esterna.
IP destinazione	(Facoltativo) Se si desidera che la regola venga applicata solo per il traffico verso un dominio specifico, immettere un indirizzo IP per questo dominio o un elenco di indirizzi IP. Se si lascia vuota questa casella di testo, la regola SNAT viene applicata a tutte le destinazioni esterne alla subnet locale.
Impostazioni avanzate (facoltative)	<p>Fare clic sulla scheda Impostazioni avanzate per visualizzare alcune impostazioni aggiuntive.</p> <p>Stato</p> <p>Per attivare la regola al momento della creazione, attivare l'opzione Stato.</p> <p>Registrazione</p> <p>Per registrare la conversione degli indirizzi da parte di questa regola, attivare l'opzione Registrazione.</p> <p>Priorità</p> <p>Se per un indirizzo sono presenti più regole NAT, è possibile assegnare priorità diverse alle regole per stabilire l'ordine in cui verranno applicate. Un valore più basso indica una priorità più alta per la regola.</p> <p>Corrispondenza firewall</p> <p>È possibile impostare una regola di corrispondenza firewall per stabilire la modalità di applicazione del firewall durante NAT. Dal menu a discesa, selezionare una delle opzioni seguenti.</p> <ul style="list-style-type: none"> ■ Per applicare le regole del firewall all'indirizzo interno di una regola NAT, selezionare Corrispondenza con indirizzo interno. ■ Per applicare le regole del firewall all'indirizzo esterno di una regola NAT, selezionare Corrispondenza con indirizzo esterno. ■ Per ignorare l'applicazione delle regole del firewall, selezionare Ignora.

5 Configurare una regola DNAT o NO DNAT (dall'esterno verso l'interno).

Opzione	Descrizione
Nome	Immettere un nome significativo per la regola.
Descrizione	(Facoltativo) Immettere una descrizione per la regola.
Tipo di interfaccia	Dal menu a discesa, selezionare DNAT o NO DNAT.
IP esterno	<p>Immettere l'indirizzo IP pubblico del gateway edge per il quale si sta configurando la regola DNAT.</p> <p>Gli indirizzi IP immessi devono essere sottoallocati al gateway edge.</p>

Opzione	Descrizione
Porta esterna	(Facoltativo) Specificare una porta in cui la regola DNAT esegue la conversione per i pacchetti in entrata per le macchine virtuali.
IP interno	<p>In base al tipo di regola che si sta creando, scegliere una delle opzioni.</p> <ul style="list-style-type: none"> ■ Se si crea una regola DNAT, immettere l'indirizzo IP o un elenco di indirizzi IP delle macchine virtuali per cui si sta configurando la regola DNAT in modo che possano ricevere il traffico dalla rete esterna. ■ Se si crea una regola NO DNAT, lasciare vuota la casella di testo.
Applicazione	<p>(Facoltativo) Selezionare un profilo di porta dell'applicazione specifico a cui applicare la regola.</p> <p>Il profilo della porta dell'applicazione include una porta e un protocollo che il traffico in entrata utilizza nel gateway edge per connettersi alla rete interna.</p>
Impostazioni avanzate (facoltative)	<p>Fare clic sulla scheda Impostazioni avanzate per visualizzare alcune impostazioni aggiuntive.</p> <p>Stato</p> <p>Per attivare la regola al momento della creazione, attivare l'opzione Stato.</p> <p>Registrazione</p> <p>Per registrare la conversione degli indirizzi da parte di questa regola, attivare l'opzione Registrazione.</p> <p>Priorità</p> <p>Se per un indirizzo sono presenti più regole NAT, è possibile assegnare priorità diverse alle regole per stabilire l'ordine in cui verranno applicate. Un valore più basso indica una priorità più alta per la regola.</p> <p>Corrispondenza firewall</p> <p>È possibile impostare una regola di corrispondenza firewall per stabilire la modalità di applicazione del firewall durante NAT. Dal menu a discesa, selezionare una delle opzioni seguenti.</p> <ul style="list-style-type: none"> ■ Per applicare le regole del firewall all'indirizzo interno di una regola NAT, selezionare Corrispondenza con indirizzo interno. ■ Per applicare le regole del firewall all'indirizzo esterno di una regola NAT, selezionare Corrispondenza con indirizzo esterno. ■ Per ignorare l'applicazione delle regole del firewall, selezionare Ignora.

6 Fare clic su **Salva**.

7 Per configurare regole aggiuntive, ripetere questi passaggi.

Configurazione di un servizio di inoltro DNS su un gateway edge NSX-T

Per inoltrare query DNS a server DNS esterni, configurare un server di inoltro DNS.

Come parte della configurazione del servizio di inoltro DNS, è anche possibile aggiungere zone di inoltro condizionale. Una zona di inoltro condizionale è configurata come un elenco contenente fino a cinque zone DNS FQDN. Se una query DNS corrisponde a un nome dominio di quell'elenco, la query viene inoltrata ai server dalla zona di inoltro corrispondente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge e, in **Gestione IP**, fare clic su **DNS**.
- 3 Nella sezione **Server di inoltro DNS**, fare clic su **Modifica**.
- 4 Per abilitare il servizio del server di inoltro DNS, fare clic sull'interruttore **Stato**.
- 5 Immettere un nome e, facoltativamente, una descrizione per la zona DNS predefinita.
- 6 Immettere uno o più indirizzi IP del server upstream, separati da virgole.
- 7 Fare clic su **Salva**.
- 8 (Facoltativo) Aggiungere una zona di inoltro condizionale.
 - a Nella sezione **Zona del server di inoltro condizionale**, fare clic su **Aggiungi**.
 - b Immettere un nome per la zona di inoltro.
 - c Immettere uno o più indirizzi IP del server upstream, separati da virgole.
 - d Immettere uno o più nomi di dominio, separati da virgole e fare clic su **Salva**.

Creazione di profili delle porte dell'applicazione personalizzata

Per creare regole firewall e NAT, è possibile utilizzare profili delle porte dell'applicazione preconfigurati e profili delle porte dell'applicazione personalizzati.

I profili delle porte dell'applicazione includono una combinazione di un protocollo e una porta o un gruppo di porte, che viene utilizzata per i servizi firewall e NAT nel gateway edge. Oltre ai profili delle porte predefiniti, che sono preconfigurati per NSX-T Data Center, è possibile creare profili delle porte dell'applicazione personalizzati.

Quando si crea un profilo della porta dell'applicazione personalizzato in un gateway edge, questo diventa visibile a tutti gli altri gateway edge NSX-T Data Center che si trovano nello stesso VDC dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 In **Sicurezza**, fare clic su **Profili porte applicazione**.
- 4 Nella sezione **Applicazioni personalizzate**, fare clic su **Nuova**.

- 5 Immettere un nome e, facoltativamente, una descrizione per il profilo della porta dell'applicazione.
- 6 Selezionare un protocollo nel menu a discesa.
- 7 Immettere una porta, o un intervallo di porte separate da virgole, e fare clic su **Salva**.

Operazioni successive

Utilizzare i profili delle porte dell'applicazione per creare regole firewall e NAT. Consultare [Aggiunta di una regola del firewall del gateway edge NSX-T Data Center](#) e [Aggiunta di una regola SNAT o DNAT a un gateway edge NSX-T](#).

VPN basata su criteri IPsec per i gateway edge NSX-T Data Center

A partire dalla versione 10.1, VMware Cloud Director supporta la VPN IPsec basata su criteri da sito a sito tra un'istanza del gateway edge NSX-T Data Center e un sito remoto.

La VPN IPsec offre connettività da sito a sito tra un gateway edge e siti remoti che utilizzano NSX-T Data Center o che dispongono di router hardware o gateway VPN di terze parti che supportano IPsec.

La VPN IPsec basata su criteri richiede l'applicazione di un criterio VPN ai pacchetti per determinare quale traffico deve essere protetto da IPsec prima del passaggio attraverso un tunnel VPN. Questo tipo di VPN è considerato statico perché quando la topologia e la configurazione della rete locale cambiano, è necessario aggiornare anche le impostazioni del criterio VPN in base alle modifiche.

I gateway edge di NSX-T Data Center supportano la configurazione di tunnel suddivisi, con il traffico IPsec che ha la precedenza sul routing.

VMware Cloud Director supporta la ridistribuzione automatica della route quando si utilizza VPN IPsec in un gateway edge NSX-T.

Configurazione della VPN IPsec basata sul criterio NSX-T

È possibile configurare la connettività da sito a sito tra un gateway edge di NSX-T Data Center e siti remoti. I siti remoti devono utilizzare NSX-T Data Center, nonché disporre di router hardware di terze parti o gateway VPN che supportano IPsec.

VMware Cloud Director supporta la ridistribuzione automatica della route quando si configura la VPN IPsec in un gateway edge di NSX-T Data Center.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 In **Servizi**, fare clic su **VPN IPsec**.
- 4 Per configurare un tunnel VPN IPsec, fare clic su **Nuovo**.

- 5 Immettere un nome e facoltativamente una descrizione per il tunnel VPN IPSec.
- 6 Per abilitare il tunnel al momento della creazione, attivare l'opzione **Abilitato**.
- 7 Scegliere una chiave precondivisa da immettere.

Nota La chiave precondivisa deve essere identica nell'altra estremità del tunnel VPN IPSec.

- 8 Immettere uno degli indirizzi IP disponibili per il gateway edge per l'endpoint locale.

Nota L'indirizzo IP deve essere l'IP primario del gateway edge o un indirizzo IP allocato separatamente al gateway edge dalla rete esterna.

- 9 Immettere almeno un indirizzo di subnet IP locale nella notazione CIDR da utilizzare per il tunnel VPN IPSec.
- 10 Immettere l'indirizzo IP per il sito remoto.
- 11 Immettere almeno un indirizzo di subnet IP remoto nella notazione CIDR da utilizzare per il tunnel VPN IPSec.
- 12 (Facoltativo) Per abilitare la registrazione, attivare l'opzione **Registrazione**.
- 13 Fare clic su **Salva**.
- 14 Per verificare che il tunnel funzioni, selezionarlo e fare clic su **Visualizza statistiche**.

Se il tunnel funziona, in **Stato tunnel** e in **Stato del servizio IKE** viene visualizzato **Raggiungibile**.

Risultati

Il tunnel VPN IPSec appena creato è elencato nella vista **VPN IPSec**. Il tunnel VPN IPSec viene creato con un profilo di sicurezza predefinito.

Operazioni successive

È possibile modificare le impostazioni del tunnel VPN IPSec e personalizzare il profilo di sicurezza in base alle esigenze.

Personalizzazione del profilo di sicurezza di un tunnel VPN IPSec

Se si decide di non utilizzare il profilo di sicurezza generato dal sistema assegnato al tunnel VPN IPSec al momento della creazione, è possibile personalizzarlo.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 In **Servizi**, fare clic su **VPN IPSec**.
- 4 Selezionare il tunnel VPN IPSec e fare clic su **Personalizzazione profilo di sicurezza**.

5 Configurare i profili IKE.

I profili Internet Key Exchange (IKE) forniscono informazioni sugli algoritmi utilizzati per autenticare, crittografare e stabilire un segreto condiviso tra i siti di rete quando si stabilisce un tunnel IKE.

- a Selezionare una versione del protocollo IKE per configurare un'associazione di sicurezza (SA) nella suite di protocolli IPSec.

Opzione	Descrizione
IKEv1	Quando si seleziona questa opzione, la VPN IPSec viene avviata e risponde solo al protocollo IKEv1.
IKEv2	L'opzione predefinita. Quando si seleziona questa versione, la VPN IPSec viene avviata e risponde solo al protocollo IKEv2.
IKE-Flex	Quando si seleziona questa opzione, se la creazione del tunnel non riesce con il protocollo IKEv2, il sito di origine non esegue il fallback e avvia una connessione con il protocollo IKEv1. Se invece il sito remoto avvia una connessione con il protocollo IKEv1, la connessione viene accettata.

- b Selezionare un algoritmo di crittografia supportato da utilizzare durante la negoziazione IKE (Internet Key Exchange).
- c Dal menu a discesa **Digest**, selezionare un algoritmo di hash sicuro da utilizzare durante la negoziazione IKE.
- d Dal menu a discesa **Gruppo Diffie-Hellman**, selezionare uno degli schemi di crittografia che consente al sito peer e al gateway edge di stabilire un segreto condiviso su un canale di comunicazione non sicuro.
- e (Facoltativo) Nella casella di testo **Durata associazione**, modificare il numero predefinito di secondi prima che sia necessario ristabilire il tunnel IPSec.

6 Configurare il tunnel VPN IPSec.

- a Per abilitare Perfect Forward Secrecy, attivare l'opzione.
- b Selezionare un criterio di deframmentazione.

Il criterio di deframmentazione consente di gestire i bit di deframmentazione presenti nel pacchetto interno.

Opzione	Descrizione
Copia	Copia il bit di deframmentazione dal pacchetto IP interno al pacchetto esterno.
Cancella	Ignora il bit di deframmentazione presente nel pacchetto interno.

- c Selezionare un algoritmo di crittografia supportato da utilizzare durante la negoziazione IKE (Internet Key Exchange).
- d Dal menu a discesa **Digest**, selezionare un algoritmo di hash sicuro da utilizzare durante la negoziazione IKE.

- e Dal menu a discesa **Gruppo Diffie-Hellman**, selezionare uno degli schemi di crittografia che consente al sito peer e al gateway edge di stabilire un segreto condiviso su un canale di comunicazione non sicuro.
 - f (Facoltativo) Nella casella di testo **Durata associazione**, modificare il numero predefinito di secondi prima che sia necessario ristabilire il tunnel IPsec.
- 7 (Facoltativo) Nella casella di testo **Intervallo probe**, modificare il numero predefinito di secondi per il rilevamento dei peer dead.
- 8 Fare clic su **Salva**.

Risultati

Nella vista VPN IPsec, il profilo di sicurezza del tunnel VPN IPsec viene visualizzato come **Definito dall'utente**.

Configurazione dei servizi della rete esterna dedicata

Per fornire una topologia di rete completamente instradata in un virtual data center, un **amministratore di sistema** può dedicare una rete esterna a un gateway edge NSX-T Data Center specifico.

Quando si utilizza una rete esterna dedicata, è possibile configurare servizi di routing aggiuntivi, come la gestione della comunicazione della route e la configurazione di BGP (Border Gateway Protocol).

Procedura

1 Gestione della comunicazione della route

Con la comunicazione della route, è possibile creare un ambiente di rete completamente instradata in un virtual data center (VDC) dell'organizzazione.

2 Configurazione delle impostazioni generali BGP

È possibile configurare una connessione Border Gateway Protocol (eBGP o iBGP) interna o esterna tra un gateway edge NSX-T Data Center che disponga di una rete esterna dedicata e un router nella propria infrastruttura fisica.

3 Creazione di un elenco di prefissi IP

È possibile creare elenchi di prefissi IP che contengono indirizzi IP singoli o multipli. È possibile utilizzare gli elenchi di prefissi IP per assegnare i router adiacenti BGP con autorizzazioni di accesso per la comunicazione della route.

4 Aggiunta di un router adiacente BGP

È possibile configurare impostazioni individuali per i router adiacenti BGP quando li si aggiunge.

Gestione della comunicazione della route

Con la comunicazione della route, è possibile creare un ambiente di rete completamente instradata in un virtual data center (VDC) dell'organizzazione.

È possibile decidere quali delle subnet di rete collegate al gateway edge NSX-T Data Center comunicare alla rete esterna dedicata.

Se una subnet non viene aggiunta al filtro della comunicazione, la relativa route non viene comunicata alla rete esterna e la subnet rimane privata.

Nota VMware Cloud Director comunica qualsiasi rete VDC dell'organizzazione che si trova nella route comunicata. Per questo motivo, non è necessario creare un filtro per ogni subnet che fa parte di una rete comunicata.

La comunicazione della route viene configurata automaticamente nel gateway edge NSX-T Data Center.

VMware Cloud Director supporta la ridistribuzione automatica della route quando si utilizza la comunicazione della route in un gateway edge NSX-T. La ridistribuzione della route viene configurata automaticamente nel router logico di livello 0 che rappresenta la rete esterna dedicata.

Prerequisiti

- Verificare che l'**amministratore di sistema** abbia dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione.
- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo che includa un insieme di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 In **Routing**, fare clic su **Comunicazione route** e su **Modifica**.
- 4 Per aggiungere una subnet da comunicare, fare clic su **Aggiungi**.
- 5 Aggiungere una subnet IPv4 o IPv6.

Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.

Configurazione delle impostazioni generali BGP

È possibile configurare una connessione Border Gateway Protocol (eBGP o iBGP) interna o esterna tra un gateway edge NSX-T Data Center che disponga di una rete esterna dedicata e un router nella propria infrastruttura fisica.

BGP effettua decisioni di routing di base utilizzando una tabella di reti IP o prefissi, che designano più route tra sistemi autonomi (AS).

Il termine speaker BGP si riferisce a un dispositivo di rete che esegue BGP. Due speaker BGP stabiliscono una connessione prima che qualsiasi informazione di routing venga scambiata.

Il termine router adiacente BGP si riferisce a uno speaker BGP che ha stabilito una connessione di questo tipo. Una volta stabilita la connessione, i dispositivi scambiano la route e sincronizzano le rispettive tabelle. Ogni dispositivo invia messaggi keep-alive per mantenere attiva questa relazione.

Nota In un gateway edge connesso a una rete esterna supportata da un gateway VRF, le impostazioni del numero AS locale e del riavvio normale sono di sola lettura. L'**amministratore di sistema** può modificare queste impostazioni nel gateway di livello 0 principale in NSX-T Data Center.

Prerequisiti

- Verificare che l'**amministratore di sistema** abbia dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione.
- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo che includa un insieme di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 In **Routing** fare clic su **BGP** e in **Configurazione** fare clic su **Modifica**.
- 4 Attivare l'opzione **Stato** per attivare BGP.
- 5 Immettere un numero ID del sistema autonomo (AS) da utilizzare per la funzionalità AS locale del protocollo.

VMware Cloud Director assegna il numero AS locale al gateway edge. Il gateway edge annuncia questo ID quando si connette con i router adiacenti BGP in altri sistemi autonomi.

6 Dal menu a discesa, selezionare un'opzione di **Modalità di riavvio normale**.

Opzione	Descrizione
Helper e riavvio normale	<p>Non è consigliabile attivare la funzionalità di riavvio normale nel gateway edge perché i peering BGP di tutti i gateway sono sempre attivi.</p> <p>In caso di failover, la funzionalità di riavvio normale aumenta il tempo impiegato da un router adiacente remoto per selezionare un gateway alternativo di livello 0. Ciò fa ritardare la convergenza basata su BFD.</p> <p>Nota La configurazione del gateway edge si applica a tutti i router adiacenti BGP a meno che la configurazione specifica del router adiacente non la sostituisca.</p>
Solo Helper	Utile per ridurre o eliminare l'interruzione delle attività del traffico associato alle route apprese da un router adiacente in grado di eseguire un riavvio normale. Il router adiacente deve essere in grado di conservare la tabella di inoltro mentre esegue un riavvio.
Disabilita	Disattiva la modalità di riavvio normale nel gateway edge.

7 (Facoltativo) Modificare il valore predefinito per il timer di riavvio normale.

8 (Facoltativo) Modificare il valore predefinito per il timer della route obsoleta.

9 Attivare l'opzione **ECMP** per attivare ECMP.

10 Fare clic su **Salva**.

Operazioni successive

- [Creazione di un elenco di prefissi IP](#)
- [Aggiunta di un router adiacente BGP](#)

Creazione di un elenco di prefissi IP

È possibile creare elenchi di prefissi IP che contengono indirizzi IP singoli o multipli. È possibile utilizzare gli elenchi di prefissi IP per assegnare i router adiacenti BGP con autorizzazioni di accesso per la comunicazione della route.

