

Guida del portale di amministrazione del provider di servizi di VMware Cloud Director

9 APR 2020

VMware Cloud Director 10.1

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 © 2018-2020 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

Sommario

1	Guida del portale di amministrazione del provider di servizi di VMware Cloud Director™	9
2	Guida introduttiva a VMware Cloud Director Service Provider Admin Portal	10
	Panoramica dell'amministrazione di VMware Cloud Director	10
	Accedere a VMware Cloud Director Service Provider Admin Portal	14
	Visualizzazione dei task	14
	Interruzione di un'attività in corso	15
	Visualizzazione di eventi	15
	Impostazione delle preferenze utente	16
	Limiti di lunghezza di nomi e descrizioni	17
3	Gestione delle risorse vSphere	18
	Aggiunta di risorse di vCenter Server e NSX	19
	Collegamento di un'istanza di vCenter Server da sola o insieme a un'istanza di NSX Manager	19
	Individuazione e adozione delle vApp	24
	Assegnazione della chiave di licenza NSX in vCenter Server	26
	Registrazione di un'istanza di NSX-T Manager	26
	Accesso ai componenti di vSphere tramite proxy di VMware Cloud Director	27
	Aggiunta di un proxy per l'accesso alle risorse vCenter Server sottostanti	27
	Gestione dei certificati e dei CRL del proxy	29
	Aggiunta di risorse cloud	29
	Virtual data center del provider	29
	Creazione di un virtual data center del provider	30
	Reti esterne	33
	Pool di reti	36
	Visualizzazione delle istanze di vCenter Server	40
	Modifica delle impostazioni di vCenter Server	41
	Abilitazione o disabilitazione di un'istanza di vCenter Server	42
	Riconnessione di un'istanza di vCenter Server	42
	Aggiornamento di un'istanza di vCenter Server	43
	Aggiornamento dei criteri di storage di un'istanza di vCenter Server	43
	Annullamento della registrazione di un'istanza di vCenter Server	43
	Modifica delle impostazioni di NSX Manager	44
	Modifica delle impostazioni di NSX-T Manager	45
	Eliminazione di un'istanza di NSX-T Manager	45
	Configurazione e gestione di distribuzioni multisito	46

Elenchi di risorse multisito 48

4 Gestione dei virtual data center del provider 50

- Abilitazione o disabilitazione di un virtual data center del provider 50
- Eliminazione di un virtual data center del provider 51
- Modifica delle impostazioni generali di un virtual data center del provider 51
- Unione di virtual data center del provider 52
- Visualizzazione dei virtual data center dell'organizzazione di un virtual data center del provider 52
- Visualizzazione degli archivi dati in un virtual data center del provider 53
- Visualizzazione delle reti esterne in un virtual data center del provider 54
- Gestione dei criteri di storage della macchina virtuale in un virtual data center del provider 55
 - Abilitazione della crittografia della macchina virtuale nei criteri di storage di un virtual data center del provider 55
 - Aggiunta di un criterio di storage della macchina virtuale in un virtual data center del provider 57
 - Abilitazione o disabilitazione di un criterio di storage della macchina virtuale in un virtual data center del provider 57
 - Eliminazione di un criterio di storage della macchina virtuale da un virtual data center del provider 58
 - Modifica dei metadati per un criterio di storage della macchina virtuale in un virtual data center del provider 58
 - Abilitazione dell'impostazione delle operazioni di I/O al secondo 59
- Gestione dei pool di risorse in un virtual data center del provider 60
 - Aggiunta di un pool di risorse a un virtual data center del provider 60
 - Abilitazione o disabilitazione di un pool di risorse in un virtual data center del provider 61
 - Scollegamento di un pool di risorse da un virtual data center del provider 61
- Modifica dei metadati per un virtual data center del provider 62

5 Gestione delle organizzazioni 63

- Informazioni generali sui lease 63
- Creazione di un'organizzazione 64
- Abilitazione o disabilitazione di un'organizzazione 64
- Eliminazione di un'organizzazione 65
- Configurazione dei cataloghi di un'organizzazione 65
- Configurazione dei criteri di un'organizzazione 66
- Migra storage tenant 67

6 Gestione dei virtual data center dell'organizzazione 69

- Informazioni sui modelli di allocazione 69
 - Utilizzo consigliato per i modelli di allocazione 72
 - Modello di allocazione Flex 73
 - Modello di allocazione del pool di allocazioni 75

Modello di allocazione Pay-As-You-Go	77
Modello di allocazione del pool di prenotazioni	77
Informazioni sul dimensionamento delle macchine virtuali e sui criteri di posizionamento delle macchine virtuali	78
Attributi dei criteri di dimensionamento della macchina virtuale	84
Creazione di un criterio di posizionamento della macchina virtuale	86
Aggiunta di un criterio di posizionamento della macchina virtuale a un VDC dell'organizzazione	87
Eliminazione di un criterio di posizionamento della macchina virtuale	88
Creazione di un criterio di dimensionamento della macchina virtuale	88
Aggiunta di un criterio di dimensionamento della macchina virtuale a un VDC dell'organizzazione	89
Modifica di un criterio di dimensionamento della macchina virtuale	90
Eliminazione di un criterio di dimensionamento della macchina virtuale	90
Creazione di un virtual data center dell'organizzazione	91
Abilitazione o disabilitazione di un virtual data center dell'organizzazione	94
Eliminazione di un virtual data center dell'organizzazione	94
Modifica del nome e della descrizione del virtual data center dell'organizzazione	95
Modifica delle impostazioni del modello di allocazione di un virtual data center dell'organizzazione	95
Modifica delle impostazioni di storage di un virtual data center dell'organizzazione	96
Abilitazione della crittografia della macchina virtuale nei criteri di storage di un virtual data center dell'organizzazione	96
Modifica delle impostazioni di provisioning delle macchine virtuali di un virtual data center dell'organizzazione	97
Aggiunta di un criterio di storage della macchina virtuale a un virtual data center dell'organizzazione	98
Modifica del criterio di storage predefinito in un virtual data center dell'organizzazione	98
Modifica del limite di un criterio di storage in un virtual data center dell'organizzazione	99
Modifica dei metadati per un criterio di storage della macchina virtuale in un virtual data center dell'organizzazione	99
Abilitazione o disabilitazione di un criterio di storage in un virtual data center dell'organizzazione	100
Eliminazione di un criterio di storage da un virtual data center dell'organizzazione	101
Modifica delle impostazioni di rete di un virtual data center dell'organizzazione	101
Configurazione di servizi di rete inter-VDC	103
Modifica dei metadati per un virtual data center dell'organizzazione	104
Visualizzazione dei pool di risorse di un virtual data center dell'organizzazione	105
Gestione del firewall distribuito in un virtual data center dell'organizzazione	105
Abilitazione del firewall distribuito in un virtual data center dell'organizzazione	105
Aggiunta di una regola del firewall distribuito	106
Modifica di una regola del firewall distribuito	109
Raggruppamento di oggetti personalizzato	110
Utilizzo dei gruppi di sicurezza	113

Utilizzo dei tag di sicurezza 117

7 Gestione dei gateway edge NSX Data Center for vSphere 122

Utilizzo dei cluster edge di NSX Data Center for vSphere 122

Aggiunta di un gateway edge NSX Data Center for vSphere 124

Configurazione dei servizi gateway edge NSX Data Center for vSphere 126

Gestione di un firewall del gateway edge NSX Data Center for vSphere 127

Gestione del DHCP del gateway edge NSX Data Center for vSphere 131

Aggiunta di una regola SNAT o DNAT 136

Configurazione avanzata del routing 139

Bilanciamento del carico 148

Protezione dell'accesso mediante l'utilizzo di reti VPN 162

Gestione dei certificati SSL 189

Raggruppamento di oggetti personalizzato 196

Visualizzazione dell'utilizzo delle reti e delle allocazioni IP in un gateway edge 200

Modifica delle proprietà dei gateway edge 200

Abilitazione o disabilitazione del routing distribuito in un gateway edge 201

Modifica delle impostazioni di reti esterne e di gateway edge 201

Modifica delle impostazioni generali di un gateway edge 202

Modifica del gateway predefinito di un gateway edge 202

Modifica delle impostazioni IP di un gateway edge 203

Modifica dei pool di IP sottoallocati in un gateway edge 203

Modifica dei limiti di classificazione in un gateway edge 204

Ridistribuzione di un gateway edge 204

Eliminazione di un gateway edge 205

Statistiche e registri per un gateway edge 205

Visualizzazione delle statistiche 205

Abilitazione della registrazione 206

Abilitazione dell'accesso a un gateway edge dalla riga di comando SSH 207

8 Gestione dei gateway edge NSX-T Data Center 209

Reti esterne dedicate 209

Aggiunta di un gateway edge NSX-T Data Center 210

Aggiunta di un gruppo di firewall a un gateway edge NSX-T 211

Aggiunta di una regola del firewall del gateway edge NSX-T 212

Aggiunta di una regola SNAT o DNAT a un gateway edge NSX-T 213

Configurazione di un servizio di inoltro DNS su un gateway edge NSX-T 215

Modifica delle allocazioni IP di un gateway edge NSX-T 216

Allocazione IP rapida 216

Creazione di profili delle porte dell'applicazione personalizzata 217

VPN basata su criteri IPsec per i gateway edge NSX-T Data Center 218

Configurazione della VPN IPSec basata sul criterio NSX-T	219
Personalizzazione del profilo di sicurezza di un tunnel VPN IPSec	220
Configurazione dei servizi della rete esterna dedicata	221
Gestione della comunicazione della route	221
Configurazione delle impostazioni generali BGP	222
Creazione di un elenco di prefissi IP	224
Aggiunta di un router adiacente BGP	225
9 Gestione di istanze di vCenter Server dedicate	227
Abilitazione dell'accesso tenant di un'istanza di vCenter Server collegata	229
Pubblicazione di un'istanza di vCenter Server dedicata	230
10 Gestione degli amministratori di sistema e dei ruoli	232
Gestione di diritti e ruoli	232
Ruoli predefiniti e relativi diritti	234
Diritti dell'amministratore di sistema	236
Diritti nei ruoli tenant globali predefiniti	245
Gestione dei bundle diritti	251
Gestione dei ruoli tenant globali	254
Gestione dei ruoli di Provider	258
Gestione di utenti e gruppi di Provider	260
Gestione degli utenti di Provider	260
Gestione di gruppi di Provider	263
11 Gestione delle impostazioni di sistema	266
Modifica delle impostazioni generali del sistema	266
Impostazioni generali del sistema	267
Configurazione delle impostazioni e-mail di sistema	269
Modifica della licenza di VMware Cloud Director	270
Configurazione delle impostazioni di sincronizzazione del catalogo	270
Configurazione e monitoraggio delle attività bloccanti e delle notifiche	271
Configurazione di un broker AMQP	271
Configurazione delle impostazioni relative alle attività bloccanti	272
Monitoraggio delle attività bloccanti	273
Configurazione di indirizzi pubblici	273
Gestione dei provider di identità	275
Gestione di connessioni LDAP	276
Configurazione del sistema per l'utilizzo di un provider di identità SAML	279
Gestione dei plug-in	281
Caricamento di un plug-in	281
Abilitazione o disabilitazione di un plug-in	282

Eliminazione di un plug-in	282
Pubblica o Annulla la pubblicazione di un plug-in da un'organizzazione	282
Personalizzazione dei portali di VMware Cloud Director	283
Configurazione dei criteri della password	285
Configurazione dei servizi di vSphere	285
12 Monitoraggio di VMware Cloud Director	287
VMware Cloud Director e report sui costi	287
Visualizzazione delle informazioni di utilizzo per un virtual data center del provider	288
13 Gestione dei servizi	289
Integrazione di vRealize Orchestrator con VMware Cloud Director	289
Registrazione di un'istanza di vRealize Orchestrator con VMware Cloud Director	290
Creazione di una categoria di servizi	291
Modifica di una categoria di servizi	291
Importazione di un servizio	292
Ricerca di un servizio	292
Esecuzione di un servizio	293
Modifica di una categoria di servizio	294
Annullamento della registrazione di un servizio	294
Pubblicazione di un servizio	295
14 Gestione delle entità personalizzate	296
Ricerca di un'entità personalizzata	296
Modifica di una definizione entità personalizzata	297
Aggiunta di una definizione entità personalizzata	297
Istanze entità personalizzata	298
Associazione di un'azione a un'entità personalizzata	299
Annullamento dell'associazione di un'azione da un'entità personalizzata	299
Pubblicazione di un'entità personalizzata	300
Eliminazione di un'entità personalizzata	300

Guida del portale di amministrazione del provider di servizi di VMware Cloud Director™

1

Nella *Guida di VMware Cloud Director Service Provider Admin Portal* viene spiegato come utilizzare Service Provider Admin Portal. Utilizzare service provider admin portal per gestire e monitorare organizzazioni, diritti, ruoli, utenti e gruppi nel cloud. È inoltre possibile creare e gestire reti di virtual data center dell'organizzazione con supporto NSX-T.