Gli elenchi di prefissi IP vengono indicati tramite filtri di router adiacenti BGP per limitare il numero di aggiornamenti BGP scambiati tra i peer BGP. Utilizzando il filtro della route, è possibile ridurre la quantità di risorse di sistema necessarie per gli aggiornamenti BGP.

Ad esempio, è possibile aggiungere l'indirizzo IP 192.168.100.3/27 all'elenco dei prefissi IP e negare la redistribuzione della route al gateway edge.

È inoltre possibile aggiungere un indirizzo IP con i modificatori `less than or equal to (le)` e `greater than or equal to (ge)` per consentire o limitare la redistribuzione della route. Ad esempio, i modificatori 192.168.100.3/27 ge 26 le 32 corrispondono alle subnet mask maggiori o uguali a 26 bit e minori o uguali a 32 bit di lunghezza.

Prerequisiti

- Verificare che l'**amministratore di sistema** abbia dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione.
- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- [Configurazione delle impostazioni generali BGP.](#)

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 In **Routing**, fare clic su **BGP** e su **Elenchi di prefissi IP**.
- 4 Per aggiungere un elenco di prefissi IP, fare clic su **Nuovo**.
- 5 Immettere un nome e facoltativamente una descrizione per l'elenco di prefissi.
- 6 Fare clic su **Nuovo** e aggiungere una notazione CIDR per il prefisso.
- 7 Dal menu a discesa, selezionare un'azione da applicare al prefisso.
- 8 (Facoltativo) Immettere i modificatori `greater than or equal to` e `less than or equal to` per consentire o limitare la ridistribuzione delle route.

Operazioni successive

- È possibile modificare o eliminare l'elenco di prefissi IP in base alle esigenze.
- Configurare il filtraggio di routing. Vedere [Aggiunta di un router adiacente BGP](#).

Aggiunta di un router adiacente BGP

È possibile configurare impostazioni individuali per i router adiacenti BGP quando li si aggiunge.

Prerequisiti

- Verificare che l'**amministratore di sistema** abbia dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione.
- Verificare di essere un **amministratore dell'organizzazione** o di disporre di un ruolo che includa un insieme di diritti equivalente.
- Verificare di aver configurato le impostazioni BGP globali per il gateway edge. Vedere [Configurazione delle impostazioni generali BGP](#).
- Se si utilizza il filtro di routing, verificare di aver creato elenchi di prefissi IP. Vedere [Creazione di un elenco di prefissi IP](#).

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge.
- 3 In **Routing**, fare clic su **BGP** e su **Router adiacenti**.
- 4 Per aggiungere un nuovo router adiacente BGP, fare clic su **Nuovo**.
- 5 Immettere le impostazioni generali per il nuovo router adiacente BGP.
 - a Immettere un indirizzo IPv4 o IPv6 per il nuovo router adiacente BGP.
 - b Immettere un numero di sistema autonomo (AS) remoto nel formato ASPLAIN.
 - c Immettere l'intervallo di tempo che deve trascorrere tra l'invio di un messaggio keep-alive e un altro a un peer BGP.
 - d Immettere l'intervallo di tempo che deve trascorrere prima che un peer BGP venga dichiarato dead.
 - e Dal menu a discesa, selezionare un'opzione di **Modalità di riavvio normale** per questo router adiacente.

Opzione	Descrizione
Disabilita	Ignora le impostazioni globali del gateway edge e disattiva la modalità di riavvio normale per questo router adiacente.
Solo Helper	Ignora le impostazioni globali del gateway edge e configura la modalità di riavvio normale come Solo Helper per questo router adiacente.
Riavvio normale e Helper	Ignora le impostazioni globali del gateway edge e configura la modalità di riavvio normale come Riavvio normale e Helper per questo router adiacente.

- f Attivare l'interruttore **AllowAS-in** per abilitare le route di ricezione con lo stesso AS.
 - g Se il router adiacente BGP richiede l'autenticazione, immettere la password del router adiacente BGP.
- 6 Configurare le impostazioni di Bidirectional Forwarding Detection (BFD) per il nuovo router adiacente BGP.
 - a (Facoltativo) Attivare l'opzione **BFD** per abilitare BFD per il rilevamento degli errori.
 - b Nella casella di testo dell'intervallo BFD, definire l'intervallo di tempo tra l'invio dei pacchetti heartbeat.
 - c Nella casella di testo **Multiplo dead**, immettere il numero di volte per cui il router adiacente BGP può fallire l'invio dei pacchetti heartbeat prima che BFD lo dichiari non raggiungibile.

7 (Facoltativo) Configurare il filtraggio di routing.

- a Dal menu a discesa **Famiglia di indirizzi IP**, selezionare una famiglia di indirizzi IP.
- b Per configurare un filtro in entrata, selezionare un elenco di prefissi IP.
- c Per configurare un filtro in uscita, selezionare un elenco di prefissi IP.

8 Fare clic su **Salva**.**Operazioni successive**

È possibile visualizzare lo stato di ciascun router adiacente BGP, modificare o eliminare i router adiacenti BGP in base alle esigenze.

Utilizzo del bilanciamento del carico avanzato NSX

Configurando servizi virtuali che distribuiscono il traffico tra più pool di server, un **amministratore dell'organizzazione** può bilanciare i carichi di lavoro nei data center supportati da NSX-T Data Center.

A partire dalla versione 10.2, VMware Cloud Director fornisce servizi di bilanciamento del carico utilizzando le funzionalità di VMware NSX Advanced Load Balancer (Avi Networks).

VMware Cloud Director supporta il bilanciamento del carico L4 e L7 che è possibile configurare in un gateway edge NSX-T Data Center.

Il bilanciamento del carico di livello 4 (L4) indirizza il traffico in base ai dati dei protocolli dei livelli di rete e di trasporto, ad esempio l'indirizzo IP e la porta TCP.

Il bilanciamento del carico di livello 7 (L7) distribuisce il traffico in base ad attributi come intestazione HTTP, URI (Uniform Resource Identifier), ID sessione SSL e dati del modulo HTML.

Abilitazione del bilanciamento del carico in un gateway edge NSX-T Data Center

Prima che un **amministratore dell'organizzazione** possa configurare i servizi di bilanciamento del carico, un **amministratore di sistema** deve abilitare il bilanciamento del carico nel gateway edge di NSX-T Data Center.

Prerequisiti

- Assicurarsi di essere un **amministratore di sistema**.
- Verificare di aver integrato VMware NSX Advanced Load Balancer nell'infrastruttura cloud. Per ulteriori informazioni sulla gestione di NSX Advanced Load Balancer, vedere *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge NSX-T Data Center in cui si desidera abilitare il bilanciamento del carico.

- 3 In Bilanciamento del carico, fare clic su **Impostazioni generali**.
- 4 Fare clic su **Modifica** e attivare l'opzione **Stato bilanciamento del carico**.
- 5 Immettere un CIDR di rete per una subnet di rete di servizio da cui utilizzare gli indirizzi IP per la creazione di servizi virtuali.

È possibile utilizzare la subnet della rete di servizio predefinita selezionando la casella di controllo **Usa predefinito**.
- 6 Fare clic su **Salva**.

Operazioni successive

[Assegnazione di un gruppo di motori di servizio a un gateway edge NSX-T Data Center.](#)

Assegnazione di un gruppo di motori di servizio a un gateway edge NSX-T Data Center

Prima che un **amministratore dell'organizzazione** possa configurare i servizi di bilanciamento del carico in un gateway edge NSX-T Data Center, un **amministratore di sistema** deve assegnare un gruppo di motori di servizio al gateway edge.

L'infrastruttura di calcolo del bilanciamento del carico fornita da NSX Advanced Load Balancer è organizzata in gruppi di motori di servizio. Un **amministratore di sistema** può assegnare uno o più gruppi di motori di servizio a un gateway edge NSX-T Data Center.

Tutti i gruppi di motori di servizio assegnati a un singolo gateway edge utilizzano la stessa rete di servizio.

Prerequisiti

- Assicurarsi di essere un **amministratore di sistema**.
- [Abilitazione del bilanciamento del carico in un gateway edge NSX-T Data Center.](#)

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge NSX-T Data Center a cui si desidera assegnare un gruppo di motori di servizio.
- 3 In Bilanciamento del carico, fare clic su **Gruppi di motori di servizio**.
- 4 Fare clic su **Aggiungi**.
- 5 Selezionare un gruppo di motori di servizio disponibile dall'elenco.
- 6 Immettere un numero per indicare il limite massimo di servizi virtuali che possono essere posizionati nel gateway edge.
- 7 Immettere un numero per i servizi virtuali garantiti disponibili per il gateway edge.
- 8 Per confermare le impostazioni, fare clic su **Salva**.

Modifica delle impostazioni di un gruppo di motori di servizio

Un **amministratore di sistema** può modificare il numero massimo di servizi virtuali supportati e il numero di servizi virtuali riservati per un gruppo di motori di servizio.

Dopo aver sincronizzato un gruppo di motori di servizio, se il nuovo numero massimo di servizi virtuali supportati è inferiore al numero di servizi virtuali riservati, il gruppo di motori di servizio viene contrassegnato come sovra-allocato.

Se un gruppo di motori di servizio è sovra-allocato, la creazione di un nuovo servizio virtuale può avere esito negativo, anche se la capacità riservata nel gateway edge in cui si crea il servizio virtuale è sufficiente.

Per evitare l'esito negativo della creazione del servizio virtuale, quando si modificano le impostazioni di un gruppo di motori di servizio, non impostare il numero massimo di servizi virtuali supportati al di sotto del numero di servizi virtuali inizialmente riservati.

Prerequisiti

- Assicurarsi di essere un **amministratore di sistema**.
- [Abilitazione del bilanciamento del carico in un gateway edge NSX-T Data Center](#).
- [Assegnazione di un gruppo di motori di servizio a un gateway edge NSX-T Data Center](#).

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge NSX-T Data Center a cui è assegnato il gruppo di motori di servizio.
- 3 In Bilanciamento del carico, fare clic su **Gruppi di motori di servizio**.
- 4 Fare clic su **Modifica**.
- 5 Modificare il numero massimo di servizi virtuali consentiti che il gateway edge può utilizzare.
Non ridurre il numero a meno che non sia obbligatorio. In caso contrario, è possibile che si verifichino errori durante la creazione di servizi virtuali.
- 6 Modificare il numero dei servizi virtuali garantiti disponibili per il gateway edge.
- 7 Fare clic su **Salva**.

Aggiunta di un pool di server di bilanciamento del carico

Un pool di server è un gruppo di uno o più server configurati per eseguire la stessa applicazione e per fornire disponibilità elevata.

Prerequisiti

- Assicurarsi di essere un **amministratore dell'organizzazione**.
- Verificare che l'**amministratore di sistema** abbia abilitato il bilanciamento del carico nel gateway edge NSX-T.

- Verificare che l'**amministratore di sistema** abbia assegnato almeno un gruppo di motori di servizio al gateway edge.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge NSX-T Data Center per cui si desidera configurare un pool di bilanciamento del carico.
- 3 In Bilanciamento del carico, fare clic su **Pool** e quindi fare clic su **Aggiungi**.
- 4 Configurare le impostazioni generali per il pool di bilanciamento del carico.
 - a Immettere un nome significativo e, facoltativamente, una descrizione per il pool di server.
 - b Selezionare un metodo di bilanciamento dell'algoritmo.

L'algoritmo di bilanciamento del carico definisce il modo in cui le connessioni in entrata vengono distribuite tra i membri del pool di server.

Opzione	Descrizione
Connessioni minime	Le nuove connessioni vengono inviate al server che al momento dispone del minor numero di connessioni.
Round Robin	Le nuove connessioni vengono inviate al server idoneo successivo nel pool in ordine sequenziale.
Risposta più rapida	Le nuove connessioni vengono inviate al server che fornisce la risposta più rapida alle nuove connessioni o richieste.
Hash uniforme	Le nuove connessioni vengono distribuite tra i server utilizzando l'indirizzo IP del client per generare una chiave hash IP.
Carico minimo	Le nuove connessioni vengono inviate al server con il carico più leggero, indipendentemente dal numero di connessioni del server.
Minor numero di server	Anziché tentare di distribuire tutte le connessioni o richieste in tutti i server, il bilanciamento del carico determina il numero minimo di server necessari per soddisfare il carico del client corrente.
Casuale	Il bilanciamento del carico seleziona i server in modo casuale.
Minor numero di attività	Il carico viene bilanciato in modo adattivo, in base al feedback del server.
Affinità core	Ogni core della CPU utilizza un sottoinsieme di server e ciascun server viene utilizzato da un sottoinsieme di core. Essenzialmente, fornisce una mappatura multi-a-molti tra server e core.

- c Per abilitare il pool di server al momento della creazione, attivare l'opzione **Stato**.
- d Immettere una porta del server di destinazione predefinita da utilizzare per il traffico verso il membro del pool.

- e (Facoltativo) Nella casella di testo **Timeout di disabilitazione normale**, immettere il tempo massimo in minuti per disattivare un membro del pool in modo normale.

Il servizio virtuale attende il tempo specificato prima di chiudere le connessioni esistenti ai membri disattivati.

- f (Facoltativo) Per attivare un monitoraggio di integrità passivo, attivare l'opzione **Monitoraggio integrità passivo**.
- g (Facoltativo) Selezionare un monitoraggio integrità attivo.

Opzione	Descrizione
HTTP	Per convalidare l'integrità, vengono utilizzate una richiesta e una risposta HTTP.
HTTPS	Utilizzato nei server Web crittografati HTTPS per convalidare l'integrità.
TCP	Per convalidare l'integrità, viene utilizzata una connessione TCP.
UDP	Per convalidare l'integrità, viene utilizzato un datagramma UDP.
PING	Per convalidare l'integrità viene utilizzato un ping ICMP.

5 Aggiungere un membro al pool di server.

- a Fare clic sulla scheda **Membri**, quindi su **Aggiungi**.
- b Immettere un indirizzo IP per il membro del pool.
- c Attivare l'opzione **Stato** per abilitare il membro del pool.
- d (Facoltativo) Aggiungere una porta personalizzata per il membro del pool di server.

Il numero di porta predefinito è quello della porta di destinazione immessa per il pool.

- e Immettere un rapporto per il membro del pool.

Il rapporto di ciascun membro del pool denota il traffico che passa a ciascun membro del pool di server. Un server con un rapporto 2 ottiene il doppio della quantità di traffico di un server con un rapporto 1. Il valore predefinito è 1.

6 Nella scheda **Impostazioni SSL**, configurare le impostazioni SSL per la convalida dei certificati presentati dai membri del pool di bilanciamento del carico.

- a Per attivare SSL, attivare l'opzione **Abilitazione SSL**.
- b Per nascondere i certificati con chiavi private e visualizzare solo un elenco di certificati CA, selezionare la casella di controllo **Nascondi certificati di servizio**.

7 Per attivare il controllo del nome comune per i certificati del server, selezionare l'opzione **Controllo del nome comune** e immettere fino a 10 nomi di dominio per il pool.

8 Fare clic su **Salva**.

Operazioni successive

[Creazione di un servizio virtuale.](#)

Creazione di un servizio virtuale

Un servizio virtuale è in ascolto del traffico verso un indirizzo IP, elabora le richieste del client e indirizza le richieste valide a un membro del pool di server del bilanciamento del carico.

Un servizio virtuale è una combinazione di un indirizzo IP e una porta che utilizza un singolo protocollo di rete. Il servizio virtuale viene comunicato alle reti esterne ed è in ascolto delle richieste del client. Quando un client si connette al servizio virtuale, il bilanciamento del carico indirizza la richiesta a un membro del pool di server del bilanciamento del carico configurato.

Per garantire la terminazione SSL per un servizio virtuale è possibile utilizzare un certificato della libreria di certificati. Per ulteriori informazioni, vedere [Importazione dei certificati nella libreria di certificati](#).

Prerequisiti

- Assicurarsi di essere un **amministratore dell'organizzazione**.
- Verificare che l'**amministratore di sistema** abbia abilitato il bilanciamento del carico nel gateway edge NSX-T.
- Verificare che l'**amministratore di sistema** abbia assegnato almeno un gruppo di motori di servizio al gateway edge.
- [Aggiunta di un pool di server di bilanciamento del carico](#).

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Rete**, quindi fare clic sulla scheda **Gateway edge**.
- 2 Fare clic sul gateway edge NSX-T Data Center in cui si desidera creare un servizio virtuale.
- 3 In Bilanciamento del carico, fare clic su **Servizi virtuali**, quindi fare clic su **Aggiungi**.
- 4 Immettere un nome significativo e, facoltativamente, una descrizione per il servizio virtuale.
- 5 Per attivare il servizio virtuale al momento della creazione, attivare l'opzione **Abilitato**.
- 6 Selezionare un gruppo di motori di servizio per il servizio virtuale.
- 7 Selezionare un pool di bilanciamento del carico per il servizio virtuale.
- 8 Immettere un indirizzo IP per il servizio virtuale.

9 Selezionare il tipo di servizio virtuale.

Opzione	Descrizione
HTTP	<p>Il servizio virtuale è in ascolto delle richieste HTTP di livello 7 non sicure.</p> <p>Quando si seleziona questo tipo di servizio, la casella di testo della porta di servizio viene automaticamente compilata con il valore 80, che può essere sostituito con un altro numero di porta valido.</p>
HTTPS	<p>Il servizio virtuale è in ascolto delle richieste HTTPS di livello 7 sicure.</p> <p>Quando si seleziona questo tipo di servizio, la casella di testo della porta di servizio viene automaticamente compilata con il valore 443, che può essere sostituito con un altro numero di porta valido. Selezionare un certificato SSL da utilizzare per la terminazione SSL.</p>
L4	<p>Il servizio virtuale è in ascolto delle richieste di livello 4.</p> <p>Quando si seleziona questo tipo di servizio, la casella di testo della porta di servizio viene automaticamente compilata con il valore 80, che può essere sostituito con un altro numero di porta valido.</p>
L4 TLS	<p>Il servizio virtuale è in ascolto delle richieste TLS di livello 4 sicure.</p> <p>Quando si seleziona questo tipo di servizio, la casella di testo della porta di servizio viene automaticamente compilata con il valore 443 della porta TCP, che può essere sostituito con un altro numero di porta valido. Selezionare un certificato SSL da utilizzare per la terminazione SSL.</p>

10 Fare clic su **Salva**.

Uso dei dischi denominati e controllo dei criteri di storage

6

È possibile creare e gestire i dischi denominati e rivedere i criteri di storage dei virtual data center dell'organizzazione utilizzando il portale tenant di VMware Cloud Director.

Questo capitolo include i seguenti argomenti:

- [Creazione e utilizzo di dischi denominati](#)
- [Controllo delle proprietà dei criteri di storage](#)

Creazione e utilizzo di dischi denominati

I dischi denominati sono dischi virtuali standalone creati nei VDC dell'organizzazione. Gli **amministratori dell'organizzazione** e gli utenti con i rispettivi diritti possono creare, rimuovere e aggiornare i dischi denominati e connetterli alle macchine virtuali.

Quando si crea un disco denominato, viene associato a un VDC dell'organizzazione, ma non a una macchina virtuale. Dopo aver creato il disco in un VDC, il proprietario del disco o un amministratore può collegarlo a qualsiasi macchina virtuale distribuita nel VDC. Se si dispone del diritto **Crea disco condiviso**, è possibile creare un disco denominato condiviso che è possibile collegare a più macchine virtuali. Il proprietario del disco può anche modificare le proprietà del disco, scollegarlo da una macchina virtuale e rimuoverlo dal VDC. Gli **amministratori di sistema** e gli **amministratori organizzazione** dispongono degli stessi diritti di utilizzo e modifica del disco di cui dispone il proprietario del disco stesso.

Nota Sebbene vSphere supporti configurazioni quali Windows Server Failover Cluster (WSFC) e consenta di creare un disco condiviso tramite la condivisione fisica del bus SCSI, VMware Cloud Director 10.2 non supporta questa funzionalità. Quando si crea un disco condiviso in VMware Cloud Director, si crea solo un disco persistente indipendente sottostante in vSphere con la modalità multiwriter abilitata.

Se si collega un disco denominato, non è possibile creare snapshot della macchina virtuale. Se un disco condiviso è collegato a una macchina virtuale, non è possibile modificare l'impostazione del disco rigido dalla vista dei dettagli della macchina virtuale.

Se il VDC dell'organizzazione ha un criterio di storage con crittografia della macchina virtuale abilitata, è possibile crittografare macchine virtuali e dischi associandoli a criteri di storage che dispongono della funzionalità di crittografia della macchina virtuale. Vedere [Crittografia della macchina virtuale](#).

Creazione di un disco denominato

È possibile creare un disco denominato e collegarlo a una o più macchine virtuali in un secondo momento.

Per creare un disco denominato, è necessario specificarne il nome e le dimensioni.

Facoltativamente, è possibile includere una descrizione e selezionare un profilo di storage che verrà utilizzato dal disco. È possibile creare un disco condiviso che può essere collegato a più macchine virtuali.

Nota Sebbene vSphere supporti configurazioni quali Windows Server Failover Cluster (WSFC) e consenta di creare un disco condiviso tramite la condivisione fisica del bus SCSI, VMware Cloud Director 10.2 non supporta questa funzionalità. Quando si crea un disco condiviso in VMware Cloud Director, si crea solo un disco persistente indipendente sottostante in vSphere con la modalità multiwriter abilitata.

Prerequisiti

- 1 È necessario disporre di diritti di proprietario ruolo o il disco di un **amministratore organizzazione**.
- 2 Se si desidera creare un disco condiviso, è necessario disporre del diritto **Crea disco condiviso**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Dischi denominati** in **Storage** nel pannello sinistro.
- 2 Fare clic su **Nuovo**.
- 3 Immettere un nome e, facoltativamente, una descrizione del disco.
- 4 Selezionare il criterio di storage dal menu a discesa **Criterio di storage**.
- 5 Inserire le dimensioni del disco denominato.
- 6 Selezionare il tipo e il sottotipo di bus dai menu a discesa **Tipo di bus** e **Sottotipo di bus** rispettivamente.
- 7 Se si desidera collegare il disco denominato a più macchine virtuali, selezionare la casella di controllo **Condivisibile**.

Non è possibile modificare questa impostazione in un secondo momento.

- 8 Fare clic su **Salva**.

Operazioni successive

Utilizzare l'API di VMware Cloud Director per collegare il disco indipendente a una macchina virtuale. Vedere *Guida alla programmazione dell'API di VMware Cloud Director* su [VMware {code}](#).

Modifica di un disco denominato

Dopo aver creato il disco, è possibile modificarne il nome, la descrizione, il criterio di storage e le dimensioni.

Non è possibile modificare l'impostazione **Condivisibile** di un disco denominato.

Prerequisiti

- 1 È necessario disporre di diritti di proprietario ruolo o il disco di un **amministratore organizzazione**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Dischi denominati** in **Storage** nel pannello sinistro.
- 2 Selezionare il disco che si desidera modificare e fare clic su **Modifica**.
- 3 Modificare le impostazioni quali il nome, la descrizione, il criterio di storage e le dimensioni.
- 4 Fare clic su **Salva**.

Collegamento di un disco denominato a una macchina virtuale

Dopo aver creato un disco denominato in un VDC, è possibile collegarlo a qualsiasi macchina virtuale distribuita nel VDC. È possibile collegare un disco denominato condiviso a più macchine virtuali.

Prerequisiti

È necessario disporre di diritti di proprietario ruolo o il disco di un **amministratore organizzazione**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Dischi denominati** in **Storage** nel pannello sinistro.
- 2 Fare clic sul pulsante di opzione accanto al nome del disco denominato che si desidera collegare alla macchina virtuale e fare clic su **Collega**.
- 3 Nel menu a discesa, selezionare una macchina virtuale a cui collegare il disco denominato e fare clic su **Applica**.
- 4 Se si desidera collegare un'altra macchina virtuale a un disco condiviso, ripetere [Passaggio 2](#) e [Passaggio 3](#).

Operazioni successive

È possibile collegare più dischi denominati alla macchina virtuale oppure scollegarli in base alle esigenze.

Eliminazione di un disco denominato

Se un disco denominato non è necessario, è possibile eliminarlo.

Prerequisiti

È necessario disporre di diritti di proprietario ruolo o il disco di un **amministratore organizzazione**.

Procedura

- 1 Nella schermata del dashboard **Virtual data center** fare clic sulla scheda del virtual data center che si desidera esplorare e selezionare **Dischi denominati** in **Storage** nel pannello sinistro.
- 2 Selezionare il disco che si desidera eliminare e fare clic su **Elimina**.
- 3 Fare clic su **OK**.

Controllo delle proprietà dei criteri di storage

È possibile esaminare i criteri di storage e i dettagli dei criteri di storage.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center**, fare clic sulla scheda del virtual data center che si desidera esplorare.
- 2 Sotto **Storage**, fare clic su **Criteri di Storage**.
Viene visualizzato l'elenco dei criteri di storage disponibili.
- 3 Per visualizzare i dettagli relativi a un criterio di storage, fare clic sul nome del criterio di storage.
- 4 Controllare i dettagli nelle schede **Generale** e **Metadati** e fare clic su **OK**.
È possibile rivedere il nome, i limiti, le impostazioni IOPS e i dettagli dei metadati del criterio di storage.

Controllo e modifica delle proprietà del virtual data center

7

In qualità di **amministratore dell'organizzazione**, è possibile esaminare le proprietà del virtual data center. È inoltre possibile controllare l'accesso ai VDC dell'organizzazione da parte di utenti e gruppi dell'organizzazione.

Questo capitolo include i seguenti argomenti:

- [Controllo delle proprietà del virtual data center](#)
- [Controllo dei metadati del virtual data center](#)
- [Limitazione dell'accesso a un VDC dell'organizzazione per utenti e gruppi specifici dell'organizzazione](#)

Controllo delle proprietà del virtual data center

È possibile esaminare le proprietà dei virtual data center assegnati all'organizzazione.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center**, fare clic sulla scheda del virtual data center che si desidera esplorare.
- 2 In **Impostazioni** fare clic su **Generale**.

Risultati

È possibile controllare le proprietà del virtual data center, ad esempio nome, descrizione e stato. Le informazioni sulle metriche del data center includono modello di allocazione e vCPU, oltre a CPU e utilizzo della memoria.

Controllo dei metadati del virtual data center

VMware Cloud Director è dotato di una funzionalità di uso generico che consente di associare metadati definiti dall'utente a un oggetto. Se l'amministratore di sistema ha creato metadati

per il virtual data center dell'organizzazione, è possibile esaminare i metadati del data center dell'organizzazione.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella schermata del dashboard **Virtual data center**, fare clic sulla scheda del virtual data center che si desidera esplorare.
- 2 In **impostazioni**, fare clic su **Metadati**.

Viene visualizzato l'elenco dei metadati disponibili.

Limitazione dell'accesso a un VDC dell'organizzazione per utenti e gruppi specifici dell'organizzazione

L'**amministratore organizzazione** può limitare l'accesso a ogni singolo VDC dell'organizzazione a utenti e gruppi specifici.

Per impostazione predefinita, i VDC dell'organizzazione sono condivisi con tutti gli utenti e i gruppi a cui è assegnato un ruolo che include il diritto **Consenti accesso a tutti i VDC dell'organizzazione**.

Se l'organizzazione include più VDC e si desidera gestirli separatamente, è possibile creare un ruolo personalizzato che funga da amministratore del VDC dell'organizzazione e assegnarlo a utenti o gruppi specifici all'interno dell'organizzazione, consentendo loro di accedere solo alle risorse di elaborazione e di rete di un determinato VDC.

Prerequisiti

- 1 Assicurarsi di essere un **amministratore dell'organizzazione**.
- 2 Creare un ruolo personalizzato per gli utenti e i gruppi a cui si desidera fornire accesso a uno specifico VDC dell'organizzazione. Questo ruolo deve escludere il diritto **Consenti accesso a tutti i VDC dell'organizzazione**. Vedere [Capitolo 13 Gestione di utenti, gruppi e ruoli](#).

Procedura

- 1 Nella schermata del dashboard **Virtual data center**, fare clic sulla scheda del virtual data center a cui si desidera limitare l'accesso.
- 2 In **Impostazioni**, fare clic su **Condivisione**.
Viene visualizzato l'elenco degli utenti e dei gruppi dell'organizzazione che hanno accesso al VDC.
- 3 Per modificare le impostazioni di accesso al VDC dell'organizzazione, fare clic su **Modifica**.
- 4 Selezionare **Utenti e gruppi specifici**.

- 5 Nell'elenco **Utenti**, selezionare gli utenti a cui si desidera concedere accesso al VDC.
- 6 Nell'elenco **Gruppi**, selezionare i gruppi a cui si desidera concedere accesso al VDC.
- 7 Per condividere il VDC con gli utenti e i gruppi selezionati, fare clic su **Condividi**.

Risultati

L'accesso al VDC dell'organizzazione viene limitato agli utenti e ai gruppi selezionati.

Utilizzo di istanze, endpoint e proxy di vCenter Server dedicati



È possibile accedere a un ambiente di vCenter Server dedicato o ai componenti di vCenter Server da VMware Cloud Director Tenant Portal.

Data center di vSphere dedicati

In VMware Cloud Director, un SDDC (Software-Defined Data Center) incapsula un intero ambiente di vCenter Server dedicato.

Le istanze di vCenter Server dedicate in VMware Cloud Director rimuovono il requisito per cui un'istanza di vCenter Server deve essere accessibile pubblicamente.

L'**amministratore di sistema** può pubblicare una o più istanze di vCenter Server dedicate nell'organizzazione. È possibile utilizzare gli endpoint per accedere all'interfaccia utente o all'API dei componenti con proxy o senza proxy.

Endpoint

Un'istanza di vCenter Server dedicata può includere uno o più endpoint che forniscono l'accesso a componenti diversi dell'ambiente sottostante. Gli endpoint possono fornire un punto di accesso a un componente del data center, ad esempio un'istanza di vCenter Server, un host ESXi, un'istanza di NSX Manager o un'istanza di NSX-T Manager.

Gli endpoint possono essere connessi o meno a un proxy.

Proxy

VMware Cloud Director può fungere da server proxy HTTPS e fornire l'accesso a un'istanza di vCenter Server dedicata e a diversi componenti di istanze di vCenter Server condivise o dedicate che eseguono il backup dell'ambiente.

L'utente può accedere all'interfaccia utente o all'API dei componenti con proxy utilizzando il proprio account VMware Cloud Director.

Per accedere ai componenti con proxy, è necessario utilizzare Chrome Browser Extension for VMware Cloud Director oppure configurare manualmente il browser con le impostazioni del proxy.

Questo capitolo include i seguenti argomenti:

- [Utilizzo di Chrome Browser Extension for VMware Cloud Director](#)
- [Configurazione del browser con le impostazioni del proxy](#)
- [Accesso all'interfaccia utente di un componente utilizzando un endpoint](#)

Utilizzo di Chrome Browser Extension for VMware Cloud Director

È possibile utilizzare Chrome Browser Extension for VMware Cloud Director per accedere ai componenti di vSphere con proxy nel proprio ambiente.

Chrome Browser Extension for VMware Cloud Director fornisce la configurazione e l'autenticazione del proxy.

Chrome Browser Extension for VMware Cloud Director supporta ambienti multisito.

È possibile aggiungere l'estensione al browser Chrome tramite [Chrome Web Store](#).

Configurazione del browser con le impostazioni del proxy

Per poter accedere all'interfaccia utente di un componente vSphere con proxy, è necessario configurare i proxy pubblicati nell'organizzazione.

Per configurare il browser in modo che utilizzi i proxy pubblicati, copiare l'URL del file di configurazione automatica del proxy (PAC) nel browser.

Nota Quando l'**amministratore di sistema** pubblica un data center di vSphere dedicato nell'organizzazione o aggiunge un proxy a uno dei data center di vSphere dedicati, è possibile che sia necessario attendere qualche minuto prima che il browser recuperi nuovamente il PAC dall'URL specificato. Per forzare un aggiornamento del browser, è possibile ripetere questa procedura.

Prerequisiti

- Verificare che l'**amministratore di sistema** abbia pubblicato almeno un'istanza di vCenter Server dedicata e abilitata nell'organizzazione.
- Verificare che l'**amministratore di sistema** abbia pubblicato i diritti **SDDC_VIEW** e **Token: Gestione** nell'organizzazione e che il proprio ruolo includa tali diritti.
- Verificare che l'**amministratore di sistema** abbia pubblicato e abilitato il plug-in **COM Extension** nell'organizzazione. Questo plug-in fornisce la funzionalità per la visualizzazione e l'utilizzo di data center di vSphere dedicati nel VMware Cloud Director Tenant Portal.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Data center** e quindi su **Virtual data center**.
- 2 Nel riquadro **Data center vSphere dedicati**, fare clic su **Fare clic qui per visualizzare la guida alla configurazione del proxy**.

- 3 Copiare l'URL del PAC e fare clic su **Avanti**.
- 4 Seguire le istruzioni per configurare il browser in modo che punti all'URL del PAC.
- 5 Se il componente con proxy utilizza certificati autofirmati, importare i certificati nel browser.
 - a Nella scheda del data center di vSphere di destinazione, fare clic su **Azioni** e quindi su **Importa certificato**.
 - b Scaricare il certificato e l'elenco di revoche dei certificati (CRL).
 - c Importare il certificato scaricato nel browser.Consultare le istruzioni per l'utente relative al browser.

Accesso all'interfaccia utente di un componente utilizzando un endpoint

È possibile utilizzare gli endpoint per accedere all'interfaccia utente dei componenti con proxy o senza proxy con il proprio account VMware Cloud Director.

Prerequisiti

Se si desidera accedere a un componente con proxy, [Configurazione del browser con le impostazioni del proxy](#) oppure [Utilizzo di Chrome Browser Extension for VMware Cloud Director](#) a Google Chrome.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Data center** e quindi su **Virtual data center**.
- 2 Selezionare la scheda **Data center di vSphere dedicati**.
- 3 Aprire l'endpoint dell'istanza di vCenter Server dedicata.
 - Per aprire l'endpoint predefinito, fare clic su **Apri vSphere**.
 - Per aprire un endpoint non predefinito, eseguire i passaggi seguenti:
 - Fare clic sul menu **Azioni**, quindi su **Visualizza endpoint**.
 - Fare clic sull'URL dell'endpoint.

Se si accede a un componente con proxy, viene aperta una nuova scheda con le credenziali del proxy.

- 4 Se si accede a un componente con proxy, accedere al componente utilizzando le proprie credenziali.
 - a Immettere il nome utente e la password.
 - b Per attivare il proxy, fare clic su **Apri**.

Viene aperta una nuova scheda con la richiesta di eseguire l'autenticazione nel proxy.

- c Nella casella di testo **Nome utente**, incollare il nome utente copiato.
- d Nella casella di testo **Password**, incollare la password copiata e fare clic su **OK**.

Gestione dei modelli di vApp

9

Un modello di vApp è un'immagine della macchina virtuale caricata con un sistema operativo, applicazioni e dati. Tali modelli consentono di effettuare una configurazione uniforme delle macchine virtuali in tutta l'organizzazione. I modelli di vApp vengono aggiunti ai cataloghi.

Questo capitolo include i seguenti argomenti:

- [Visualizzazione di un modello di vApp](#)
- [Creazione di un modello di vApp da un file OVF](#)
- [Importazione di una macchina virtuale da vCenter Server come modello di vApp](#)
- [Assegnazione di un criterio di posizionamento della macchina virtuale e di un criterio di dimensionamento della macchina virtuale a un modello di vApp](#)
- [Download di un modello di vApp](#)
- [Eliminazione di un modello di vApp](#)

Visualizzazione di un modello di vApp

È possibile visualizzare l'elenco dei modelli di vApp che sono disponibili nei cataloghi a cui si ha accesso. È possibile visualizzare un modello di vApp ed esplorare le macchine virtuali che contiene.

Un utente può accedere solo ai modelli di vApp inclusi in elementi di catalogo che sono stati condivisi con tale utente. Per ulteriori informazioni sulla condivisione di cataloghi, vedere [Condividi un catalogo](#).

Prerequisiti


Questa operazione richiede i diritti inclusi nel ruolo **Autore vApp** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di vApp**.

L'elenco dei modelli viene visualizzato in una vista griglia.


- 2 (Facoltativo) Configurare la vista griglia in modo che contenga gli elementi che si desidera visualizzare.

- a Dalla vista griglia, fare clic sull'icona dell'editor () che si trova sotto l'elenco dei modelli di vApp.
- b Selezionare gli elementi che si desidera includere nella vista griglia, ad esempio versione, stato, catalogo, proprietario e così via.
- c Fare clic su **OK**.

Nella griglia vengono visualizzati gli elementi selezionati per ciascun modello di vApp nell'elenco.

- 3 Per visualizzare le macchine virtuali incluse in un modello di vApp, fare clic sul nome del modello di vApp.

Le macchine virtuali incluse nel modello di vApp vengono visualizzate in una griglia.

- 4 (Facoltativo) Per selezionare gli elementi che si desidera includere nella vista griglia, fare clic sull'icona dell'editor griglia () sotto l'elenco delle macchine virtuali.
 - a Selezionare gli elementi che si desidera includere nella vista griglia.
 - b Fare clic su **OK**.

Creazione di un modello di vApp da un file OVF

È possibile caricare un pacchetto OVF per creare un modello di vApp in un catalogo.

VMware Cloud Director supporta le specifiche OVF (Open Virtualization Format) e OVA (Open Virtualization Appliance). Se si carica un file OVF che include proprietà OVF per la personalizzazione delle rispettive macchine virtuali, tali proprietà vengono conservate nel modello di vApp. Per informazioni sulla creazione di pacchetti OVF, vedere *OVF Tool User Guide* e *VMware vCenter Converter User's Guide*.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di vApp**.
L'elenco dei modelli viene visualizzato in una vista griglia.
- 2 Fare clic su **Nuovo**.

- 3 Immettere un indirizzo URL per il file OVF o fare clic sull'icona **Carica** per scegliere una posizione accessibile dal proprio computer e selezionare il file del modello OVF/OVA.

Il percorso può essere il disco rigido locale, una condivisione di rete o un'unità CD/DVD.

Le estensioni di file supportate includono `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` e `.strings`. Se si sceglie di caricare un file OVF, che fa riferimento a più file rispetto a quelli che si sta tentando di caricare, ad esempio un file VMDK, è necessario cercare e selezionare tutti i file.

- 4 Verificare i dettagli del modello OVF/OVA da distribuire e fare clic su **Avanti**.
- 5 Digitare un nome e, facoltativamente, una descrizione per il modello di vApp, quindi fare clic su **Avanti**.
- 6 Dal menu a discesa **Catalogo**, selezionare il catalogo a cui si desidera aggiungere il modello.
- 7 Controllare le impostazioni del modello di vApp e fare clic su **Fine**.

Risultati

Il nuovo modello di vApp viene visualizzato nella vista griglia dei modelli.

Importazione di una macchina virtuale da vCenter Server come modello di vApp

Se si dispone dei diritti di **amministratore di sistema**, è possibile importare le macchine virtuali di vCenter Server in VMware Cloud Director come modelli di vApp nei cataloghi.