Destinatari della guida

Questa guida è pensata per gli amministratori dei provider dei servizi che desiderano utilizzare le funzionalità fornite in VMware Cloud Director Service Provider Admin Portal.

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

Guida introduttiva a VMware Cloud Director Service Provider Admin Portal

2

VMware Cloud Director Service Provider Admin Portal è un'interfaccia dedicata per gli amministratori dei provider di servizi.

Questo capitolo include i seguenti argomenti:

- [Panoramica dell'amministrazione di VMware Cloud Director](#)
- [Accedere a VMware Cloud Director Service Provider Admin Portal](#)
- [Visualizzazione dei task](#)
- [Interruzione di un'attività in corso](#)
- [Visualizzazione di eventi](#)
- [Impostazione delle preferenze utente](#)
- [Limiti di lunghezza di nomi e descrizioni](#)

Panoramica dell'amministrazione di VMware Cloud Director

Con VMware VMware Cloud Director è possibile creare cloud multi-tenant sicuri eseguendo il pooling delle risorse dell'infrastruttura virtuale in virtual data center ed esponendole agli utenti tramite portali basati su Web e interfacce programmatiche come un servizio completamente automatizzato, basato su catalogo.

La *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director* fornisce informazioni sull'aggiunta di risorse al sistema, sulla creazione e sul provisioning delle organizzazioni, sulla gestione delle risorse e delle organizzazioni, nonché sul monitoraggio del sistema.

Risorse di vSphere e NSX

VMware Cloud Director utilizza le risorse di vSphere per fornire CPU e memoria per l'esecuzione delle macchine virtuali. Gli archivi dati di vSphere forniscono inoltre spazio di storage per i file delle macchine virtuali e per gli altri file necessari per le operazioni relative alle macchine virtuali. VMware Cloud Director utilizza anche commutatori distribuiti di vSphere, gruppi di porte di vSphere e NSX Data Center for vSphere per supportare servizi di rete delle macchine virtuali.

VMware Cloud Director può inoltre utilizzare le risorse da NSX-T Data Center. Per informazioni sulla registrazione di un'istanza di NSX-T Manager con il cloud, vedere *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director* oppure *Guida alla programmazione dell'API di VMware Cloud Director*

È possibile utilizzare le risorse di vSphere e NSX sottostanti per creare risorse cloud.

A partire dalla versione 9.7, VMware Cloud Director può fungere da server proxy HTTP, con cui è possibile abilitare le organizzazioni per accedere all'ambiente vSphere sottostante.

Risorse Cloud

Le risorse cloud rappresentano un'astrazione delle risorse di vSphere sottostanti corrispondenti e forniscono le risorse di calcolo e memoria per le macchine virtuali VMware Cloud Director e le vApp. Una vApp è un sistema virtuale che contiene una o più macchine virtuali, insieme ai parametri che definiscono i dettagli operativi. Le risorse Cloud consentono inoltre di accedere allo spazio di storage e alla connettività di rete.

Le risorse cloud includono virtual data center di provider e organizzazioni, reti esterne, reti di virtual data center dell'organizzazione e pool di reti.

Per poter aggiungere risorse cloud a VMware Cloud Director, è necessario aggiungere risorse di vSphere.

Istanze e proxy di vCenter Server dedicati

Un'istanza di vCenter Server dedicata è una risorsa cloud che incapsula un'intera installazione di vCenter Server. Un'istanza di vCenter Server dedicata include uno o più proxy che sono punti di accesso a diversi componenti dell'ambiente vSphere sottostante. Il provider può creare e abilitare istanze e proxy di vCenter Server dedicati. Il provider può pubblicare un'istanza di vCenter Server dedicata nei tenant.

Per creare e gestire le istanze e i proxy di vCenter Server dedicati, è possibile utilizzare il Service Provider Admin Portal o vCloud OpenAPI. Consultare [Capitolo 9 Gestione di istanze di vCenter Server dedicate](#) e *Guida introduttiva a VMware Cloud Director OpenAPI* in <https://code.vmware.com>.

Virtual data center del provider

Un virtual data center del provider combina le risorse di calcolo e di memoria di un singolo pool di risorse vCenter Server con le risorse di storage di uno o più archivi dati disponibili per tale pool di risorse.

Un virtual data center del provider può utilizzare risorse di rete provenienti da un'istanza di NSX Manager associata all'istanza di vCenter Server o da un'istanza di NSX-T Manager registrata nel cloud.

È possibile creare più virtual data center del provider per gli utenti che si trovano in posizioni geografiche o in business unit diverse o per gli utenti con requisiti di prestazioni differenti.

Virtual data center dell'organizzazione

Un virtual data center dell'organizzazione fornisce le risorse a un'organizzazione e viene partizionato da un virtual data center del provider. I virtual data center dell'organizzazione forniscono un ambiente in cui è possibile archiviare, distribuire e utilizzare i sistemi virtuali. Forniscono inoltre lo spazio di storage per media virtuali, quali dischi floppy e CD ROM.

Una singola organizzazione può disporre di più virtual data center dell'organizzazione.

Servizi di rete di VMware Cloud Director

VMware Cloud Director supporta tre tipi di rete.

- Reti esterne
- Reti del virtual data center dell'organizzazione
- Reti di vApp

Alcune reti di virtual data center dell'organizzazione e tutte le reti di vApp sono supportate dai pool di reti.

Reti esterne

Una rete esterna è una rete logica differenziata, basata su un gruppo di porte di vSphere. Le reti di virtual data center dell'organizzazione possono connettersi alle reti esterne per fornire connettività Internet alle macchine virtuali in una vApp.

A partire dalla versione 9.5, VMware Cloud Director supporta le reti esterne IPv6. Una rete esterna IPv6 supporta le subnet IPv4 e IPv6 e una rete esterna IPv4 supporta le subnet IPv4 e IPv6.

Per impostazione predefinita, le reti esterne possono essere create e gestite solo dagli **amministratori di sistema**.

Reti del virtual data center dell'organizzazione

La rete del virtual data center di un'organizzazione appartiene al 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. Per la connettività esterna, è possibile connettere la rete di virtual data center dell'organizzazione a una rete esterna. È anche possibile creare una rete di virtual data center dell'organizzazione isolata che sia interna all'organizzazione.

VMware Cloud Director 9.5 include il supporto di IPv6 per le reti di virtual data center dell'organizzazione dirette e instradate.

A partire da VMware Cloud Director 9.5, gli **amministratori di sistema** possono creare reti di virtual data center isolate supportate da un commutatore logico NSX-T. Gli **amministratori dell'organizzazione** possono creare reti di virtual data center isolate supportate da pool di reti.

VMware Cloud Director 9.5 include anche servizi di rete inter-VDC tramite la configurazione di reti estese nei gruppi di virtual data center.

Per impostazione predefinita, solo gli **amministratori di sistema** possono creare reti dirette e inter-VDC. Gli **amministratori di sistema** e gli **amministratori dell'organizzazione** possono gestire le reti di virtual data center dell'organizzazione, sebbene esistano alcuni limiti per le operazioni che gli **amministratori dell'organizzazione** possono eseguire.

Reti di vApp

Una rete di vApp appartiene a una vApp e consente la comunicazione tra le macchine virtuali della vApp. Per abilitare la comunicazione di una vApp con le altre vApp dell'organizzazione, è possibile connettere la rete di vApp a una rete di virtual data center dell'organizzazione. Se la rete di virtual data center dell'organizzazione è connessa a una rete esterna, la vApp può comunicare con le vApp di altre organizzazioni. Le reti di vApp sono supportate da pool di reti.

La maggior parte degli utenti con accesso a una vApp può creare e gestire le proprie reti di vApp. Per informazioni sull'utilizzo delle reti in una vApp, vedere *VMware Cloud Director Tenant Portal Guide*.

Pool di reti

Un pool di reti è un gruppo di reti indifferenziate disponibili per l'utilizzo nel virtual data center di un'organizzazione. Un pool di reti è supportato dalle risorse di rete di vSphere quali ID VLAN o gruppi di porte. VMware Cloud Director utilizza i pool di reti per creare reti di virtual data center dell'organizzazione interne e instradate da NAT e tutte le reti di vApp. Il traffico di rete su ogni rete di un pool è isolato al livello del layer 2 rispetto alle altre reti.

Ogni virtual data center dell'organizzazione in VMware Cloud Director può disporre di un pool di reti. Più virtual data center dell'organizzazione possono condividere un pool di reti. Il pool di reti di un virtual data center dell'organizzazione fornisce le reti create per soddisfare la quota di rete di un virtual data center dell'organizzazione.

I pool di reti possono essere creati e gestiti solo dagli **amministratori di sistema**.

Organizzazioni

VMware Cloud Director supporta la multi-tenancy mediante le 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. Le attività degli **amministratori dell'organizzazione** sono descritte in *VMware Cloud Director Tenant Portal Guide*.

Utenti e gruppi

Un'organizzazione può contenere un numero arbitrario di utenti e gruppi. Gli **amministratori dell'organizzazione** possono creare utenti e importare utenti e gruppi da un servizio di directory come LDAP. L'**amministratore di sistema** gestisce il set di diritti disponibili per ogni organizzazione. L'**amministratore di sistema** può creare e pubblicare i ruoli tenant globali in una o più organizzazioni. L'**amministratore dell'organizzazione** può creare ruoli locali nelle proprie organizzazioni.

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. Un **amministratore di sistema** può consentire a un'organizzazione la pubblicazione di un catalogo per renderlo disponibile per le altre organizzazioni. Gli **amministratori delle organizzazioni** possono quindi scegliere quali voci di catalogo rendere disponibili per i propri utenti.

Accedere a VMware Cloud Director Service Provider Admin Portal

È possibile accedere a VMware Cloud Director Service Provider Admin Portal utilizzando un browser Web.

Prerequisiti

È necessario disporre dei diritti di amministratore di sistema per accedere a VMware Cloud Director Service Provider Admin Portal.

Procedura

- 1 In un browser digitare l'URL del Service Provider Admin Portal del sito VMware Cloud Director e premere Invio.

Ad esempio, digitare **`https://vcloud.example.com/provider`**.

- 2 Accedere con il nome utente dell'amministratore di sistema e la password.


Visualizzazione dei task

Da Service Provider Admin Portal è possibile visualizzare i task recenti e il relativo stato.

La visualizzazione dei task è utile per visualizzare un riepilogo generale dello stato dei task nel portale dell'amministratore del provider di servizi. La vista indica la data di esecuzione dei task e se sono stati completati correttamente. Questo strumento può essere un valido punto di partenza per risolvere eventuali problemi nell'ambiente in uso.

Le descrizioni popup di colore blu e rosso sopra l'icona Task indicano, rispettivamente, il numero di task eseguiti e di quelli non riusciti.

Procedura

- ◆ Dal menu in alto a destra, selezionare l'icona Task ()

Risultati

Verrà visualizzato un elenco dei task recenti insieme all'ora di esecuzione e allo stato del task.

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 su **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**.

Limiti di lunghezza di nomi e descrizioni

Attenersi alle linee guida seguenti quando si immettono valori in VMware Cloud Director.

I valori stringa per l'attributo `name` e gli elementi `Description` e `ComputerName` hanno limitazioni di lunghezza che dipendono dall'oggetto a cui sono allegati.

Tabella 2-1. Limiti di lunghezza delle proprietà degli oggetti

Oggetto	Proprietà	Lunghezza massima in caratteri
Catalog	name	128
Catalog	Description	256
EdgeGateway	name	35
Media	name	128
Media	Description	256
VApp	name	128
VApp	Description	256
VAppTemplate	name	128
VAppTemplate	Description	256
Vdc	name	128
Vdc	Description	256
Vm	name	128
Vm	ComputerName	15 su Windows, 63 su tutte le altre piattaforme
Vm	Description	256

Gestione delle risorse vSphere

3

VMware Cloud Director deriva le proprie risorse da un'infrastruttura virtuale vSphere sottostante. Dopo aver registrato le risorse di vSphere in VMware Cloud Director, è possibile allocarle in modo che possano essere utilizzate dalle organizzazioni nell'installazione di vSphere.

VMware Cloud Director utilizza uno o più ambienti vCenter Server per eseguire il backup dei virtual data center. A partire dalla versione 9.7, VMware Cloud Director può anche utilizzare un ambiente vCenter Server per incapsulare un SDDC con uno o più proxy. È possibile abilitare i tenant per l'utilizzo di questi proxy come punti di accesso all'ambiente vSphere sottostante da VMware Cloud Director con i rispettivi account VMware Cloud Director.

Per poter utilizzare un'istanza di vCenter Server in VMware Cloud Director, è necessario collegare questa istanza di vCenter Server.

Quando si crea un virtual data center del provider supportato da un'istanza di vCenter Server collegata, questa istanza di vCenter Server viene visualizzata come pubblicata nel provider di servizi e denominata anche con ambito provider. Per informazioni sulla creazione di un virtual data center del provider, vedere [Creazione di un virtual data center del provider](#).