Prerequisiti

Per visualizzare e importare macchine virtuali da vCenter Server come modelli di vApp, verificare di disporre dei diritti di **amministratore di sistema**.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di vApp**.
L'elenco dei modelli viene visualizzato in una vista griglia.
- 2 Fare clic su **Importa da vCenter**.
- 3 Dal menu a discesa, selezionare un'istanza di vCenter Server da cui importare il modello di vApp.
- 4 Selezionare un modello nell'elenco delle macchine virtuali.
- 5 Immettere un nome e, facoltativamente, una descrizione per il modello di vApp.
- 6 Dal menu a discesa, selezionare un catalogo in cui aggiungere il modello di vApp.
- 7 (Facoltativo) Per eliminare la macchina virtuale di origine, attivare l'opzione **Sposta macchina virtuale**.
- 8 (Facoltativo) Contrassegnare il modello di vApp come modello preferito nel catalogo.

9 Fare clic su **Importa**.

Assegnazione di un criterio di posizionamento della macchina virtuale e di un criterio di dimensionamento della macchina virtuale a un modello di vApp

Per associare le macchine virtuali di un modello di vApp a specifici criteri di posizionamento e dimensionamento della macchina virtuale, è possibile contrassegnare singole macchine virtuali di un modello di vApp con i criteri che si desidera assegnare.

A partire da VMware Cloud Director 10.0 è possibile consentire agli utenti di modificare i criteri predefiniti di posizionamento o dimensionamento delle macchine virtuali durante la modifica di una macchina virtuale.

Nota Dopo aver eseguito l'aggiornamento a VMware Cloud Director 10.0 o versione successiva, tutte le assegnazioni dei tag del modello preesistenti diventano modificabili. Se si desidera impedire le modifiche ai criteri predefiniti di posizionamento o dimensionamento delle macchine virtuali, è necessario deselezionare la casella di controllo **Modificabile** per i criteri da rendere non modificabili.

Prerequisiti

- Questa operazione richiede il diritto di modificare un modello di vApp.
- Verificare che nel proprio ambiente VMware Cloud Director sia presente almeno un modello di vApp.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di vApp**.
L'elenco dei modelli viene visualizzato in una vista griglia.
- 2 Selezionare il pulsante di opzione accanto al modello di vApp a cui si desidera aggiungere un tag e fare clic su **Tag con criteri di calcolo**.
- 3 Se si desidera assegnare un criterio di posizionamento della macchina virtuale a una macchina virtuale nel modello di vApp, selezionare un criterio dal menu a discesa **Criteri posizionamento macchina virtuale** nella riga corrispondente alla macchina virtuale.
- 4 Se si desidera assegnare un criterio di dimensionamento della macchina virtuale a una macchina virtuale nel modello di vApp, selezionare un criterio dal menu a discesa **Criterio di dimensionamento macchina virtuale** nella riga corrispondente alla macchina virtuale.
- 5 (Facoltativo) Per consentire agli utenti di modificare i criteri di posizionamento o dimensionamento della macchina virtuale predefiniti durante la modifica di una macchina virtuale, selezionare la casella di controllo **Modificabile** nel menu a discesa del criterio.
- 6 Fare clic su **Tag**.

Download di un modello di vApp

È possibile scaricare nel computer locale un modello di vApp da un catalogo come file OVA.


Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di vApp**.

L'elenco dei modelli viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra del modello di vApp che si desidera scaricare e scegliere **Scarica**.

Nota È possibile scaricare i modelli di vApp dai cataloghi dell'organizzazione. Se l'utente è un amministratore dell'organizzazione, può scaricare i modelli di vApp da un catalogo pubblico. In caso contrario, il pulsante **Scarica** è inattivo.

- 3 (Facoltativo) Per preservare gli UUID e gli indirizzi MAC delle macchine virtuali nel pacchetto OVA scaricato, selezionare la casella di controllo **Mantieni informazioni di identità**.
- 4 Fare clic su **OK** e attendere il completamento del download.

Il file OVA viene salvato nel percorso di download predefinito del browser Web.

Eliminazione di un modello di vApp

È possibile eliminare un modello di vApp dal catalogo di un'organizzazione. Se il catalogo è pubblicato, il modello di vApp viene eliminato anche dai cataloghi pubblici.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore vApp** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di vApp**.

L'elenco dei modelli viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra del modello di vApp che si desidera eliminare e scegliere **Elimina**.

3 Confermare l'eliminazione.

Il modello di vApp eliminato viene rimosso dalla vista griglia.

Gestione dei file multimediali

10

Il catalogo consente di caricare, copiare, spostare e modificare le proprietà dei file multimediali.

Questo capitolo include i seguenti argomenti:

- [Caricamento di file multimediali](#)
- [Eliminazione di un file multimediale](#)
- [Download di un file multimediale](#)

Caricamento di file multimediali

È possibile caricare in un catalogo nuovi file multimediali o nuove versioni di file multimediali esistenti. Gli utenti autorizzati ad accedere al catalogo possono aprire i file multimediali con le proprie macchine virtuali.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Multimedia e altro**.

L'elenco dei file multimediali viene visualizzato in una vista griglia.

- 2 Fare clic su **Aggiungi**.
- 3 Dal menu a discesa **Catalogo**, selezionare il catalogo in cui si desidera caricare il file multimediale.

- 4 Immettere un nome per il file multimediale.

Se non si immette alcun nome, la casella di testo del nome viene compilata automaticamente in base al nome del file multimediale.

- 5 Fare clic sull'icona di caricamento per cercare e selezionare il file di immagine del disco, ad esempio un file `.iso`.

6 Fare clic su **OK**.

Dopo aver avviato il caricamento, il file multimediale viene visualizzato nella griglia.

Operazioni successive

A seconda delle dimensioni del file, il completamento del caricamento potrebbe richiedere qualche minuto. È possibile monitorare lo stato del caricamento nella visualizzazione **Task recenti**. Per ulteriori informazioni, vedere [Visualizzazione dei task](#).

Eliminazione di un file multimediale

È possibile eliminare dal catalogo i file multimediali che non si desidera più utilizzare.


Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Multimedia e altro**.

L'elenco dei file multimediali viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra del file multimediale che si desidera eliminare e scegliere **Elimina**.
- 3 Confermare l'eliminazione.

Il file multimediale eliminato viene rimosso dalla visualizzazione griglia.

Download di un file multimediale

È possibile scaricare un file multimediale da un catalogo.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Multimedia e altro**.

L'elenco dei file multimediali viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra del file multimediale che si desidera scaricare e scegliere **Scarica**.

L'attività di download viene avviata e il file viene salvato nel percorso di download predefinito del browser Web.

Operazioni successive

A seconda delle dimensioni del file, il completamento del download potrebbe richiedere qualche minuto. È possibile monitorare lo stato del download nel pannello **Task recenti**. Per ulteriori informazioni, vedere [Visualizzazione dei task](#).

Gestione dei cataloghi

11

Un catalogo è un contenitore per i modelli di vApp e i file multimediali in un'organizzazione. Gli amministratori dell'organizzazione e gli autori del catalogo possono creare cataloghi in un'organizzazione. I contenuti dei cataloghi possono essere condivisi con altri utenti o organizzazioni nell'installazione di VMware Cloud Director. Oppure, possono essere pubblicati esternamente per consentirne l'accesso da parte di organizzazioni esterne all'installazione di VMware Cloud Director.

VMware Cloud Director contiene cataloghi privati, condivisi e accessibili esternamente. I cataloghi privati includono modelli di vApp e file multimediali che è possibile condividere con altri utenti dell'organizzazione. Se un amministratore di sistema abilita la condivisione di cataloghi per l'organizzazione, è possibile condividere un catalogo dell'organizzazione per creare un catalogo accessibile per le altre organizzazioni incluse nell'installazione di VMware Cloud Director. Se un amministratore di sistema abilita la pubblicazione esterna di un catalogo per l'organizzazione, è possibile pubblicare un catalogo dell'organizzazione a cui le organizzazioni esterne all'installazione di VMware Cloud Director possono accedere. Un'organizzazione esterna all'installazione di VMware Cloud Director deve effettuare la sottoscrizione a un catalogo pubblicato esternamente per poter accedere al relativo contenuto.

È possibile caricare un pacchetto OVF direttamente in un catalogo, salvare una vApp come modello di vApp oppure importare un modello vApp da vSphere. Vedere [Creazione di un modello di vApp da un file OVF](#) e [Salvataggio di una vApp come modello di vApp in un catalogo](#).

I membri di un'organizzazione possono accedere a modelli di vApp e file multimediali posseduti o condivisi con loro. Gli amministratori dell'organizzazione e di sistema possono condividere un catalogo con chiunque all'interno dell'organizzazione o con utenti e gruppi specifici. Vedere [Condividi un catalogo](#).

Questo capitolo include i seguenti argomenti:

- [Visualizzazione dei cataloghi](#)
- [Creazione di un catalogo](#)
- [Condividi un catalogo](#)
- [Eliminazione di un catalogo](#)
- [Modifica del proprietario di un catalogo](#)
- [Gestione dei metadati per un catalogo](#)

- Pubblicazione di un catalogo
- Sottoscrizione a un catalogo esterno
- Aggiornamento dell'URL della posizione e della password per un catalogo sottoscritto
- Sincronizzazione di un catalogo sottoscritto

Visualizzazione dei cataloghi

L'utente può accedere ai cataloghi condivisi con il suo account all'interno dell'organizzazione. È possibile accedere ai cataloghi pubblici se un amministratore dell'organizzazione li ha resi accessibili all'interno dell'organizzazione.


L'accesso ai cataloghi è controllato mediante la condivisione dei cataloghi e non mediante i diritti inclusi nel ruolo dell'utente. Un utente può accedere solo ai cataloghi o agli elementi dei cataloghi che vengono condivisi con tale utente. Per ulteriori informazioni, vedere [Condividi un catalogo](#).

Procedura


- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.

L'elenco dei cataloghi viene visualizzato in una vista griglia.

- 2 (Facoltativo) Configurare la vista griglia in modo che contenga gli elementi che si desidera visualizzare.

- a Dalla vista griglia, fare clic sull'icona dell'editor () che si trova sotto l'elenco di cataloghi.
- b Selezionare gli elementi che si desidera includere nella vista griglia, ad esempio versione, descrizione, stato e così via.
- c Fare clic su **OK**.

Nella griglia sono visualizzati gli elementi selezionati per ciascun catalogo.

- 3 (Facoltativo) Dalla vista griglia utilizzare la barra dell'elenco () per visualizzare le azioni che è possibile eseguire per ciascun catalogo.

Ad esempio, è possibile condividere o eliminare un catalogo.

Creazione di un catalogo

È possibile creare nuovi cataloghi e associarli a un criterio di storage.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.
L'elenco dei cataloghi viene visualizzato in una vista griglia.
- 2 Fare clic su **Nuovo** per creare un nuovo catalogo.
- 3 Immettere il nome e, facoltativamente, una descrizione del catalogo.
- 4 (Facoltativo) Scegliere se si desidera assegnare un criterio di storage al catalogo e selezionare un criterio di storage.
- 5 Fare clic su **OK**.

Risultati

Il nuovo catalogo viene visualizzato nella visualizzazione griglia nella scheda **Cataloghi**.


Condividi un catalogo

È possibile condividere un catalogo con tutti i membri dell'organizzazione o con membri specifici.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.
- È necessario essere il proprietario del catalogo.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.
L'elenco dei cataloghi viene visualizzato in una vista griglia.
- 2 Fare clic sulla barra dell'elenco () a sinistra del catalogo che si desidera condividere e scegliere **Condividi**.
L'elenco degli utenti che possono accedere al catalogo viene visualizzato nella vista griglia della finestra **Condividi catalogo**.
- 3 Fare clic su **Aggiungi** per condividere il catalogo con altri utenti.

Opzione	Descrizione
Condividi con chiunque nell'organizzazione	Concede l'accesso a tutti gli utenti e i gruppi nell'organizzazione.
Condividi con utenti o gruppi specifici	Selezionare gli utenti o gruppi a cui si desidera concedere l'accesso al catalogo e fare clic su Aggiungi .

4 Selezionare il livello di accesso.

Opzione	Descrizione
Sola lettura	Gli utenti che dispongono dell'accesso a questo catalogo hanno accesso in lettura ai modelli di vApp e ai file ISO del catalogo.
Lettura/Scrittura	Gli utenti che dispongono dell'accesso a questo catalogo hanno accesso in lettura ai modelli di vApp e ai file ISO del catalogo e possono aggiungere modelli di vApp e file ISO al catalogo.
Controllo completo	Gli utenti con accesso a questo catalogo hanno il controllo completo dei contenuti e delle impostazioni del catalogo.

5 Fare clic su **OK**.

Gli utenti o i gruppi che ora dispongono dell'accesso al catalogo vengono visualizzati nella vista griglia della finestra di dialogo **Condividi catalogo**.

6 (Facoltativo) Scegliere di condividere l'accesso in sola lettura con gli amministratori di tutte le altre organizzazioni

7 Fare clic su **Salva**.

Risultati

Nella scheda **Cataloghi**, cambia lo stato Condiviso di questo catalogo nella vista griglia.

Eliminazione di un catalogo

È possibile eliminare un catalogo dall'organizzazione.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Autore catalogo** predefinito o un set di diritti equivalente.

Nota Il catalogo non deve contenere alcun modello di vApp o file multimediale. È possibile spostare questi elementi in un catalogo diverso o eliminarli.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.

L'elenco dei cataloghi viene visualizzato in una vista griglia.

2 Fare clic sulla barra dell'elenco () a sinistra del catalogo che si desidera eliminare e scegliere **Elimina**.

3 Confermare l'eliminazione.

L'elemento del catalogo eliminato viene rimosso dalla vista griglia.

Modifica del proprietario di un catalogo

Un **amministratore dell'organizzazione** può cambiare il proprietario di un catalogo.

Prima di poter eliminare un utente che possiede un catalogo, è necessario modificare il proprietario o eliminare il catalogo.


Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.

L'elenco dei cataloghi viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra di un catalogo e selezionare **Cambia proprietario**.

L'elenco degli utenti che possono accedere al catalogo viene visualizzato nella vista griglia della finestra **Cambia proprietario**.

- 3 Selezionare l'utente che si desidera impostare come nuovo proprietario del catalogo e fare clic su **OK**.

Risultati

Nella scheda **Cataloghi**, il nome del proprietario del catalogo nella vista griglia cambia.

Gestione dei metadati per un catalogo

In qualità di **amministratore di un'organizzazione** o **proprietario di un catalogo**, è possibile creare o aggiornare i metadati per i cataloghi di cui si è proprietario.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.

L'elenco dei cataloghi viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra di un catalogo e selezionare **Metadati**.

I metadati per il catalogo selezionato vengono visualizzati in una griglia.

3 (Facoltativo) Per aggiungere metadati, fare clic su **Aggiungi**.

- a Immettere il nome dei metadati.

Il nome deve essere univoco rispetto ai nomi dei metadati collegati a questo oggetto.

- b Selezionare il tipo di metadati, come **Testo**, **Numero**, **Data e ora** o **Sì o No**.
- c Immettere il valore dei metadati.
- d Fare clic su **Salva**.

4 (Facoltativo) Aggiornare i metadati esistenti.

Il nome dei metadati non può essere aggiornato.

- a Aggiornare il tipo di metadati.
- b Immettere il nuovo valore dei metadati.
- c Fare clic su **Salva**.

5 (Facoltativo) Eliminare i metadati esistenti.

- a Fare clic sull'icona di eliminazione.
- b Fare clic su **Salva**.

Pubblicazione di un catalogo

Se l'**amministratore di sistema** ha autorizzato l'accesso al catalogo, è possibile pubblicare un catalogo esternamente per renderne i modelli di vApp e i file multimediali disponibili per la sottoscrizione a tutte le organizzazioni esterne all'installazione di VMware Cloud Director.


Prerequisiti

Verificare che l'**amministratore di sistema** abbia abilitato la pubblicazione di cataloghi esterna per l'organizzazione e abbia fornito l'accesso al catalogo.

Procedura

- 1** Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.

L'elenco dei cataloghi viene visualizzato in una vista griglia.

- 2** Fare clic sulla barra dell'elenco () a sinistra del catalogo che si desidera pubblicare e scegliere **Impostazioni di pubblicazione**.

- 3** Selezionare **Abilita pubblicazione** e, facoltativamente, immettere una password per l'accesso al catalogo.

Sono supportati solo caratteri ASCII.

- 4** Fare clic su **Salva**.

Sottoscrizione a un catalogo esterno

È possibile effettuare la sottoscrizione a un catalogo esterno e quindi creare una copia di sola lettura di un catalogo pubblicato esternamente. Non è possibile modificare un catalogo sottoscritto.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- L'**amministratore di sistema** deve concedere all'organizzazione l'autorizzazione a sottoscrivere cataloghi esterni.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.
L'elenco dei cataloghi viene visualizzato in una vista griglia.
- 2 Fare clic su **Nuovo** per creare un nuovo catalogo.
- 3 Immettere il nome e, facoltativamente, una descrizione del catalogo.
- 4 Scegliere di sottoscrivere un catalogo esterno e specificare l'URL di sottoscrizione.
- 5 Immettere la password opzionale per accedere al catalogo.
- 6 Scegliere se si desidera scaricare automaticamente il contenuto dal catalogo esterno.
- 7 Fare clic su **OK**.

Aggiornamento dell'URL della posizione e della password per un catalogo sottoscritto

Dopo aver creato un catalogo sottoscritto, è possibile aggiornare l'URL della posizione e la password per il catalogo sottoscritto.


Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- È necessario aver creato un catalogo sottoscritto.
- L'**amministratore di sistema** deve concedere all'organizzazione l'autorizzazione a sottoscrivere cataloghi esterni.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.

L'elenco dei cataloghi viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra di un catalogo sottoscritto e scegliere **Impostazioni di sottoscrizione**.

Se il catalogo non è stato sottoscritto, l'opzione è disattivata.

- 3 Aggiornare l'URL della posizione e la password per questo catalogo sottoscritto.
- 4 Scegliere se si desidera scaricare automaticamente il contenuto dal catalogo esterno.
- 5 Fare clic su **Salva**.

Sincronizzazione di un catalogo sottoscritto

Dopo aver creato un catalogo sottoscritto, è possibile sincronizzarlo con il catalogo originale per verificare se sono state apportate modifiche. Ad esempio, se i metadati del catalogo originale sono stati modificati, quando si esegue la sincronizzazione, i metadati del catalogo sottoscritto vengono aggiornati.


Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- È necessario aver creato un catalogo sottoscritto.
- L'**amministratore di sistema** deve concedere all'organizzazione l'autorizzazione a sottoscrivere cataloghi esterni.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Cataloghi**.

L'elenco dei cataloghi viene visualizzato in una vista griglia.

- 2 Fare clic sulla barra dell'elenco () a sinistra di un catalogo sottoscritto e scegliere **Sincronizza**.

Se il catalogo non è stato sottoscritto, l'opzione è disattivata.

Il catalogo sottoscritto viene sincronizzato con quello originale.

Gestione dei modelli di virtual data center dell'organizzazione

12

Gli amministratori dell'organizzazione e gli utenti che dispongono di qualsiasi altro ruolo con i diritti per visualizzare e creare istanze di modelli di virtual data center dell'organizzazione, possono creare virtual data center dell'organizzazione aggiuntivi.

Un modello di virtual data center dell'organizzazione specifica una configurazione per un virtual data center dell'organizzazione e, facoltativamente, un gateway edge e una rete di virtual data center dell'organizzazione. Gli amministratori di sistema possono consentire agli amministratori dell'organizzazione di creare queste risorse nella loro organizzazione creando modelli di virtual data center dell'organizzazione e condividendoli con tali organizzazioni.

Creando e condividendo modelli di virtual data center, gli amministratori di sistema abilitano il provisioning self-service dei virtual data center dell'organizzazione, mantenendo al tempo stesso il controllo amministrativo sull'allocazione delle risorse di sistema come i virtual data center del provider e le reti esterne.

Gli amministratori di sistema creano modelli di virtual data center dell'organizzazione e forniscono alle diverse organizzazioni l'accesso ai modelli.