Quando si crea un SDDC che incapsula un'istanza di vCenter Server collegata, il vCenter Server viene dedicato a un tenant. Questa istanza di vCenter Server viene visualizzata come pubblicata in un tenant, detta anche ambito tenant. Per informazioni sulla creazione di un SDDC, vedere [Capitolo 9 Gestione di istanze di vCenter Server dedicate](#).

Nota Per impostazione predefinita, con un'istanza di vCenter Server collegata, è possibile creare un VDC del provider o un'istanza di vCenter Server dedicata. Se è stato creato un VDC del provider supportato da un'istanza di vCenter Server, non è possibile utilizzare questa istanza di vCenter Server per creare un'istanza di vCenter Server dedicata e viceversa.

Gestione di SSL centralizzata

A partire dalla versione 10.1, VMware Cloud Director sta passando a in un'area di storage centralizzata con supporto del tenant per la gestione dei certificati. In questo modo, VMware Cloud Director centralizza tutti i certificati in un'unica posizione per consentire agli **amministratori di sistema** e agli **amministratori dell'organizzazione** di visualizzare, controllare e gestire tutti i certificati utilizzati dai vari componenti nel sistema. È possibile utilizzare l'API di VMware Cloud Director per aggiungere, aggiornare o rimuovere certificati dalla nuova area di storage con supporto del tenant. Vedere *Riferimento dello schema dell'API di VMware Cloud Director*.

Quando si aggiunge o si modifica una nuova istanza di vCenter Server, di NSX Manager o di NSX-T Manager, l'interfaccia utente di VMware Cloud Director esegue il probe dell'endpoint per tutti i certificati che presenta. VMware Cloud Director aggiunge a un'area di storage di certificati centralizzata qualsiasi certificato che si decide di considerare attendibile.

Questo capitolo include i seguenti argomenti:

- Aggiunta di risorse di vCenter Server e NSX
- Accesso ai componenti di vSphere tramite proxy di VMware Cloud Director
- Aggiunta di risorse cloud
- Visualizzazione delle istanze di vCenter Server
- Modifica delle impostazioni di vCenter Server
- Abilitazione o disabilitazione di un'istanza di vCenter Server
- Riconnesione di un'istanza di vCenter Server
- Aggiornamento di un'istanza di vCenter Server
- Aggiornamento dei criteri di storage di un'istanza di vCenter Server
- Annullamento della registrazione di un'istanza di vCenter Server
- Modifica delle impostazioni di NSX Manager
- Modifica delle impostazioni di NSX-T Manager
- Eliminazione di un'istanza di NSX-T Manager
- Configurazione e gestione di distribuzioni multisito
- Elenchi di risorse multisito

Aggiunta di risorse di vCenter Server e NSX

VMware Cloud Director utilizza le risorse di vSphere per fornire CPU, memoria e storage per l'esecuzione delle macchine virtuali. A partire dalla versione 9.7, VMware Cloud Director può inoltre fungere da server HTTP tra i tenant e l'ambiente vSphere sottostante.

Per informazioni sui requisiti di sistema di VMware Cloud Director e le versioni supportate di vCenter Server e ESXi, vedere *Matrici di interoperabilità dei prodotti VMware* in http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Collegamento di un'istanza di vCenter Server da sola o insieme a un'istanza di NSX Manager

È possibile collegare un'istanza di vCenter Server in modo che le sue risorse siano disponibili per l'utilizzo in VMware Cloud Director. È possibile collegare un'istanza di vCenter Server solo insieme alla relativa istanza di NSX Manager associata. Per le istanze di vCenter Server dedicate o per quelle associate a un'istanza di NSX-T Manager, è possibile collegare soltanto un'istanza di vCenter Server.

VMware Cloud Director può utilizzare un'istanza di vCenter Server con l'istanza di NSX Manager associata o con un'istanza di NSX-T Manager.

Se si desidera che VMware Cloud Director utilizzi questa istanza di vCenter Server con l'istanza di NSX Manager associata, è necessario collegare le istanze di vCenter Server e NSX Manager insieme.

Se si desidera che VMware Cloud Director utilizzi questa istanza di vCenter Server con un'istanza di NSX-T Manager, è necessario collegare l'istanza di vCenter Server da sola. Dopo aver collegato l'istanza di vCenter Server da sola, è necessario eseguire la procedura [Registrazione di un'istanza di NSX-T Manager](#).

Nota Dopo aver collegato un'istanza di vCenter Server da sola, non sarà possibile aggiungere in un secondo momento l'istanza di NSX Manager associata. È possibile annullare la registrazione e collegare nuovamente l'istanza di vCenter Server insieme all'istanza di NSX Manager associata.

È possibile collegare un'istanza di vCenter Server a qualsiasi sito dell'ambiente di VMware Cloud Director.

È possibile collegare un'istanza di vCenter Server accessibile direttamente o collegare un'istanza di vCenter Server presente dietro un proxy. Tramite vCloud OpenAPI, è possibile utilizzare configurazioni proxy all'interno di VMware Cloud Director per creare una connessione con proxy tra un'istanza di VMware Cloud Director e l'istanza di vCenter Server aggiunta a tale istanza. In questo modo, le istanze di VMware Cloud Director e vCenter Server possono esistere in posizioni o siti differenti.

Per collegare un'istanza di vCenter Server presente dietro un proxy, è necessario innanzitutto dichiarare una configurazione del proxy. È quindi necessario collegare un'istanza di vCenter Server e configurare VMware Cloud Director per l'utilizzo della configurazione del proxy durante l'accesso all'istanza di vCenter Server. È inoltre possibile collegare una soluzione di NSX Data Center for vSphere tramite un proxy. VMware Cloud Director non supporta le configurazioni del proxy per NSX-T Data Center. Non sono necessarie configurazioni SSL o del proxy aggiuntive per il Platform Services Controller in cui è registrata l'istanza di vCenter Server.

Prerequisiti

- Se VMware Cloud Director è stato configurato per verificare i certificati SSO di vCenter e vSphere, assicurarsi di aver caricato i certificati di vCenter Server in VMware Cloud Director. Per informazioni sulle impostazioni di sistema generali, vedere [Modifica delle impostazioni generali del sistema](#).

- Se VMware Cloud Director è stato configurato per verificare i certificati di NSX Manager, assicurarsi di aver caricato i certificati di NSX Manager in VMware Cloud Director. Per informazioni sulle impostazioni di sistema generali, vedere [Modifica delle impostazioni generali del sistema](#).

Procedura

1 Aggiunta dell'istanza di vCenter Server

Per aggiungere un'istanza di vCenter Server, immettere i dettagli di accesso di vCenter Server.