Se l'organizzazione dispone dell'accesso ai modelli di virtual data center, è possibile utilizzare VMware Cloud Director Tenant Portal per creare virtual data center dai modelli disponibili.

Questo capitolo include i seguenti argomenti:

- [Visualizzazione dei modelli di virtual data center disponibili](#)
- [Creazione di un'istanza di virtual data center da un modello](#)

Visualizzazione dei modelli di virtual data center disponibili

Un utente può visualizzare i modelli di virtual data center dell'organizzazione che un amministratore di sistema ha creato per lui.

Visualizzare i modelli di virtual data center prima di creare un nuovo virtual data center dell'organizzazione da tale modello.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un ruolo che disponga dei diritti per visualizzare e creare istanze di modelli di virtual data center dell'organizzazione.

Procedura

- ◆ Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di VDC dell'organizzazione**.

L'elenco dei modelli di virtual data center viene visualizzato in una vista griglia.

Operazioni successive

Rivedere le descrizioni dei modelli di virtual data center dell'organizzazione e selezionare il modello da cui si desidera creare un nuovo virtual data center dell'organizzazione.

Creazione di un'istanza di virtual data center da un modello

Quando un amministratore di sistema crea un modello di virtual data center (VDC) dell'organizzazione e lo pubblica nell'organizzazione, è possibile creare un VDC dell'organizzazione dal modello.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un ruolo che disponga dei diritti per visualizzare e creare istanze di modelli di VDC dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e nel pannello sinistro selezionare **Modelli di VDC dell'organizzazione**.

L'elenco dei modelli di virtual data center viene visualizzato in una vista griglia.

- 2 Selezionare un modello e fare clic su **Nuovo VDC**.

A partire da VMware Cloud Director 10.2.2, dopo aver selezionato un modello è necessario fare clic su **Crea istanza di VDC**.

- 3 Immettere il nome del VDC e, facoltativamente, una descrizione.
- 4 Fare clic su **Crea**.

Risultati

La creazione dell'istanza del nuovo virtual data center dell'organizzazione potrebbe richiedere qualche minuto. È possibile visualizzare l'avanzamento dell'attività nel pannello **Task recenti**.

Operazioni successive

È possibile gestire il virtual data center dell'organizzazione appena creato mediante la creazione di macchine virtuali e vApp, la gestione delle impostazioni di rete e di sicurezza e così via.

Gestione di utenti, gruppi e ruoli

13

È possibile aggiungere gli amministratori dell'organizzazione a VMware Cloud Director singolarmente o come parte di un gruppo LDAP. È inoltre possibile aggiungere e modificare i ruoli che determinano i diritti di cui un utente dispone nell'ambito della propria organizzazione.

Importante Per gestire utenti, gruppi e ruoli all'interno dell'organizzazione, è necessario essere un **amministratore dell'organizzazione**. L'**amministratore di sistema** può pubblicare uno o più ruoli tenant globali per il tenant, mentre un **amministratore dell'organizzazione** può visualizzarli nell'elenco dei ruoli. Tali ruoli sono, ad esempio, **Autore catalogo**, **Autore vApp**, **Utente vApp**, **Amministratore organizzazione** e così via. Non è possibile modificare i ruoli tenant globali predefiniti, ma è possibile creare e aggiornare ruoli tenant personalizzati simili e assegnarli agli utenti all'interno del tenant.

Questo capitolo include i seguenti argomenti:

- [Gestione degli utenti](#)
- [Gestione di gruppi](#)
- [Ruoli e diritti](#)

Gestione degli utenti

Dal portale tenant è possibile creare, modificare, importare ed eliminare utenti. È inoltre possibile sbloccare un account utente nel caso in cui un utente abbia tentato di accedere con una password non corretta bloccando il proprio account.

Creazione di un utente

È possibile creare un utente all'interno dell'organizzazione di VMware Cloud Director.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Utenti**.

Viene visualizzato l'elenco degli utenti.

- 3 Fare clic su **Nuovo**.

- 4 Immettere un nome utente e una password per l'utente.

La lunghezza minima della password è di sei caratteri.

- 5 Specificare se si desidera abilitare l'utente al momento della creazione.

- 6 Se si desidera impostare una limitazione specifica per le risorse disponibili per l'utente, attivare l'opzione **Configura quota utente**.

Se si attiva l'opzione, al termine della procedura guidata, VMware Cloud Director reindirizza alla pagina **Quote**. È possibile aggiungere quote per il numero di cluster di Tanzu Kubernetes, tutte le macchine virtuali in esecuzione gestite dall'utente, nonché CPU, memoria e storage consumati. Selezionare **Illimitato** se si desidera che l'utente disponga di risorse del tipo selezionato illimitate.

- 7 Scegliere il ruolo che si desidera assegnare all'utente.

Il menu **Ruoli disponibili** contiene un elenco dei ruoli predefiniti e di tutti i ruoli personalizzati creati dall'utente corrente o dall'amministratore di sistema.

Ruolo predefinito	Descrizione
Autore vApp	I diritti associati al ruolo Autore vApp predefinito consentono a un utente di utilizzare i cataloghi e creare vApp.
Solo accesso console	I diritti associati al ruolo Solo accesso console predefinito consentono a un utente di visualizzare le proprietà e lo stato della macchina virtuale e di utilizzare il sistema operativo guest.
Utente vApp	I diritti associati al ruolo Utente vApp predefinito consentono a un utente di utilizzare le vApp esistenti.
Amministratore dell'organizzazione	L'utente con ruolo Amministratore organizzazione predefinito può utilizzare Cloud Director OpenAPI o il portale tenant di VMware Cloud Director per gestire utenti e gruppi dell'organizzazione e assegnare loro i ruoli, incluso quello di Amministratore organizzazione predefinito. Un Amministratore organizzazione può utilizzare Cloud Director OpenAPI per creare o aggiornare gli oggetti ruolo locali dell'organizzazione. I ruoli creati o modificati da un amministratore organizzazione non sono visibili per le altre organizzazioni.
Rimanda a provider di identità	I diritti associati al ruolo Rimanda a provider di identità predefinito sono determinati in base alle informazioni ricevute dall'OAuth dell'utente o dal provider di identità SAML. Affinché l'utente a cui è stato assegnato il ruolo Rimanda a provider di identità possa essere incluso, il nome del ruolo fornito dal provider di identità deve essere esattamente uguale a un ruolo o un nome definito nell'organizzazione, maiuscole e minuscole comprese.
Autore catalogo	I diritti associati al ruolo Autore catalogo predefinito consentono a un utente di creare e pubblicare cataloghi.

- 8 (Facoltativo) Immettere le informazioni di contatto, come nome, indirizzo e-mail, numero di telefono e ID di messaggistica istantanea.
- 9 Fare clic su **Salva**.

Operazioni successive

Se è stata abilitata la configurazione delle quote per l'utente e VMware Cloud Director reindirizza alla pagina **Quote**, consultare [Gestione delle quote delle risorse di un utente](#).

Importa utenti

È possibile aggiungere utenti alle organizzazioni importando utenti LDAP o SAML e assegnando loro un determinato ruolo.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- Assicurarsi di disporre di una connessione valida a un server LDAP o di [Consentire all'organizzazione l'uso di un provider di identità SAML](#).

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Utenti**.
Viene visualizzato l'elenco degli utenti.
- 3 Fare clic su **Importa utenti**.
- 4 Selezionare l'origine da cui si desidera importare gli utenti.

Sarà possibile visualizzare solo il server LDAP o il server SAML di origine configurato come provider di identità.

Origine	Azione
LDAP	<p>Importare utenti da un server LDAP.</p> <ol style="list-style-type: none"> a Immettere un nome completo o parziale nella casella di testo e fare clic su Cerca. b Selezionare gli utenti da importare e fare clic su Aggiungi.
SAML	<p>Importare utenti da un server SAML. Immettere i nomi degli utenti che si desidera importare.</p> <p>I nomi utente devono essere nel formato identificatore nome supportato dal provider di identità SAML configurato per questa organizzazione.</p> <p>Nota Se si utilizza vCenter Single Sign-On come provider di identità SAML, i nomi utente importati da un dominio vCenter Single Sign-On devono essere nel formato UPN (User Principal Name), ad esempio jdoe@mydomain.com.</p> <p>Utilizzare una nuova riga per ciascun nome utente.</p>

5 Selezionare il ruolo da assegnare agli utenti importati.

6 Fare clic su **Salva**.

Modifica di un utente

In qualità di amministratore dell'organizzazione, è possibile modificare la password, il contatto e le impostazioni di quota della macchina virtuale di un utente esistente. È inoltre possibile modificare il ruolo dell'utente.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Utenti**.

Viene visualizzato l'elenco degli utenti.

3 Fare clic sul pulsante di opzione accanto al nome dell'utente che si desidera modificare e fare clic su **Modifica**.

4 Aggiornare le impostazioni che si desidera modificare.

a Modificare la password in base alle necessità.

b Selezionare se attivare o disattivare l'utente.

c Aggiornare il ruolo dell'utente.

d Aggiornare le informazioni di contatto, come nome, indirizzo e-mail, numero di telefono e ID di messaggistica istantanea.

e Modificare la quota della macchina virtuale per l'utente.

5 Fare clic su **Salva**.

Disattivazione o attivazione di un account utente

È possibile disattivare un account utente per impedire a tale utente di accedere a VMware Cloud Director. Per eliminare un utente, è innanzitutto necessario disattivarne l'account.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Utenti**.

Viene visualizzato l'elenco degli utenti.

- 3 Per disattivare un account utente, fare clic sul pulsante di opzione accanto al nome utente, fare clic su **Disabilita** e confermare.
- 4 Per attivare un account che è già stato disattivato, fare clic sul pulsante di opzione accanto al nome utente e quindi su **Abilita**.

Eliminazione di un utente

È possibile rimuovere un utente dall'organizzazione VMware Cloud Director eliminando il relativo account utente.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- Disattivare l'account che desideri eliminare.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Utenti**.
Viene visualizzato l'elenco degli utenti.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'utente che si desidera eliminare e fare clic su **Elimina**.
- 4 Per confermare che si desidera eliminare l'account utente, fare clic su **OK**.

Sblocco di un account utente bloccato

Se nell'organizzazione di VMware Cloud Director è abilitato un criterio di blocco, un account utente viene bloccato dopo un determinato numero di tentativi di accesso non validi. È possibile sbloccare l'account utente bloccato. La procedura consigliata consiste nel modificare la password dell'utente e sbloccare l'account.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Utenti**.
Viene visualizzato l'elenco degli utenti.

- 3 Fare clic sul pulsante di opzione accanto al nome utente e quindi su **Sblocca**.

Gestione delle quote delle risorse di un utente

È possibile gestire il limite di consumo complessivo delle risorse di un utente. È possibile aggiungere, modificare e rimuovere le quote dell'utente su macchine virtuali, Tanzu Kubernetes cluster, CPU, memoria o storage.

Gli utenti possono visualizzare le quote pertinenti solo per il tipo di utente. Gli utenti ereditano le quote dal gruppo a cui appartengono. Se un utente eredita una quota di risorsa dal proprio gruppo e dispone di una quota a livello di utente esplicita definita per tale risorsa, la quota a livello di utente avrà la priorità sulla quota a livello di gruppo.

Per informazioni sulla creazione o l'importazione di utenti, vedere [Creazione di un utente](#) o [Importa utenti](#).

Prerequisiti

Verificare di disporre dei diritti necessari per aggiungere, modificare ed eliminare le quote di risorse. Per impostazione predefinita, gli **amministratori dell'organizzazione** possono modificare le quote degli utenti.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Utenti**.
- 3 Selezionare il nome di un utente e selezionare la scheda **Quote**.

Per impostazione predefinita, gli utenti non dispongono di quote. Tutti gli utenti appartenenti a un gruppo ereditano le quote del gruppo. Se l'utente appartiene a un gruppo che dispone di una quota nelle risorse, la quota viene visualizzata nell'elenco di quote dell'utente come non modificabile.

- 4 Fare clic su **Modifica**.
- 5 Modificare la quota per l'utente selezionato.

È possibile aggiungere, modificare o rimuovere le quote nel numero di cluster di Tanzu Kubernetes, di tutte le macchine virtuali gestite dall'utente o in esecuzione, nonché di CPU, memoria e storage consumati. Selezionare **Illimitato** se si desidera che l'utente disponga di risorse del tipo selezionato illimitate.

- 6 Fare clic su **Salva**.

Gestione di gruppi

Se si dispone di una connessione valida a un server LDAP o se si è consentito all'organizzazione di utilizzare un provider di identità SAML, è possibile importare un gruppo LDAP o SAML. È inoltre possibile modificare o eliminare un gruppo importato.

Importazione di un gruppo

Per aggiungere un gruppo di utenti, è possibile importare un gruppo LDAP o un gruppo SAML.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- Assicurarsi di disporre di una connessione valida a un server LDAP o di [Consentire all'organizzazione l'uso di un provider di identità SAML](#).

Procedura

1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Gruppi**.

Viene visualizzato l'elenco dei gruppi di utenti.

3 Fare clic su **Importa gruppi**.

4 Selezionare l'origine da cui si desidera importare il gruppo di utenti.

È possibile visualizzare solo il server LDAP o il server SAML di origine configurato come provider di identità.

Origine	Azione
LDAP	Importare un gruppo di utenti da un server LDAP. <ol style="list-style-type: none"> a Immettere un nome completo o parziale nella casella di testo e fare clic su Cerca. b Selezionare i gruppi di utenti da importare e fare clic su Aggiungi.
SAML	Importare gruppi di utenti da un server SAML. Immettere i nomi dei gruppi che si desidera importare. Utilizzare una nuova riga per ciascun nome di gruppo.

5 Selezionare il ruolo da assegnare al gruppo di utenti importati.

6 Fare clic su **Salva**.

Operazioni successive

Se è stata abilitata la configurazione delle quote per il gruppo e VMware Cloud Director reindirizza alla pagina **Quote**, consultare [Gestione delle quote delle risorse di un gruppo](#).

Eliminazione di un gruppo

È possibile rimuovere un gruppo dall'organizzazione di VMware Cloud Director eliminando il gruppo LDAP.

Quando si elimina un gruppo LDAP, gli utenti che dispongono di un account VMware Cloud Director basato unicamente sulla propria appartenenza a tale gruppo vengono bloccati e non possono più effettuare l'accesso.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Gruppi**.
Viene visualizzato l'elenco dei gruppi di utenti.
- 3 Fare clic sul pulsante di opzione accanto al nome del gruppo che si desidera eliminare e fare clic su **Elimina**.
- 4 Per confermare che si desidera eliminare il gruppo, fare clic su **OK**.

Modifica di un gruppo

È possibile modificare un gruppo dal portale tenant di VMware Cloud Director.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Gruppi**.
Viene visualizzato l'elenco dei gruppi di utenti.
- 3 Fare clic sul pulsante di opzione accanto al nome del gruppo che si desidera modificare e fare clic su **Modifica**.
- 4 Modificare il gruppo in base alle necessità.
 - a Modificare la descrizione.
 - b Modificare il ruolo dei membri del gruppo in base alle necessità.
- 5 Fare clic su **Salva**.

Gestione delle quote delle risorse di un gruppo

Se si imposta direttamente la quota in un gruppo, è possibile gestire il limite di consumo complessivo delle risorse di ogni utente in esso. È possibile aggiungere, modificare e rimuovere le quote del gruppo su macchine virtuali, Tanzu Kubernetes cluster, CPU, memoria o storage. Le quote del gruppo vengono applicate in ogni membro del gruppo.

Gli utenti ereditano le quote dal gruppo a cui appartengono. Se un utente eredita una quota di risorsa dal proprio gruppo e dispone di una quota a livello di utente esplicita definita per tale risorsa, la quota a livello di utente avrà la priorità sulla quota a livello di gruppo.

Per informazioni sull'importazione di gruppi, vedere [Importazione di un gruppo](#).

Prerequisiti

Verificare di disporre dei diritti necessari per aggiungere, modificare ed eliminare le quote di risorse. Per impostazione predefinita, gli **amministratori dell'organizzazione** possono modificare le quote dei gruppi.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Gruppi**.
- 3 Selezionare il nome di un gruppo e selezionare la scheda **Quote**.

Per impostazione predefinita, i gruppi non dispongono di quote. Tutti gli utenti appartenenti a un gruppo ereditano le quote del gruppo. Se l'utente appartiene a un gruppo che dispone di una quota nelle risorse, la quota viene visualizzata nell'elenco di quote dell'utente come non modificabile.

- 4 Fare clic su **Modifica**.
- 5 Modificare la quota per il gruppo selezionato.

È possibile aggiungere, modificare o rimuovere le quote nel numero di cluster di Tanzu Kubernetes, di tutte le macchine virtuali gestite dal gruppo o in esecuzione, nonché di CPU, memoria e storage consumati. Selezionare **Illimitato** se si desidera che il gruppo di utenti disponga di risorse del tipo selezionato illimitate.

- 6 Fare clic su **Salva**.

Ruoli e diritti

VMware Cloud Director utilizza ruoli e diritti per determinare le azioni che un utente può eseguire in un'organizzazione. VMware Cloud Director include diversi ruoli predefiniti con diritti specifici.

Gli **amministratori di sistema** e gli **amministratori dell'organizzazione** devono assegnare un ruolo a ogni utente o gruppo. Lo stesso utente può presentare un ruolo diverso nelle varie organizzazioni. Gli **amministratori di sistema** possono creare ruoli e modificare quelli esistenti per l'intero sistema, mentre gli **amministratori dell'organizzazione** possono creare e modificare solo i ruoli per l'organizzazione che amministrano.

Il portale tenant di VMware Cloud Director consente agli **amministratori dell'organizzazione** di gestire i ruoli nella propria organizzazione. Se un **amministratore di sistema** pubblica uno o più ruoli tenant predefiniti nell'organizzazione, l'**amministratore dell'organizzazione** può visualizzare questi ruoli, ma non può modificarli. Può però creare ruoli tenant personalizzati con diritti simili e assegnarli agli utenti all'interno dell'organizzazione.

Per informazioni sui ruoli predefiniti e sui relativi diritti, vedere [Ruoli predefiniti e relativi diritti](#).

Ruoli predefiniti e relativi diritti

Ogni ruolo predefinito di VMware Cloud Director contiene un set predefinito di permessi che consentono di eseguire le operazioni tipiche di flussi di lavoro comuni. Per impostazione predefinita, tutti i ruoli tenant predefiniti globali vengono pubblicati in tutte le organizzazioni nel sistema.

Ruoli del provider predefiniti

Per impostazione predefinita, i ruoli del provider che sono locali solo per l'organizzazione del provider sono i ruoli **Amministratore di sistema** e **Sistema multisito**. Un **amministratore di sistema** può creare ruoli del provider personalizzati aggiuntivi.

Amministratore di sistema

Il ruolo **Amministratore di sistema** esiste solo nell'organizzazione del provider. Il ruolo **Amministratore di sistema** include tutti i diritti del sistema. Per un elenco dei diritti disponibili solo per il ruolo **Amministratore di sistema**, vedere *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*. Le credenziali del ruolo **Amministratore di sistema** vengono stabilite durante l'installazione e la configurazione. Un **Amministratore di sistema** può creare ulteriori account di amministratore di sistema e utenti nell'organizzazione del provider.

Sistema multisito

Utilizzato per eseguire il processo heartbeat per le distribuzioni multisito. Questo ruolo dispone di un unico diritto, ovvero **Operazioni sistema multisito**, che fornisce le autorizzazioni per creare una richiesta di Cloud Director OpenAPI che recuperi lo stato del membro remoto di un'associazione di siti.

Ruoli tenant globali predefiniti

Per impostazione predefinita, i ruoli tenant globali predefiniti e i diritti che includono vengono pubblicati in tutte le organizzazioni. Gli utenti che dispongono del ruolo **Amministratore di sistema** possono annullare la pubblicazione dei diritti e dei ruoli tenant globali nelle singole organizzazioni. Gli utenti che dispongono del ruolo **Amministratore di sistema** possono modificare o eliminare i ruoli tenant globali predefiniti. Gli **amministratori di sistema** possono creare e pubblicare ruoli tenant globali aggiuntivi.

Amministratore organizzazione

Dopo avere creato un'organizzazione, un **Amministratore di sistema** può assegnare il ruolo **Amministratore organizzazione** a qualsiasi utente nell'organizzazione. L'utente con ruolo **Amministratore organizzazione** predefinito può gestire utenti e gruppi dell'organizzazione e assegnare loro i ruoli, incluso quello di **Amministratore organizzazione** predefinito. I ruoli creati o modificati da un **amministratore organizzazione** non sono visibili per le altre organizzazioni.

Autore catalogo

I diritti associati al ruolo **Autore catalogo** predefinito consentono a un utente di creare e pubblicare cataloghi.

Autore vApp

I diritti associati al ruolo **Autore vApp** predefinito consentono a un utente di utilizzare i cataloghi e creare vApp.

Utente vApp

I diritti associati al ruolo **Utente vApp** predefinito consentono a un utente di utilizzare le vApp esistenti.

Solo accesso console

I diritti associati al ruolo **Solo accesso console** predefinito consentono a un utente di visualizzare le proprietà e lo stato della macchina virtuale e di utilizzare il sistema operativo guest.

Rimanda a provider di identità

I diritti associati al ruolo **Rimanda a provider di identità** predefinito sono determinati in base alle informazioni ricevute dall'OAuth dell'utente o dal provider di identità SAML. Affinché un utente o un gruppo a cui è assegnato il ruolo **Rimanda a provider di identità** possa essere incluso, il nome del ruolo o del gruppo fornito dal provider di identità deve essere esattamente uguale al nome del ruolo o del gruppo definito nella propria organizzazione, maiuscole e minuscole comprese.

- Se un provider di identità OAuth definisce l'utente, l'utente viene assegnato ai ruoli denominati nell'array `roles` del token OAuth dell'utente.
- Se un provider di identità SAML definisce l'utente, l'utente viene assegnato ai ruoli denominati nell'attributo SAML i cui nomi vengono visualizzati nell'elemento `RoleAttributeName`, ovvero l'elemento `SamlAttributeMapping` nell'array `OrgFederationSettings` dell'organizzazione.

Se a un utente viene assegnato il ruolo **Rimanda a provider di identità** ma non è presente alcun nome di ruolo o gruppo corrispondente nella propria organizzazione, l'utente potrà accedere all'organizzazione, ma non avrà alcun diritto. Se un provider di identità associa un utente a un ruolo a livello di sistema, ad esempio **Amministratore di sistema**, l'utente può accedere all'organizzazione ma non dispone di alcun diritto. È necessario assegnare manualmente un ruolo a tali utenti.

Ad eccezione del ruolo **Rimanda a provider di identità**, ciascun ruolo predefinito include un set di diritti predefiniti. Solo un **Amministratore di sistema** può modificare i diritti in un ruolo predefinito. Se un **amministratore di sistema** modifica un ruolo predefinito, le modifiche vengono propagate a tutte le istanze del ruolo nel sistema.

Diritti nei ruoli tenant globali predefiniti

Diversi diritti sono comuni a più ruoli globali predefiniti. Tali diritti vengono concessi per impostazione predefinita a tutte le nuove organizzazioni e possono essere utilizzati in altri ruoli creati da un **Amministratore organizzazione**. Per un elenco dei diritti nei ruoli tenant predefiniti, vedere [Diritti nei ruoli tenant globali predefiniti](#).

Diritti nei ruoli tenant globali predefiniti

Diversi diritti sono comuni a più ruoli globali predefiniti. Tali diritti vengono concessi per impostazione predefinita a tutte le nuove organizzazioni e possono essere utilizzati in altri ruoli creati da un **Amministratore organizzazione**.

Diritti inclusi nei ruoli tenant globali in VMware Cloud Director

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Accesso a tutti i VDC dell'organizzazione	✓				
	Catalogo: Aggiungi vApp da Cloud personale	✓	✓	✓		
	Catalogo: Cambia proprietario	✓				
	Catalogo: Pubblicazione e iscrizione con CLSP	✓	✓			
	Catalogo: Crea/Elimina catalogo	✓	✓			
	Catalogo: Modifica proprietà	✓	✓			
	Catalogo: Pubblica	✓	✓			
	Catalogo: Condivisione	✓	✓			
	Catalogo: Visualizza ACL	✓	✓			
	Catalogo: Visualizza cataloghi privati e condivisi	✓	✓	✓		
	Catalogo: Visualizza cataloghi pubblicati	✓				
	Entità personalizzata: Visualizza tutte le istanze di entità personalizzata nell'organizzazione	✓				
	Entità personalizzata: Visualizza istanza entità personalizzata	✓				
	Disco: Cambia proprietario	✓	✓			
	Disco: Crea	✓	✓	✓		

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Disco: Elimina	✓	✓	✓		
	Disco: Modifica proprietà	✓	✓	✓		
	Disco: visualizzazione stato crittografia	✓		✓		
	Disco: Visualizza proprietà	✓	✓	✓	✓	
	Generale: Controllo amministratore	✓				
	Generale: Vista amministratore	✓				
	Generale: Invia notifica	✓				
	Gruppo/Utente: Visualizza	✓				
	Operazioni cloud ibride: Acquisisci ticket di controllo	✓				
	Operazioni cloud ibrido: Acquisisci ticket del tunnel dal cloud	✓				
	Operazioni cloud ibrido: Acquisisci ticket del tunnel verso il cloud	✓				
	Operazioni cloud ibrido: Crea tunnel dal cloud	✓				
	Operazioni cloud ibrido: Crea tunnel verso il cloud	✓				
	Operazioni cloud ibrido: Elimina tunnel dal cloud	✓				
	Operazioni cloud ibrido: Elimina tunnel verso il cloud	✓				
	Operazioni cloud ibrido: Aggiorna il tag dell'endpoint per il tunnel dal cloud	✓				
	Operazioni cloud ibrido: Visualizza tunnel dal Cloud	✓				
	Operazioni cloud ibrido: Visualizza tunnel verso il cloud	✓				
	Rete organizzazione: Modifica proprietà	✓				
	Rete organizzazione: Visualizza	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Criterio di calcolo del vDC dell'organizzazione: Visualizza	✓	✓	✓	✓	
	Firewall distribuito del vDC dell'organizzazione: Configura regole	✓				
	Firewall distribuito del vDC dell'organizzazione: Visualizza regole	✓				
	Gateway vDC dell'organizzazione: Configura DHCP	✓				
	Gateway vDC dell'organizzazione: Configura DNS	✓				
	Gateway vDC dell'organizzazione: Configura routing ECMP	✓				
	Gateway vDC dell'organizzazione: Configura firewall	✓				
	Gateway vDC dell'organizzazione: Configura VPN IPSec	✓				
	Gateway vDC dell'organizzazione: Configura bilanciamento del carico	✓				
	Gateway vDC dell'organizzazione: Configura NAT	✓				
	Gateway vDC dell'organizzazione: Configura routing statico	✓				
	Gateway vDC dell'organizzazione: Configura syslog	✓				
	Gateway vDC dell'organizzazione: Converti in servizi di rete avanzati	✓				
	Gateway vDC dell'organizzazione: Visualizza	✓				
	Gateway vDC dell'organizzazione: Visualizza DHCP	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Gateway vDC dell'organizzazione: Visualizza DNS	✓				
	Gateway vDC dell'organizzazione: Visualizza firewall	✓				
	Gateway vDC dell'organizzazione: Visualizza VPN IPSec	✓				
	Gateway vDC dell'organizzazione: Visualizza bilanciamento del carico	✓				
	Gateway vDC dell'organizzazione: Visualizza NAT	✓				
	Gateway vDC dell'organizzazione: Visualizza routing statico	✓				
	Rete vDC dell'organizzazione: Modifica proprietà	✓				
	Rete vDC dell'organizzazione: Visualizza proprietà	✓		✓		
	Criterio di storage vDC dell'organizzazione: visualizzazione funzionalità	✓				
	Profilo di storage vDC dell'organizzazione: Imposta valore predefinito	✓				
	vDC dell'organizzazione: Modifica	✓				
	vDC dell'organizzazione: Modifica ACL	✓				
	vDC dell'organizzazione: Gestisci firewall	✓				
	vDC dell'organizzazione: Visualizza	✓	✓			
	vDC dell'organizzazione: Visualizza ACL	✓				
	VDC dell'organizzazione: Visualizza metriche	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	vDC dell'organizzazione: Modifica affinità macchina virtuale-macchina virtuale	✓	✓	✓		
	Organizzazione: Modifica impostazioni di associazione	✓				
	Organizzazione: Modifica impostazioni di federazione	✓				
	Organizzazione: Modifica impostazioni LDAP	✓				
	Organizzazione: Modifica criterio dei lease	✓				
	Organizzazione: Modifica impostazioni OAuth	✓				
	Organizzazione: Modifica criterio password	✓				
	Organizzazione: Modifica proprietà	✓				
	Organizzazione: Modifica criterio quote	✓				
	Organizzazione: Modifica impostazioni SMTP	✓				
	Organizzazione: Importa utente/gruppo da IdP durante la modifica dell'ACL del VDC	✓				
	Organizzazione: Visualizza	✓	✓	✓		
	Organizzazione: Visualizza metriche	✓				
✓	Funzionalità criterio di quota: Visualizza	✓				
	Ruolo: Crea, Modifica, Elimina o Copia	✓				
	Libreria dei servizi: Visualizza librerie dei servizi	✓				
	Plug-in interfaccia utente: Visualizza	✓	✓	✓	✓	
	Modello di vApp/media: Copia	✓	✓	✓		
	Modello di vApp/media: Crea/Carica	✓	✓			
	Modello di vApp/media: Modifica	✓	✓	✓		

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Modello di vApp/media: Visualizza	✓	✓	✓	✓	
	Modello di vApp: Cambia proprietario	✓	✓			
	Modello di vApp: Checkout	✓	✓	✓	✓	
	Modello di vApp: Scarica	✓	✓			
	vApp: Cambia proprietario	✓				
	vApp: Copia	✓	✓	✓	✓	
	vApp: Crea/Riconfigura	✓	✓	✓		
	vApp: Elimina	✓	✓	✓	✓	
	vApp: Scarica	✓	✓	✓		
	vApp: Modifica proprietà	✓	✓	✓	✓	
	vApp: Modifica criterio di calcolo della macchina virtuale	✓	✓	✓		
	vApp: Modifica CPU della macchina virtuale	✓	✓	✓		
	vApp: Modifica disco rigido della macchina virtuale	✓	✓	✓		
	vApp: Modifica memoria della macchina virtuale	✓	✓	✓		
	vApp: Modifica rete della macchina virtuale	✓	✓	✓	✓	
	vApp: Modifica proprietà della macchina virtuale	✓	✓	✓	✓	
	vApp: Gestisci impostazioni password macchina virtuale	✓	✓	✓	✓	✓
	vApp: Operazioni di attivazione	✓	✓	✓	✓	
	vApp: Condivisione	✓	✓	✓	✓	
	vApp: Operazioni di creazione di snapshot	✓	✓	✓	✓	
	vApp: Carica	✓	✓	✓		
	vApp: Utilizza console	✓	✓	✓	✓	✓
	vApp: Visualizza ACL	✓	✓	✓	✓	

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	vApp: visualizzazione macchina virtuale e stato crittografia dischi macchina virtuale	✓		✓		
	vApp: Visualizza metriche della macchina virtuale	✓		✓	✓	
	vApp: Opzioni di avvio della macchina virtuale	✓	✓	✓		
	vApp: metadati macchina virtuale in vCenter	✓	✓	✓		
✓	Gruppo di VDC: Configura	✓				
✓	Gruppo di VDC: Visualizza	✓				
✓	Gruppo di VDC: Configura registrazione	✓				
	Modello di VDC: Crea istanze	✓				
	Modello di VDC: Visualizza	✓				

Creazione di un ruolo tenant personalizzato

Gli amministratori dell'organizzazione possono utilizzare il portale tenant per creare oggetti ruolo tenant personalizzati nelle organizzazioni da loro amministrate.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Ruoli**.
Viene visualizzato l'elenco dei ruoli.
- 3 Fare clic su **Aggiungi**.
- 4 Immettere un nome e, facoltativamente, una descrizione del ruolo.

5 Espandere i diritti per il ruolo e selezionarli.

I diritti sono raggruppati in categorie e sottocategorie che consentono la visualizzazione o la gestione degli oggetti.

Opzione	Descrizione
Controllo accessi	Diritti che controllano l'accesso per visualizzare e gestire determinati oggetti.
Amministrazione	Diritti che controllano l'accesso amministrativo.
Calcola	Diritti che controllano l'accesso e la gestione dei virtual data center del provider e dell'organizzazione, le vApp, i modelli dei virtual data center dell'organizzazione, i gruppi di macchine virtuali e il monitoraggio della macchina virtuale.
Estensioni	Diritti che controllano l'accesso a tutti i plug-in e le estensioni di VMware Cloud Director aggiuntivi.
Infrastruttura	Diritti che controllano l'accesso e la gestione degli oggetti dell'infrastruttura, come archivi dati, dischi, host e così via.
Librerie	Diritti che controllano l'accesso e la gestione di tutti i cataloghi e gli elementi dei cataloghi.
Rete	Diritti che controllano l'accesso e la gestione delle impostazioni di rete.

6 Fare clic su **Salva**.

Modifica di un ruolo tenant personalizzato

Gli amministratori delle organizzazioni possono utilizzare il portale tenant per modificare gli oggetti ruolo tenant personalizzati nelle organizzazioni che amministrano. Come amministratore dell'organizzazione, è possibile solo visualizzare i ruoli tenant globali che un amministratore di sistema ha pubblicato all'organizzazione. Non è possibile modificarli.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Ruoli**.
Viene visualizzato l'elenco dei ruoli.
- 3 Fare clic sul pulsante di opzione accanto al ruolo che si desidera modificare e fare clic su **Modifica**.
- 4 Modificare le impostazioni del ruolo in base alle necessità.
 - a Modificare il nome e, facoltativamente, la descrizione del ruolo.
 - b Modificare i diritti per il ruolo.

- 5 Fare clic su **Salva**.

Eliminazione di un ruolo

Gli amministratori di un'organizzazione possono utilizzare il portale tenant per eliminare gli oggetti ruolo nell'organizzazione amministrata.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi**, fare clic su **Ruoli**.
Viene visualizzato l'elenco dei ruoli.
- 3 Fare clic sul pulsante di opzione accanto al ruolo che si desidera eliminare e fare clic su **Elimina**.
- 4 Confermare che si desidera eliminare il ruolo facendo clic su **OK**.

Configurazione dei provider di identità

14

È possibile integrare il cloud con un provider di identità esterno e importare utenti e gruppi nell'organizzazione.

È possibile abilitare l'organizzazione per l'utilizzo di un provider di identità SAML oppure configurare una connessione al server LDAP.

Questo capitolo include i seguenti argomenti:

- [Consentire all'organizzazione l'uso di un provider di identità SAML](#)
- [Modifica delle impostazioni LDAP dell'organizzazione](#)
- [Configurazione, prova e sincronizzazione di una connessione LDAP](#)

Consentire all'organizzazione l'uso di un provider di identità SAML

È possibile consentire all'organizzazione di utilizzare un provider di identità SAML (Security Assertion Markup Language), noto anche come Single Sign-On, per importare utenti e gruppi da un provider di identità SAML e permettere agli utenti importati di accedere all'organizzazione con le credenziali stabilite nel provider di identità SAML.

Quando si importano utenti e gruppi, il sistema estrae un elenco degli attributi dal token SAML, se disponibile, e li utilizza per interpretare le informazioni corrispondenti relative all'utente che prova ad accedere.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

L'attributo ruolo è configurabile.

Le informazioni sul gruppo sono necessarie se l'utente non viene importato direttamente ma è previsto che sia in grado di accedere in virtù dell'appartenenza ai gruppi importati. Un utente può appartenere a più gruppi e pertanto disporre di più ruoli durante una sessione.

Se a un utente o un gruppo importato viene assegnato il ruolo **Rimanda a provider di identità**, i ruoli vengono assegnati in base alle informazioni raccolte dall'attributo Ruoli nel token. Se viene utilizzato un attributo diverso, il nome di questo attributo può essere configurato solo mediante API ed è configurabile solo l'attributo Ruoli. Se viene utilizzato il ruolo **Rimanda a provider di identità**, ma non è possibile estrarre alcuna informazione sul ruolo, l'utente può accedere ma non dispone di alcun diritto per eseguire le attività.

Prerequisiti

- Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.
- Verificare di disporre dell'accesso a un provider di identità compatibile con SAML 2.0.
- Assicurarsi di ricevere i metadati richiesti dal provider di identità SAML. È necessario importare i metadati in VMware Cloud Director manualmente o come file XML. I metadati devono includere le informazioni seguenti:
 - Posizione del servizio Single Sign-On
 - Posizione del servizio single logout
 - Posizione del certificato del servizio X.509

Per informazioni sulla configurazione e sull'acquisizione di metadati da un provider SAML, consultare la documentazione del provider di identità SAML.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 In **Provider di identità** fare clic su **SAML**.
- 3 Fare clic su **Modifica**.
- 4 Nella scheda **Provider di servizi**, immettere l'ID entità.

L'ID entità è l'identificatore univoco dell'organizzazione per il provider di identità. È possibile utilizzare il nome dell'organizzazione o qualsiasi altra stringa che soddisfi i requisiti del provider di identità SAML.

Importante Dopo aver specificato un ID entità, non è possibile eliminarlo. Per modificare l'ID entità, è necessario eseguire una riconfigurazione di SAML completa per la propria organizzazione. Per ulteriori informazioni sugli ID entità, vedere la sezione relativa ad [asserzioni e protocolli per il linguaggio SAML \(Security Assertion Markup Language\) 2.0 di OASIS](#).

- 5 Fare clic sul link **Metadati** per scaricare i metadati SAML per l'organizzazione.

I metadati scaricati devono essere forniti al provider di identità così come sono.

- 6 Verificare la data di scadenza del certificato e, se lo si desidera, fare clic su **Rigenera** per rigenerare il certificato utilizzato per firmare i messaggi relativi alla federazione.

Il certificato è incluso nei metadati SAML e viene utilizzato per la crittografia e per la firma.

Potrebbero essere necessarie la crittografia, la firma o entrambe, a seconda della modalità con cui viene stabilita l'attendibilità tra l'organizzazione e il provider di identità SAML.

- 7 Nella scheda **Provider di identità** abilitare l'interruttore **Utilizza provider identità SAML**.
- 8 Copiare e incollare i metadati SAML ricevuti dal provider di identità nella casella di testo o fare clic su **Carica** per individuare e caricare i metadati da un file XML.
- 9 Fare clic su **Salva**.

Operazioni successive

- Configurare il provider SAML con i metadati di VMware Cloud Director. Consultare la documentazione del provider di identità SAML e *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.
- Importare utenti e gruppi dal provider di identità SAML. Vedere [Capitolo 13 Gestione di utenti, gruppi e ruoli](#)

Modifica delle impostazioni LDAP dell'organizzazione

È possibile configurare l'organizzazione in modo che utilizzi la connessione LDAP del sistema come origine condivisa di utenti e gruppi. È possibile configurare l'organizzazione in modo che utilizzi una connessione LDAP distinta come origine privata di utenti e gruppi.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Provider di identità**, fare clic su **LDAP**.
Vengono visualizzate le impostazioni di LDAP correnti.
- 3 Nella scheda **Impostazioni LDAP**, fare clic su **Modifica**.

- 4 Configurare l'origine LDAP di utenti e gruppi per questa organizzazione e fare clic su **Salva**.