2 (Facoltativo) Aggiunta dell'istanza di NSX Manager associata

Se si desidera che VMware Cloud Director utilizzi questa istanza di vCenter Server con l'istanza di NSX Manager associata, è necessario aggiungere i dettagli di accesso di NSX Manager.

Aggiunta dell'istanza di vCenter Server

Per aggiungere un'istanza di vCenter Server, immettere i dettagli di accesso di vCenter Server.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel riquadro a sinistra, fare clic su **Istanze di vCenter Server** e quindi su **Aggiungi**.
- 3 Se è presente una distribuzione multisito di VMware Cloud Director, dal menu a discesa **Sito**, selezionare il sito a cui si desidera aggiungere questa istanza di vCenter Server e fare clic su **Avanti**.
- 4 Immettere un nome e, facoltativamente, una descrizione per l'istanza di vCenter Server in VMware Cloud Director.
- 5 Immettere l'URL dell'istanza di vCenter Server.

Se si utilizza la porta predefinita, è possibile ignorare il numero della porta. Se si utilizza una porta personalizzata, includere il numero della porta.

Ad esempio, `https://FQDN_or_IP_address:<custom_port_number>`.
- 6 Immettere il nome utente e la password dell'account dell'**amministratore** di vCenter Server.
- 7 (Facoltativo) Per disabilitare l'istanza di vCenter Server dopo la registrazione, disattivare l'opzione **Abilitata**.

8 Configurare l'URL del client Web di vCenter Server.

Opzione	Descrizione
Utilizza Servizi vSphere per specificare l'URL	Per utilizzare questa opzione, è necessario utilizzare l'API di vCloud per configurare VMware Cloud Director in modo che utilizzi il servizio di ricerca vSphere.
URL vSphere Web Client	Per utilizzare questa opzione, è necessario immettere l'URL di vSphere Web Client, ad esempio <code>https://example.vmware.com/vsphere-client</code> .

9 Fare clic su **Avanti**.

- 10 Se l'endpoint non dispone di un certificato attendibile, nella finestra **Certificato di attendibilità** confermare se si considera attendibile l'endpoint.

In un ambiente multisito, se si accede a un sito di vCloud Director 10.0 o si tenta di registrare un'istanza di vCenter Server in un sito di vCloud Director 10.0, VMware Cloud Director non aggiungerà l'endpoint all'area di storage dei certificati centralizzata.

- Per aggiungere l'endpoint all'area di storage dei certificati centralizzata e continuare, fare clic su **Considera attendibile**.
- Se l'endpoint non è attendibile, fare clic su **Annulla** e ripetere dal [Passaggio 5](#) al [Passaggio 9](#) con un endpoint attendibile.

- 11 (Facoltativo) Ignorare l'aggiunta dell'istanza di NSX Manager associata all'istanza di vCenter Server disattivando l'impostazione **Configura impostazioni** e fare clic su **Avanti**.

Se si desidera che VMware Cloud Director utilizzi questa istanza di vCenter Server con un'istanza di NSX-T Manager, è necessario aggiungere l'istanza di vCenter Server da sola.

Nota Non è possibile aggiungere l'istanza di NSX Manager associata in un secondo momento. È possibile annullare la registrazione e collegare nuovamente l'istanza di vCenter Server insieme all'istanza di NSX Manager associata.

- 12 Se si desidera aggiungere un'istanza di vCenter Server dedicata a un tenant che non verrà utilizzata come VDC del provider, attivare l'opzione **Abilita accesso tenant**.

Dopo aver aggiunto l'istanza di vCenter Server in VMware Cloud Director, le informazioni relative al tenant vengono visualizzate nella visualizzazione dei dettagli dell'istanza.

- 13 Se si desidera che VMware Cloud Director generi proxy predefiniti per l'istanza di vCenter Server e i servizi SSO, attivare l'opzione **Genera proxy**.

Dopo aver aggiunto l'istanza di vCenter Server in VMware Cloud Director, i proxy vengono visualizzati nella scheda **Proxy** in **Risorse vSphere**.

- 14 Nella pagina **Pronto per il completamento**, controllare i dettagli della registrazione e fare clic su **Fine**.

(Facoltativo) Aggiunta dell'istanza di NSX Manager associata

Se si desidera che VMware Cloud Director utilizzi questa istanza di vCenter Server con l'istanza di NSX Manager associata, è necessario aggiungere i dettagli di accesso di NSX Manager.

Procedura

- 1 Nella pagina **NSX-V Manager**, lasciare attivata l'opzione **Configura impostazioni**.
- 2 Immettere l'URL dell'istanza di NSX Manager.

Se si utilizza la porta predefinita, è possibile ignorare il numero della porta. Se si utilizza una porta personalizzata, includere il numero della porta.

Ad esempio, **https://FQDN_or_IP_address:<custom_port_number>**.

- 3 Immettere il nome utente e la password dell'account dell'amministratore di NSX.
- 4 (Facoltativo) Per abilitare la rete inter-VDC per i virtual data center supportati da questa istanza di vCenter Server, attivare l'opzione **Networking VDC incrociato**, quindi specificare le proprietà di distribuzione della macchina virtuale di controllo e un nome per l'ambito del provider di rete.

Le proprietà di distribuzione della macchina virtuale di controllo vengono utilizzate per la distribuzione di un'appliance nell'istanza di NSX Manager per i componenti del networking inter-VDC, come un router universale.

Opzione	Descrizione
Ambito del provider di rete	Corrisponde al dominio di errore di rete nelle topologie di rete dei gruppi di data center. ad esempio boston-fault1 . Per informazioni sulla gestione dei gruppi inter-VDC, vedere <i>VMware Cloud Director Tenant Portal Guide</i> .
Percorso pool di risorse	Il percorso gerarchico di un pool di risorse specifico nell'istanza di vCenter Server, a partire dal cluster <i>Cluster/Resource_Pool_Parent/Target_Resource</i> . Ad esempio TestbedCluster1/mgmt-rp . In alternativa, è possibile immettere l'ID di riferimento oggetto gestito del pool di risorse. Ad esempio, resgroup-1476 .
Nome archivio dati	Nome dell'archivio dati che ospiterà i file dell'appliance, ad esempio shared-disk-1 .
Interfaccia di gestione	Il nome della rete in vCenter Server o gruppo di porte utilizzato per l'interfaccia di gestione HA DLR, ad esempio TestbedPG1 .

- 5 Fare clic su **Avanti**.

- 6 Se l'endpoint non dispone di un certificato attendibile, nella finestra **Certificato di attendibilità** confermare se si considera attendibile l'endpoint.