Opzione	Descrizione
Non utilizzare LDAP	L'organizzazione non utilizza un server LDAP come origine di utenti e gruppi dell'organizzazione.
Servizio LDAP del sistema VMware Cloud Director	L'organizzazione utilizza la connessione LDAP del sistema VMware Cloud Director configurata dal provider di servizi. Immettere il nome distinto per l'unità organizzativa.
Servizio LDAP personalizzato	L'organizzazione utilizza un server LDAP privato come origine di utenti e gruppi dell'organizzazione.

Operazioni successive

Se è stata selezionata l'opzione **Servizio LDAP personalizzato**, fare clic sulla scheda **LDAP personalizzato** per [Configurazione, prova e sincronizzazione di una connessione LDAP](#).

Configurazione, prova e sincronizzazione di una connessione LDAP

Per configurare una connessione LDAP, è necessario impostare i dettagli del server LDAP. È possibile provare la connessione per verificare che le impostazioni immesse e la mappatura degli attributi di utenti e gruppi siano corrette. Dopo aver configurato correttamente una connessione LDAP, è possibile sincronizzare i dati di utenti e gruppi con il server LDAP in qualsiasi momento.

Prerequisiti

Se si prevede di connettersi a un server LDAP su SSL (LDAPS), verificare che il certificato del server LDAP sia conforme all'identificazione dell'endpoint introdotta in Java 8 Update 181. Il nome comune (CN) o il nome alternativo dell'oggetto (SAN) del certificato deve coincidere con il nome di dominio completo del server LDAP. Per ulteriori informazioni, vedere *l'argomento relativo alle modifiche di Java 8* all'indirizzo <https://www.java.com>.

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella scheda **Connessione**, immettere le informazioni richieste per la connessione LDAP.

Informazioni richieste	Descrizione
Server	Il nome host o l'indirizzo IP del server LDAP.
Porta	Il numero della porta in cui il server LDAP è in ascolto. Per LDAP, il numero di porta predefinito è 389. Per LDAPS, il numero di porta predefinito è 636.

Informazioni richieste	Descrizione
Nome distinto di base	<p>Il nome distinto di base (DN) è la posizione nella directory LDAP per la connessione con VMware Cloud Director.</p> <p>Per connettersi al livello root, immettere solo i componenti del dominio, ad esempio DC=example,DC=com.</p> <p>Per connettersi a un nodo nella struttura del dominio, immettere il nome distinto del nodo, ad esempio OU=ServiceDirector,DC=example,DC=com.</p> <p>La connessione a un nodo limita l'ambito della directory disponibile per VMware Cloud Director.</p>
Tipo di connettore	Il tipo di server LDAP in uso. Può essere Active Directory o OpenLDAP .
Usa SSL	Se il server è LDAPS, selezionare questa casella di controllo.
Accetta tutti i certificati	Se il server è LDAPS, selezionare questa casella di controllo o caricare il certificato SSL LDAP.
Archivio attendibilità personalizzato	Se il server è LDAPS, fare clic sul pulsante Carica e importare un certificato SSL LDAP o selezionare Accetta tutti i certificati .
Metodo di autenticazione	<p>L'autenticazione semplice consiste nell'invio del nome distinto e della password dell'utente al server LDAP. Se si utilizza LDAP, la password LDAP viene inviata attraverso la rete come testo normale.</p> <p>Se si desidera utilizzare Kerberos, è necessario configurare la connessione LDAP usando l'API di vCloud.</p>
Nome utente	<p>Immettere il nome distinto LDAP completo di un account di servizio con diritti di amministratore del dominio. VMware Cloud Director utilizza questo account per eseguire una query nella directory LDAP e recuperare le informazioni dell'utente.</p> <p>Se sul server LDAP è abilitato il supporto per la lettura anonima, è possibile lasciare vuote queste caselle di testo.</p>
Password	<p>Password dell'account di servizio che si connette al server LDAP.</p> <p>Se sul server LDAP è abilitato il supporto per la lettura anonima, è possibile lasciare vuote queste caselle di testo.</p>

- 2 Fare clic sulla scheda **Attributi utente**, esaminare i valori predefiniti per gli attributi degli utenti e, se la directory LDAP utilizza uno schema diverso, modificare i valori.
- 3 Fare clic sulla scheda **Attributi gruppo**, esaminare i valori predefiniti per gli attributi del gruppo e, se la directory LDAP utilizza uno schema diverso, modificare i valori.
- 4 Fare clic su **Salva**.
- 5 Se è stata selezionata la casella di controllo **Usa SSL** e se il certificato del server LDAPS non è ancora attendibile, nella finestra **Certificato di attendibilità**, confermare se si ritiene attendibile il certificato presentato dall'endpoint del server.

6 Per testare le impostazioni della connessione LDAP e le mappature degli attributi LDAP:

- a Fare clic su **Test**
- b Immettere la password dell'utente del server LDAP configurato e fare clic su **Test**.

Se la connessione è riuscita, viene visualizzato un segno di spunta verde.

I valori degli attributi di utenti e gruppi recuperati vengono visualizzati in una tabella. I valori che sono correttamente mappati agli attributi LDAP sono contrassegnati con segni di spunta verdi. I valori che non sono mappati agli attributi LDAP sono contrassegnati con punti esclamativi rossi.

- c Per uscire, fare clic su **Annulla**.

7 Per sincronizzare VMware Cloud Director con il server LDAP configurato, fare clic su **Sincronizza**.

VMware Cloud Director sincronizza regolarmente le informazioni di utenti e gruppi con il server LDAP, in base all'intervallo di sincronizzazione impostato nelle impostazioni generali del sistema.

Attendere alcuni minuti fino al termine della sincronizzazione.

Risultati

Dal server LDAP appena configurato è possibile importare utenti e gruppi.

È possibile importare, scaricare, modificare ed eliminare certificati in VMware Cloud Director. È possibile copiare i dati PEM del certificato negli Appunti.

Questo capitolo include i seguenti argomenti:

- [Importazione di certificati attendibili](#)
- [Importazione dei certificati nella libreria di certificati](#)

Importazione di certificati attendibili

È possibile importare certificati di server con cui VMware Cloud Director comunica, ad esempio vCenter Server, NSX Manager e così via.

Quando si utilizza VMware Cloud Director in modalità FIPS, è necessario utilizzare chiavi private compatibili con FIPS. È possibile utilizzare pyOpenSSL per generare chiavi private nel formato PKCS#8 compatibile con FIPS. Se si generano chiavi private PKCS#8 utilizzando OpenSSL, le chiavi private non sono compatibili con FIPS. Per ulteriori informazioni sulla modalità FIPS, vedere [Attivazione della modalità FIPS nelle celle nel gruppo di server](#) o [Attivazione o disattivazione della modalità FIPS nell'appliance di VMware Cloud Director](#).

Prerequisiti

Verificare di aver effettuato l'accesso come **amministratore di sistema** o **amministratore dell'organizzazione**.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Gestione certificato**, selezionare **Certificati attendibili**, quindi fare clic su **Importa**.
- 3 Caricare un file PEM contenente i certificati che si desidera importare e fare clic su **Importa**.
- 4 (Facoltativo) Modificare il nome del certificato.
- 5 Fare clic su **Importa**.

Operazioni successive

- Scaricare un certificato.

- Modificare il nome di un certificato.
- Eliminare un certificato.
- Copiare i dati PEM negli Appunti.

Importazione dei certificati nella libreria di certificati

Nella libreria di certificati di VMware Cloud Director, è possibile importare i certificati utilizzati durante la creazione delle entità che è necessario proteggere, ad esempio i server, i gateway edge e così via.

La libreria di certificati contiene informazioni su singoli certificati, catene di certificati, chiavi private, date di scadenza dei certificati, entità protette dai certificati e così via.

Quando si utilizza VMware Cloud Director in modalità FIPS, è necessario utilizzare certificati autofirmati e chiavi private compatibili con FIPS. È possibile generare certificati non crittografati autofirmati e chiavi private utilizzando PyOpenSSL. Se si generano certificati autofirmati e chiavi private utilizzando OpenSSL, i certificati e le chiavi private non sono compatibili con FIPS. Per ulteriori informazioni sulla modalità FIPS, vedere [Attivazione della modalità FIPS nelle celle nel gruppo di server](#) o [Attivazione o disattivazione della modalità FIPS nell'appliance di VMware Cloud Director](#).

Prerequisiti

Verificare di aver effettuato l'accesso come **amministratore di sistema** o **amministratore dell'organizzazione**.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Gestione certificato**, selezionare **Libreria certificati**, quindi fare clic su **Importa**.
- 3 Digitare un nome e, facoltativamente, una descrizione per questo certificato nella libreria di certificati, quindi fare clic su **Avanti**.
- 4 Caricare un file PEM contenente la catena di certificati che si desidera importare e fare clic su **Avanti**.
- 5 (Facoltativo) Caricare un file di chiave privata.
Il file di chiave privata potrebbe non essere protetto con una passphrase.
- 6 Fare clic su **Importa**.

Risultati

Il certificato importato viene visualizzato nell'elenco dei certificati disponibili durante la creazione di entità che è necessario proteggere.

Operazioni successive

- Scaricare un certificato.
- Modificare il nome e la descrizione di un certificato.
- Eliminare un certificato. È possibile eliminare solo i certificati che non proteggono alcuna entità.
- Copiare i dati PEM del certificato negli Appunti.

In qualità di **amministratore dell'organizzazione**, è possibile modificare diverse impostazioni all'interno dell'organizzazione. È possibile modificare il nome dell'organizzazione, le impostazioni del programma e-mail, le impostazioni del dominio, i metadati, i criteri e così via.

È possibile utilizzare l'API di VMware Cloud Director per effettuare la sottoscrizione ai messaggi relativi a eventi e attività nell'organizzazione tramite il protocollo MQTT. Vedere le informazioni sulla sottoscrizione di eventi e attività tramite un client MQTT nella *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

Questo capitolo include i seguenti argomenti:

- [Modifica del nome e della descrizione di un'organizzazione](#)
- [Modifica delle impostazioni e-mail](#)
- [Test delle impostazioni SMTP](#)
- [Modifica delle impostazioni del dominio per le macchine virtuali dell'organizzazione](#)
- [Utilizzo di più siti](#)
- [Configurazione e gestione di distribuzioni multisito](#)
- [Informazioni generali sui lease](#)
- [Modifica dei criteri di lease delle vApp e dei modelli di vApp nell'organizzazione](#)
- [Modifica dei criteri di password e account utente nell'organizzazione](#)
- [Creazione di un dashboard di avvisi](#)

Modifica del nome e della descrizione di un'organizzazione

È possibile modificare il nome completo e la descrizione della propria organizzazione.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

2 In **Impostazioni** fare clic su **Generale**.

Viene visualizzato l'elenco delle impostazioni generali, ad esempio il nome dell'organizzazione, l'URL predefinito, il nome completo e la descrizione.

3 Per modificare il nome completo e la descrizione dell'organizzazione, fare clic su **Modifica**.

4 Applicare le modifiche necessarie e fare clic su **Salva**.

Modifica delle impostazioni e-mail

È possibile rivedere e modificare le impostazioni e-mail predefinite configurate dall'amministratore di sistema durante la creazione dell'organizzazione.

VMware Cloud Director invia e-mail di avviso quando deve segnalare informazioni importanti, ad esempio quando un archivio dati sta esaurendo lo spazio disponibile. Per impostazione predefinita, un'organizzazione invia avvisi tramite e-mail agli amministratori di sistema oppure a un elenco di indirizzi e-mail specificato a livello di sistema utilizzando un server SMTP specificato a livello di sistema. È possibile modificare le impostazioni e-mail a livello di organizzazione se si desidera che VMware Cloud Director invii gli avvisi per tale organizzazione a un gruppo di indirizzi e-mail diverso da quello specificato a livello di sistema o se si desidera che l'organizzazione utilizzi per l'invio degli avvisi un server SMTP diverso da quello specificato a livello di sistema.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

2 In **Impostazioni**, fare clic su **E-mail**.

Vengono visualizzate le impostazioni e-mail per l'organizzazione.

3 Fare clic su **Modifica**.

4 Modificare le impostazioni del server SMTP nella scheda **Server SMTP**.

- a Selezionare se utilizzare un server SMTP personalizzato o quello predefinito.
- b Se si sceglie di utilizzare un server SMTP personalizzato, immettere il nome host DNS o l'indirizzo IP del server SMTP nella casella di testo **Nome server SMTP**.
- c (Facoltativo) Immettere la porta del server SMTP.
- d (Facoltativo) Scegliere se richiedere l'autenticazione e immettere un nome utente e la password.

- 5 Per modificare le impostazioni di notifica, fare clic sulla scheda **Impostazioni di notifica**.
 - a Scegliere di utilizzare impostazioni di notifica personalizzate.
 - b Immettere l'indirizzo che verrà visualizzato come mittente dei messaggi e-mail dell'organizzazione.
 - c (Facoltativo) Immettere il testo da utilizzare come prefisso dell'oggetto dell'e-mail.
 - d (Facoltativo) Scegliere se inviare le notifiche a tutti gli amministratori dell'organizzazione oppure a indirizzi e-mail specifici.
 - e (Facoltativo) Se si sceglie di inviare le notifiche a indirizzi e-mail specifici, immettere gli indirizzi e-mail separandoli con una virgola.
- 6 Fare clic su **Salva**.

Test delle impostazioni SMTP

Dopo aver modificato le impostazioni e-mail per l'organizzazione, è possibile testare le impostazioni SMTP.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 In **Impostazioni**, fare clic su **E-mail**.

Vengono visualizzate le impostazioni e-mail per l'organizzazione.
- 3 Fare clic su **Test**.
- 4 Immettere un indirizzo e-mail di destinazione e la password del server SMTP per provare le impostazioni SMTP, quindi fare clic sul pulsante **Test**.

Modifica delle impostazioni del dominio per le macchine virtuali dell'organizzazione

È possibile impostare un dominio Windows predefinito a cui è possibile aggiungere le macchine virtuali create nell'organizzazione. Le macchine virtuali possono sempre essere aggiunte a un dominio per il quale dispongono di credenziali, indipendentemente dal fatto che venga specificato o meno un dominio predefinito.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 In **Impostazioni**, fare clic su **Personalizzazione guest**.
- 3 Selezionare questa opzione per abilitare l'aggiunta al dominio per le macchine virtuali dell'organizzazione.
- 4 Inserire il nome del dominio, il nome utente e la password.
Le credenziali immesse si riferiscono a un utente di dominio standard, non a un amministratore di dominio.
- 5 (Facoltativo) Immettere l'unità organizzativa dell'account.
- 6 Fare clic su **Salva**.

Utilizzo di più siti

La funzionalità Multisito di VMware Cloud Director consente ai provider di servizi o ai tenant di più installazioni di VMware Cloud Director distribuite geograficamente (gruppi di server), di gestire e monitorare tali installazioni e le relative organizzazioni come singole entità.

Il portale tenant di VMware Cloud Director consente agli **amministratori delle organizzazioni** di associare le organizzazioni a siti.

Per ulteriori informazioni sulle associazioni dei siti, vedere la *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*.

Configurazione e gestione di distribuzioni multisito

Dopo che un **amministratore di sistema** ha associato due siti, gli **amministratori dell'organizzazione** di qualsiasi sito membro possono iniziare ad associare le proprie organizzazioni.

Per creare un'associazione tra due organizzazioni (chiamate Org-A e Org-B in questo esempio), è necessario essere **amministratore dell'organizzazione** di entrambe le organizzazioni. In questo modo, è possibile accedere a ciascuna organizzazione, recuperare i dati dell'associazione locale e inviare i dati recuperati all'altra organizzazione.

Importante Il processo di associazione di due organizzazioni può essere scomposto in modo logico in due operazioni di associazione complementari. La prima operazione (in questo esempio) consente di associare Org-A nel Sito-A a Org-B nel Sito-B. Successivamente, sarà necessario associare Org-B nel Sito-B a Org-A nel Sito-A. L'associazione non sarà completa finché non verranno completate entrambe le operazioni di associazione.

Prerequisiti

- I siti occupati dalle organizzazioni devono essere associati.

- È necessario essere un **amministratore di sistema** di entrambi i siti o un **amministratore dell'organizzazione** di entrambe le organizzazioni.

Procedura

- 1 Accedere al portale tenant VMware Cloud Director di Org-A nel Sito-A per recuperare i rispettivi dati dell'associazione locale.
 - a Fare clic su **Amministrazione**.
 - b In **Impostazioni**, fare clic su **Multisito**.
 - c Per scaricare i dati in formato XML, fare clic su **Esporta dati associazione locale**.
I dati vengono salvati in un file nella cartella dei download del browser.
- 2 Accedere al portale tenant VMware Cloud Director di Org-B nel Sito-B per inviare i dati dell'associazione locale da Org-A nel Sito-A.
 - a Fare clic su **Amministrazione**.
 - b In **Impostazioni**, fare clic su **Multisito**.
 - c Fare clic su **Crea nuova associazione organizzazione**.
Inviare i dati dell'associazione scaricati nel [Passaggio 1](#) a Org-B facendo clic sulla freccia di caricamento sotto la casella di testo **Nuovo XML associazione** e selezionando i dati dell'associazione locale scaricati nel [Passaggio 1](#).
 - d Fare clic su **Avanti** per verificare e inviare i dati.
Il sistema associa Org-A nel Sito-A a Org-B nel Sito-B.
 - e Fare clic su **Fine** per visualizzare l'organizzazione associata.
 - f Per visualizzare i dettagli dell'organizzazione associata o per eliminare l'associazione, fare clic sulla scheda **Nome organizzazione**.
- 3 Completare l'associazione ripetendo il passaggio 1 e il passaggio 2 per recuperare i dati dell'associazione locale da Org-B e inviarli a Org-A.

Informazioni generali sui lease

La creazione di un'organizzazione implica la specifica dei lease. I lease forniscono un livello di controllo sulle risorse di storage e di calcolo di un'organizzazione specificando l'intervallo di tempo massimo per l'esecuzione delle vApp e per l'archiviazione delle vApp e dei modelli di vApp.

L'obiettivo di un lease di runtime consiste nell'impedire l'utilizzo delle risorse di calcolo alle vApp inattive. Se ad esempio un utente avvia una vApp e va in ferie senza arrestarla, la vApp continua a utilizzare le risorse.

Un lease di runtime inizia quando un utente avvia una vApp. Allo scadere del lease di runtime, VMware Cloud Director arresta la vApp.

L'obiettivo di un lease dello storage è impedire l'utilizzo delle risorse dello storage a vApp e modelli di vApp non utilizzati. Un lease dello storage di una vApp inizia quando un utente arresta la vApp. I lease dello storage non influiscono sulle vApp in esecuzione. Un lease dello storage di un modello di vApp inizia quando un utente aggiunge il modello di vApp a una vApp o a un'area di lavoro, oppure lo scarica, lo copia o lo sposta.

Allo scadere di un lease dello storage, VMware Cloud Director contrassegna la vApp o il modello di vApp come scaduto oppure elimina la vApp o il modello di vApp in base ai criteri dell'organizzazione impostati.

Modifica dei criteri di lease delle vApp e dei modelli di vApp nell'organizzazione

È possibile rivedere e modificare i criteri predefiniti impostati dall'amministratore di sistema durante la creazione dell'organizzazione.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

2 In **Impostazioni** fare clic su **Criteri**.

È possibile visualizzare i criteri predefiniti impostati dall'**amministratore di sistema**.

3 Fare clic su **Modifica**.

4 Modificare i lease delle vApp.

I lease delle vApp forniscono un livello di controllo sulle risorse di storage e di calcolo di un'organizzazione specificando la quantità di tempo massima per cui le vApp possono essere eseguite e archiviate. È anche possibile specificare cosa accade alle vApp quando il loro lease dello storage scade.

- a Per definire per quanto tempo è possibile eseguire le vApp prima che vengano arrestate automaticamente, immettere il lease di runtime massimo.
- b Selezionare un'azione di scadenza del runtime, ad esempio lo spegnimento o la sospensione.
- c Per definire per quanto tempo le vApp arrestate rimangono disponibili prima di venire eliminate automaticamente, immettere il tempo massimo di lease dello storage.
- d Selezionare un'azione di pulizia dello storage, ad esempio l'eliminazione definitiva delle vApp o lo spostamento delle vApp negli elementi scaduti.

5 Modificare i lease dei modelli delle vApp.

I lease dei modelli delle vApp forniscono un livello di controllo sulle risorse di storage e di calcolo di un'organizzazione specificando la quantità di tempo massima per cui i modelli delle vApp possono essere archiviati. È anche possibile specificare cosa accade ai modelli delle vApp quando il loro lease dello storage scade.

- a Per definire per quanto tempo i modelli delle vApp rimangono disponibili prima di venire eliminati automaticamente, immettere il lease dello storage massimo.
- b Selezionare un'azione di pulizia dell'archivio, ad esempio l'eliminazione definitiva dei modelli delle vApp o lo spostamento dei modelli delle vApp negli elementi scaduti.

6 Fare clic su **OK**.

Modifica dei criteri di password e account utente nell'organizzazione

È possibile rivedere e modificare i criteri di account utente e password predefiniti impostati dall'amministratore di sistema durante la creazione dell'organizzazione.

I criteri di account utente e password definiscono il comportamento di VMware Cloud Director quando un utente immette una password non valida.

Prerequisiti

Questa operazione richiede i diritti inclusi nel ruolo **Amministratore organizzazione** predefinito o un set di diritti equivalente.

Procedura

1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.

2 In **Impostazioni** fare clic su **Criteri**.

È possibile visualizzare i criteri predefiniti impostati dall'**amministratore di sistema**.

3 Fare clic su **Modifica**.

4 Abilitare il blocco di un account utente dopo diversi tentativi di login non validi.

5 Immettere il numero di tentativi di accesso non validi prima che l'account venga bloccato.

6 Inserire l'intervallo di tempo in minuti per cui l'utente con account bloccato non può accedere nuovamente.

7 Fare clic su **OK**.

Creazione di un dashboard di avvisi

È possibile creare notifiche che vengono visualizzate nella parte superiore delle pagine dell'interfaccia utente in Tenant Portal. I messaggi possono essere visualizzati per gli utenti di un'organizzazione o gli utenti di tutte le organizzazioni.

Una volta creati gli avvisi, non è possibile modificarli.

Prerequisiti

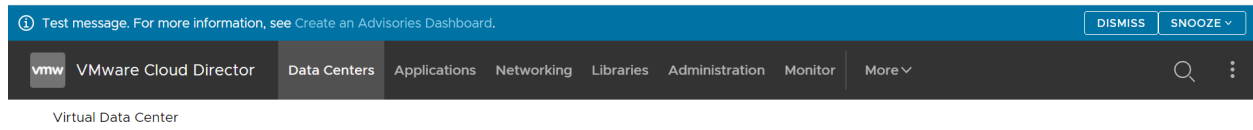
Verificare di aver effettuato l'accesso come **amministratore di sistema**.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Impostazioni**, selezionare **Avvisi** e fare clic su **Nuovo**.
- 3 Nella casella Descrizione, aggiungere il testo della notifica.
È possibile utilizzare il Markdown di base per aggiungere collegamenti alle notifiche.
- 4 Selezionare la priorità del messaggio.
I messaggi con priorità diverse vengono visualizzati con colori diversi. Le notifiche vengono visualizzate nell'ordine di priorità. Non è possibile ignorare o posticipare gli avvisi obbligatori.
- 5 Selezionare il periodo per il quale si desidera che la notifica venga visualizzata nell'interfaccia utente.
È possibile visualizzare tutti gli avvisi nella scheda **Avvisi**, tuttavia vengono visualizzati nel gruppo di utenti selezionato solo durante il periodo selezionato.
- 6 Fare clic su **OK**.

Risultati

La notifica viene visualizzata sopra la barra di navigazione superiore del portale selezionato.



Operazioni successive

È possibile eliminare la notifica selezionando il relativo pulsante di opzione e facendo clic su **Elimina**. Gli avvisi vengono visualizzati nella scheda **Avvisi** anche dopo la loro scadenza. Per rimuoverli dall'elenco, è necessario eliminarli.

Utilizzo della Libreria dei servizi

17

Gli elementi della Libreria dei servizi in VMware Cloud Director sono flussi di lavoro di vRealize Orchestrator che estendono le funzionalità di gestione cloud e consentono agli amministratori di provider o tenant di monitorare e gestire servizi diversi.

Questo capitolo include i seguenti argomenti:

- [Ricerca di un servizio](#)
- [Esecuzione di un servizio](#)

Ricerca di un servizio

La pagina **Libreria dei servizi** nel portale tenant di VMware Cloud Director elenca la serie di flussi di lavoro vRealize Orchestrator importati in VMware Cloud Director e pubblicati nella propria organizzazione.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Libreria dei servizi nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore fare clic su **Librerie** e in **Servizi** selezionare **Libreria dei servizi**.

L'elenco degli elementi dei servizi viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ciascuna scheda mostra il nome del servizio e un tag che corrisponde alla categoria di servizio in cui è stato importato vRealize Orchestrator.

- 2 Nella casella di testo **Cerca** nella parte superiore della pagina, immettere la prima parola del nome del servizio o del nome della categoria a cui il servizio appartiene.

a Scegliere se si desidera cercare tra i nomi del servizio o tra le categorie.

I risultati della ricerca vengono elencati in una visualizzazione a scheda di dodici elementi per pagina, ordinati alfabeticamente per nome.

Esecuzione di un servizio

È possibile eseguire un servizio dalla pagina Libreria dei servizi nel portale tenant di VMware Cloud Director.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Libreria dei servizi nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore fare clic su **Librerie** e in **Servizi** selezionare **Libreria dei servizi**.

L'elenco degli elementi dei servizi viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ciascuna scheda mostra il nome del servizio e un tag che corrisponde alla categoria di servizio in cui è stato importato vRealize Orchestrator.

- 2 Cercare il servizio che si desidera eseguire.

- 3 Fare clic su **Esegui** nella scheda del servizio.

Verrà aperta una nuova finestra di dialogo. È necessario immettere i valori per i parametri di input necessari del servizio.

- 4 Fare clic su **Fine** per confermare l'esecuzione del servizio.

Operazioni successive

È possibile monitorare lo stato dell'esecuzione nella visualizzazione **Task recenti**. Per ulteriori informazioni, vedere [Visualizzazione dei task](#).

A partire da VMware Cloud Director 10.2, i provider di servizi possono utilizzare l'API di VMware Cloud Director per creare estensioni che forniscano funzionalità di VMware Cloud Director aggiuntive ai tenant. Se sono state ricevute le autorizzazioni di accesso da un provider di servizi, è possibile gestire le entità definite e condividerle con gli altri tenant.

I provider di servizi possono creare RDE (Runtime Defined Entity) consentendo alle estensioni di archiviare e manipolare le informazioni specifiche dell'estensione in VMware Cloud Director. Ad esempio, un'estensione Kubernetes può archiviare nelle RDE informazioni sui cluster Kubernetes che gestisce. L'estensione può quindi fornire API di estensione per la gestione di tali cluster utilizzando le informazioni delle RDE.

Accesso alle entità definite

Due meccanismi complementari controllano l'accesso alle RDE.

- Diritti: quando un provider di servizi crea un tipo di RDE, crea un bundle di diritti per tale tipo. Un provider di servizi deve assegnare uno o più dei cinque diritti specifici dei tipi: **Visualizza: TYPE**, **Modifica: TYPE**, **Controllo completo: TYPE**, **Vista amministratore: TYPE** e **Controllo completo amministratore: TYPE**.

I diritti **Visualizza: TYPE**, **Modifica: TYPE** e **Controllo completo: TYPE** sono validi solo in combinazione con una voce ACL.

- Elenco di controllo di accesso (ACL): la tabella ACL contiene voci che definiscono l'accesso degli utenti a entità specifiche nel sistema. Fornisce un livello di controllo aggiuntivo sulle entità. Ad esempio, mentre un diritto **Modifica: TYPE** specifica che un utente può modificare le entità a cui può accedere, la tabella ACL definisce le entità a cui l'utente può accedere.

Tabella 18-1. Diritti e voci ACL per le operazioni RDE

Operazione entità	Opzione	Descrizione
Lettura	Diritto Vista amministratore: TYPE	Gli utenti con questo diritto possono visualizzare tutte le RDE di questo tipo all'interno di un'organizzazione.
	Diritto Visualizza: TYPE e voce ACL >= Visualizza	Gli utenti con questo diritto e un ACL di livello lettura possono visualizzare le RDE di questo tipo.
Modifica	Diritto Controllo completo amministratore: TYPE	Gli utenti con questo diritto possono creare, visualizzare, modificare ed eliminare le RDE di questo tipo in tutte le organizzazioni.
	Diritto Modifica: TYPE e voce ACL >= Modifica	Gli utenti con questo diritto e un ACL di livello modifica possono creare, visualizzare e modificare le RDE di questo tipo.
Elimina	Diritto Controllo completo amministratore: TYPE	Gli utenti con questo diritto possono creare, visualizzare, modificare ed eliminare le RDE di questo tipo in tutte le organizzazioni.
	Diritto Controllo completo: TYPE e voce ACL = Controllo completo	Gli utenti con questo diritto e una ACL di livello controllo completo possono creare, visualizzare, modificare ed eliminare le RDE di questo tipo.

Condivisione delle entità definite con un altro utente

Se un **amministratore di sistema** pubblica il bundle dei diritti per un tipo di entità definito e concede all'utente l'accesso `ReadWrite` o `FullControl` oppure l'utente è proprietario dell'entità definita, l'utente può condividere l'accesso a tali entità con altri utenti.

- 1 Assegnare il diritto **Visualizza: TYPE**, **Modifica: TYPE** o **Controllo completo: TYPE** dal bundle ai ruoli utente che si desidera dispongano del livello di accesso specifico all'entità definita.

Nota È necessario aver effettuato l'accesso come **amministratore di sistema** o **amministratore dell'organizzazione** per assegnare diritti.

Ad esempio, se si desidera che gli utenti con il ruolo **tkg_viewer** possano visualizzare i cluster Tanzu Kubernetes all'interno dell'organizzazione, è necessario aggiungere il diritto **Visualizza: Cluster guest Tanzu Kubernetes** al ruolo. Se si desidera che gli utenti con il ruolo **tkg_author** possano creare, visualizzare e modificare i cluster Tanzu Kubernetes all'interno di questa organizzazione, aggiungere il diritto **Modifica: Cluster guest Tanzu Kubernetes** a tale ruolo. Se si desidera che gli utenti con il ruolo **tkg_admin** possano creare, visualizzare, modificare ed eliminare i cluster Tanzu Kubernetes all'interno di questa organizzazione, aggiungere il diritto **Controllo completo: Cluster guest Tanzu Kubernetes** al ruolo.

- 2 Concedere all'utente specifico un elenco di controllo di accesso (ACL) effettuando la seguente chiamata REST API.

```
POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
[version]:[UUID]/accessControls
{
  "grantType" : "MembershipAccessControlGrant",
  "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
  "memberId" : "urn:vcloud:user:[User_ID]"
}
```

Access_level deve essere `ReadOnly`, `ReadWrite` o `FullControl`. *User_ID* deve essere l'ID dell'utente a cui si desidera concedere l'accesso all'entità definita.

È necessario disporre di accesso `ReadWrite` o `FullControl` a un'entità per concedere l'accesso ACL a tale entità.

Gli utenti con il ruolo **tkg_viewer**, descritto nell'esempio, non possono concedere l'accesso ACL. Gli utenti con il ruolo **tkg_author** o **tkg_admin** possono condividere l'accesso a un'entità VMWARE:TKGCLUSTER con gli utenti che dispongono del ruolo **tkg_viewer**, **tkg_author** o **tkg_admin** concedendo loro l'accesso ACL mediante la richiesta API.

Gli utenti con il diritto **Controllo completo amministratore: Cluster guest Tanzu Kubernetes** possono concedere l'accesso ACL a qualsiasi entità VMWARE:TKGCLUSTER.

È inoltre possibile utilizzare le chiamate REST API per revocare l'accesso o per visualizzare chi ha accesso all'entità. Consultare la documentazione della REST API di VMware Cloud Director su code.vmware.com.

Modifica del proprietario di un'entità definita

Il proprietario di un'entità definita o un utente con il diritto **Controllo completo amministratore: TYPE** può trasferire la proprietà a un altro utente aggiornando il modello dell'entità definita e modificando il campo del proprietario con l'ID del nuovo proprietario.

Questo capitolo include i seguenti argomenti:

- [Utilizzo delle definizioni entità personalizzata](#)

Utilizzo delle definizioni entità personalizzata

Le definizioni delle entità personalizzate in VMware Cloud Director sono tipi di oggetto associati ai tipi di oggetto vRealize Orchestrator. Gli utenti all'interno di un'organizzazione VMware Cloud Director possono possedere, gestire e modificare questi tipi in base alle proprie esigenze.

Mediante l'esecuzione di servizi, gli utenti delle organizzazioni possono creare istanze di entità personalizzate e applicare azioni sulle istanze degli oggetti.

Ricerca di un'entità personalizzata

È possibile cercare le entità personalizzate che sono state pubblicate nella propria organizzazione.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Nella casella di testo di **ricerca** nella parte superiore della pagina, immettere una parola o un carattere del nome dell'entità da trovare.

I risultati della ricerca vengono elencati in una visualizzazione a scheda di dodici elementi per pagina, ordinati alfabeticamente per nome.

Modifica di una definizione entità personalizzata

È possibile modificare il nome e la descrizione di un'entità personalizzata. Non è possibile cambiare il tipo di entità o il tipo di oggetto vRealize Orchestrator a cui l'entità è associata, poiché si tratta di proprietà predefinite dell'entità personalizzata. Se si desidera modificare una delle proprietà predefinite, è necessario eliminare la definizione dell'entità personalizzate e ricrearla.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Nella scheda dell'entità personalizzata selezionata, selezionare **Azioni > Modifica**.

Verrà aperta una nuova finestra di dialogo.

- 3 Modificare il nome o la descrizione della definizione dell'entità personalizzata.

- 4 Fare clic su **OK** per confermare la modifica.

Aggiunta di una definizione entità personalizzata

È possibile creare un'entità personalizzata e mapparla a un tipo di oggetto vRealize Orchestrator esistente.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Per aggiungere una nuova entità personalizzata, fare clic su **Nuovo**.

Verrà aperta una nuova finestra di dialogo.

- 3 Seguire i passaggi della procedura guidata **Definizione entità personalizzata**.

Passaggio	
Nome e descrizione	Immettere un nome e una descrizione facoltativa per la nuova entità. Immettere un nome per il tipo di entità, ad esempio <code>sshHost</code> .
vRO	Dal menu a discesa, selezionare il vRealize Orchestrator che verrà utilizzato per mappare la definizione dell'entità personalizzata.
Nota Se si dispone di più di un server vRealize Orchestrator, è necessario creare una definizione di entità personalizzata per ognuno di essi separatamente.	

Passaggio

Tipo	Fare clic sull'icona Visualizza elenco per visualizzare i tipi di oggetti di vRealize Orchestrator disponibili raggruppati per plug-in. Ad esempio, SSH > Host . Se si conosce il nome del tipo, è possibile immetterlo direttamente nella casella di testo. Ad esempio <code>SSH:Host</code> .
Verifica	Riesaminare i dettagli specificati e fare clic su Fine per completare la creazione.

Risultati

La nuova definizione di entità personalizzata compare nella visualizzazione scheda.

Istanze entità personalizzata

Eseguendo un flusso di lavoro vRealize Orchestrator con un parametro di input di un tipo di oggetto già definito come definizione di un'entità personalizzata in VMware Cloud Director, è possibile mostrare il parametro di output come un'istanza di un'entità personalizzata.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.


Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Nella scheda dell'entità personalizzata selezionata, fare clic su **Istanze**.

Vengono mostrate le istanze disponibili in una visualizzazione a griglia.

- 3 Fare clic sulla barra di elenco () a sinistra di ciascuna entità per visualizzare i flussi di lavoro associati.

Facendo clic su un flusso di lavoro ne avvia un'esecuzione di un flusso di lavoro che accetta l'istanza dell'entità come parametro di input.

Associazione di un'azione a un'entità personalizzata

Associando un'azione a una definizione di entità personalizzata, è possibile eseguire una serie di flussi di lavoro di vRealize Orchestrator nelle istanze di un'entità personalizzata particolare.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Nella scheda dell'entità personalizzata selezionata, selezionare **Azioni > Associa azione**.

Verrà aperta una nuova finestra di dialogo.

- 3 Seguire i passaggi della procedura guidata **Associa entità personalizzato a flusso di lavoro VRO**.

Passaggio	Dettagli
Seleziona flusso di lavoro VRO	Selezionare uno dei flussi di lavoro elencati. Questi sono i flussi di lavoro disponibili nella pagina Libreria dei servizi .
Seleziona parametro di input flusso di lavoro	Selezionare un parametro di input disponibile dall'elenco. Associare il tipo del flusso di lavoro di vRealize Orchestrator al tipo di definizione dell'entità personalizzata.
Verifica associazione	Riesaminare i dettagli specificati e fare clic su Fine per completare l'associazione.

Esempio

Ad esempio, se si dispone di un'entità personalizzata di tipo `SSH:Host`, è possibile associarla al flusso di lavoro `Add a Root Folder to SSH Host` selezionando il parametro di input `sshHost`, che corrisponde al tipo dell'entità personalizzata.

Annullamento dell'associazione di un'azione a una definizione entità personalizzata

È possibile rimuovere un flusso di lavoro di vRealize Orchestrator dall'elenco delle azioni associate.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Nella scheda dell'entità personalizzata selezionata, selezionare **Azioni > Annulla associazione azione**.

Verrà aperta una nuova finestra di dialogo.

- 3 Selezionare il flusso di lavoro da rimuovere e fare clic su **Annulla associazione azione**.

Il flusso di lavoro vRealize Orchestrator non è più associato all'entità personalizzata.

Pubblicazione di un'entità personalizzata

È necessario pubblicare un'entità personalizzata in modo che gli utenti di altri tenant o provider di servizi possano eseguire i flussi di lavoro utilizzando le istanze di entità personalizzate come parametri di input.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Nella scheda dell'entità personalizzata selezionata, selezionare **Azioni > Pubblica**.

Verrà aperta una nuova finestra di dialogo.

- 3 Scegliere se pubblicare la definizione dell'entità personalizzata nei provider di servizi, in tutti i tenant, oppure solo nei tenant selezionati.

- 4 Fare clic su **Salva** per confermare la modifica.

La definizione dell'entità personalizzata diventa disponibile per le parti selezionate.

Eliminazione di un'entità personalizzata

È possibile eliminare una definizione di entità personalizzata se questa non è più in uso, se è stata configurata in modo errato o se si desidera mappare il tipo di vRealize Orchestrator a un'entità personalizzata diversa.

Prerequisiti

Questa operazione richiede l'inclusione dei diritti di Entità personalizzata nel ruolo utente predefinito.

Procedura

- 1 Nella barra di navigazione superiore, fare clic su **Librerie** e in **Servizi** selezionare **Definizioni entità personalizzate**.

L'elenco di entità personalizzate viene visualizzato in una vista a schede di dodici elementi per pagina, ordinati alfabeticamente in base al nome. Ogni scheda mostra il nome dell'entità personalizzata, il tipo di vRealize Orchestrator a cui è mappata l'entità, il tipo di entità e una descrizione, se disponibile.

- 2 Nella scheda dell'entità personalizzata selezionata, scegliere **Azioni > Elimina**.
- 3 Confermare l'eliminazione.

L'entità personalizzata viene rimossa dalla visualizzazione della scheda.