In un ambiente multisito, se si accede a un sito di vCloud Director 10.0 o si tenta di registrare un'istanza di NSX Manager in un sito di vCloud Director 10.0, VMware Cloud Director non aggiungerà l'endpoint all'area di storage dei certificati centralizzata.

- Per aggiungere l'endpoint all'area di storage dei certificati centralizzata e continuare, fare clic su **Considera attendibile**.
- Se l'endpoint non è attendibile, fare clic su **Annulla** e ripetere dal [Passaggio 2](#) al [Passaggio 4](#) con un endpoint attendibile.

- 7 Abilitare o disabilitare le impostazioni di configurazione dell'accesso.

- 8 Nella pagina **Pronto per il completamento**, controllare i dettagli della registrazione e fare clic su **Fine**.

Operazioni successive

- [Assegnazione della chiave di licenza NSX in vCenter Server](#).
- [Creazione di un virtual data center del provider](#).

Individuazione e adozione delle vApp

Nella configurazione predefinita, un VDC dell'organizzazione individua le macchine virtuali create in qualsiasi pool di risorse di vCenter Server che supporta il VDC. Il sistema costruisce una vApp semplificata, di proprietà dell'amministratore di sistema, in cui includere le singole macchine virtuali individuate. Dopo che l'amministratore di sistema avrà concesso l'accesso a una vApp individuata, è possibile fare riferimento alla macchina virtuale in essa contenuta quando si compone o si ricompone una vApp o quando si modifica la vApp per adottarla e importarla.

Le vApp individuate contengono una sola macchina virtuale e sono soggette a diversi vincoli non applicabili alle vApp create in VMware Cloud Director. Anche se non vengono adottate, le vApp possono essere utili come origine delle macchine virtuali da utilizzare durante la composizione o la ricomposizione di una vApp.

A ogni vApp individuata viene assegnato un nome derivato dal nome della macchina virtuale vCenter che la contiene e un prefisso specificato dall'amministratore dell'organizzazione.

Se si desidera rilevare ulteriori vApp, un amministratore del sistema può utilizzare l'API di VMware Cloud Director per creare VDC dell'organizzazione che adottino i pool di risorse specificati disponibili in un VDC del provider. Le macchine virtuali vCenter di questi pool di risorse adottati vengono visualizzate nel nuovo VDC come vApp individuate e sono candidate per l'adozione.

Nota Le macchine virtuali con unità disco rigido IDE vengono rilevate solo se sono in stato disattivato.

Se una o più macchine virtuali vCenter non vengono individuate da VMware Cloud Director, è possibile cercare i possibili motivi tramite debug dell'individuazione delle macchine virtuali di vCenter Server. Per ulteriori informazioni, vedere *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

Abilitazione dell'individuazione delle macchine virtuali

Per impostazione predefinita, l'individuazione delle macchine virtuali è abilitata. Per disabilitarla, è necessario che un amministratore di sistema deselezioni la casella di controllo **Individuazione macchine virtuali abilitata** nella scheda **Impostazioni di sistema > Generale**. Un amministratore dell'organizzazione può utilizzare l'API di VMware Cloud Director per disabilitare il rilevamento delle macchine virtuali per singoli VDC o per tutti i VDC di un'organizzazione.

Uso di una macchina virtuale da una vApp individuata

Dopo aver ricevuto dall'amministratore di sistema le autorizzazioni per accedere a una vApp individuata, è possibile utilizzarne la macchina virtuale nello stesso modo in cui si utilizza una macchina virtuale contenuta in qualsiasi altra vApp o modello di vApp. È ad esempio possibile specificarla quando si crea una nuova vApp. È anche possibile clonare una vApp individuata o modificarne il nome, la descrizione e le impostazioni di lease senza attivare il processo di adozione.

Adozione di una vApp individuata

È possibile adottare una vApp individuata cambiandone la rete di vApp o aggiungendo una macchina virtuale alla vApp. Dopo aver adottato una vApp individuata, il sistema la importa e la gestisce come se fosse stata creata in VMware Cloud Director. Quando una vApp adottata viene recuperata con una richiesta API di vCloud, include un elemento denominato `autoNature`. Tale elemento ha il valore `false` se la vApp individuata è stata adottata o creata in VMware Cloud Director. Non è possibile ripristinare una vApp individuata da una vApp adottata.

Se si elimina o si sposta la macchina virtuale contenuta in una vApp individuata, il sistema rimuove anche la vApp contenitore. Questo comportamento non si applica alle vApp adottate.

La vApp creata per contenere una macchina virtuale vCenter individuata è simile a quella che viene creata quando si importa manualmente una macchina virtuale come vApp, ma è semplificata in un modo che potrebbe richiederne una modifica ai fini della distribuzione nel VDC. Potrebbe, ad esempio, essere necessario modificarne le proprietà di rete e di storage e apportare altre modifiche specifiche delle esigenze dell'organizzazione.

Nota L'adozione di una macchina virtuale non comporta il mantenimento delle impostazioni della prenotazione, del limite e delle condivisioni della macchina virtuale 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.

Assegnazione della chiave di licenza NSX in vCenter Server

Se è stata collegata un'istanza di vCenter Server insieme all'istanza di NSX Manager associata, è necessario utilizzare il client vSphere per assegnare una chiave di licenza per l'istanza di NSX Manager che supporta la rete di VMware Cloud Director.

Prerequisiti

Questa operazione può essere eseguita solo dagli amministratori di sistema.

Procedura

- 1 In un'istanza di vSphere Client connessa al sistema vCenter Server, selezionare **Home > Licenza**.
- 2 Per la visualizzazione del report, selezionare **Asset**.
- 3 Fare clic con il pulsante destro del mouse sull'asset NSX Manager e scegliere **Change license key**.
- 4 Selezionare **Assign a new license key**, quindi fare clic su **Enter Key**.
- 5 Immettere il codice di licenza, un'etichetta facoltativa per il codice, quindi fare clic su **OK**.
Utilizzare la chiave di licenza di NSX Manager ricevuta al momento dell'acquisto di VMware Cloud Director. È possibile utilizzare questa chiave di licenza in più istanze di vCenter Server.
- 6 Fare clic su **OK**.

Registrazione di un'istanza di NSX-T Manager

È possibile registrare un'istanza di NSX-T Manager in VMware Cloud Director, in modo che VMware Cloud Director ne possa utilizzare le risorse di rete. Un virtual data center del provider può utilizzare risorse di rete di NSX Data Center for vSphere o di NSX-T Data Center.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel riquadro a sinistra, fare clic su **NSX-T Manager** e quindi su **Aggiungi**.
- 3 Se è presente una distribuzione multisito di VMware Cloud Director, dal menu a discesa **Sito**, selezionare il sito a cui si desidera aggiungere questa istanza di NSX-T Manager e fare clic su **Avanti**.
- 4 Immettere un nome e, facoltativamente, una descrizione per l'istanza di NSX-T Manager in VMware Cloud Director.
- 5 Immettere l'URL dell'istanza di NSX-T Manager.
Ad esempio, **https://FQDN_or_IP_address**.
- 6 Immettere il nome utente e la password dell'account dell'**amministratore** di NSX-T Manager.
- 7 Fare clic su **Salva**.

Operazioni successive

Per informazioni sulla creazione di un virtual data center del provider supportato da NSX-T Data Center, vedere *Guida alla programmazione dell'API di VMware Cloud Director* all'indirizzo <https://code.vmware.com>.

Accesso ai componenti di vSphere tramite proxy di VMware Cloud Director

VMware Cloud Director può fungere da server proxy HTTP tra gli utenti di VMware Cloud Director e l'ambiente di vSphere sottostante.

Un proxy fornito da VMware Cloud Director è un punto di accesso a un componente di un data center, ad esempio un'istanza di vCenter Server, un host ESXi o un'istanza di NSX Manager. Gli utenti possono accedere all'interfaccia utente o all'API dei componenti con proxy utilizzando i loro account VMware Cloud Director. Abilitando e disabilitando un proxy fornito da VMware Cloud Director, è possibile consentire e interrompere l'accesso tenant tramite tale proxy.

I proxy forniti da VMware Cloud Director sono diversi dalle configurazioni del proxy all'interno di VMware Cloud Director. A differenza dei proxy forniti da VMware Cloud Director che hanno come ambito un tenant, le configurazioni del proxy all'interno di VMware Cloud Director si trovano a livello del provider e non è presente alcuna tenancy.

È possibile creare un proxy quando si collega un'istanza di vCenter Server a VMware Cloud Director o in un secondo momento. Se l'istanza di vCenter Server utilizza un'istanza di Platform Services Controller esterna, VMware Cloud Director crea anche un proxy per l'istanza di Platform Services Controller. Con i proxy principali e secondari, è possibile nascondere determinati proxy ai tenant oppure abilitare e disabilitare gruppi di proxy secondari tramite i loro proxy principali. Per ulteriori informazioni sulla creazione di un proxy dopo l'aggiunta di un'istanza di vCenter Server in VMware Cloud Director, vedere [Aggiunta di un proxy per l'accesso alle risorse vCenter Server sottostanti](#).

È possibile modificare, abilitare, disabilitare ed eliminare i proxy dalla scheda **Proxy in Risorse vSphere**.

Nota Quando si aggiunge un proxy a un'istanza di vCenter Server, è necessario caricare il certificato e l'identificazione personale, in modo che i tenant possano recuperare il certificato e l'identificazione personale se il componente con proxy utilizza certificati autofirmati.

Per visualizzare e gestire i certificati e gli elenchi di revoche dei certificati (CRL), vedere [Gestione dei certificati e dei CRL del proxy](#).

Aggiunta di un proxy per l'accesso alle risorse vCenter Server sottostanti

È possibile creare proxy forniti da VMware Cloud Director, che possono essere utilizzati dagli amministratori e dai tenant per accedere all'ambiente vSphere sottostante, come istanze di vCenter Server aggiunte a VMware Cloud Director.

Se si desidera generare automaticamente un proxy di vCenter Server con l'identificazione personale e i certificati recuperati, è possibile eseguire questa operazione nella griglia **Istanze di vCenter Server** o nella vista dei dettagli di vCenter Server. Se vCenter Server dispone di un Platform Services Controller esterno, questa opzione crea anche un proxy per l'endpoint SSO.

Questa procedura indica come creare manualmente un proxy per un'istanza di vCenter Server oppure un proxy per un host ESXi, un'istanza di Platform Services Controller esterna o un'istanza di NSX Manager.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.
- 3 Selezionare un'istanza di vCenter Server.
- 4 Nella pagina con informazioni dettagliate su vCenter Server, fare clic sulla scheda **Proxy**, quindi su **Nuovo**.
- 5 Immettere un nome per il proxy.
- 6 Selezionare il tipo di proxy, in base al componente di cui si desidera che VMware Cloud Director sia un proxy.

Non è possibile modificare questa impostazione dopo la creazione del proxy.

È possibile creare un solo proxy vCenter Server. Se è presente un proxy vCenter Server esistente e si desidera creare un nuovo proxy, il menu a discesa **Tipo** non include un'opzione vCenter Server.

- Se si desidera creare un proxy di vCenter Server, selezionare **vCenter** dal menu a discesa **Tipo** e continuare con il [Passaggio 10](#).
- Se si desidera creare un proxy per un host ESXi, NSX Manager o SSO, effettuare la selezione dal menu a discesa e continuare con il [Passaggio 7](#).

- 7 Immettere un nome, un host di destinazione e l'URL dell'interfaccia utente del nuovo proxy.
L'host di destinazione è il nome dell'host o l'indirizzo IP del componente per cui si desidera che VMware Cloud Director funga da proxy. L'URL dell'interfaccia utente del nuovo proxy è l'URL a cui l'interfaccia utente di VMware Cloud Director viene indirizzata quando il tenant apre il proxy.
- 8 Se si desidera che il proxy sia visibile ai tenant, attivare l'opzione **Tenant visibile**.
- 9 (Facoltativo) Fare clic su **Seleziona un proxy principale** e selezionare un proxy nell'elenco.
- 10 Fare clic su **Salva**.

Operazioni successive

[Gestione dei certificati e dei CRL del proxy.](#)

Gestione dei certificati e dei CRL del proxy

È possibile visualizzare, scaricare e caricare i certificati e gli elenchi di revoche dei certificati (CRL) del proxy.

Prerequisiti

Verificare di disporre di proxy forniti da VMware Cloud Director per almeno un'istanza di vCenter Server. Vedere [Accesso ai componenti di vSphere tramite proxy di VMware Cloud Director](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, fare clic su **Proxy** e selezionarne uno.
- 3 Fare clic su **Gestisci certificato**.
- 4 Caricare o scaricare il certificato e il CRL.
- 5 Fare clic su **Salva**.

Aggiunta di risorse cloud

Le risorse cloud rappresentano un'astrazione delle risorse vSphere sottostanti corrispondenti e forniscono le risorse di calcolo e memoria per le macchine virtuali di VMware Cloud Director e le vApp, nonché accesso allo spazio di storage e alla connettività di rete.

Le risorse cloud includono virtual data center di provider e organizzazioni, reti esterne, reti di virtual data center dell'organizzazione e pool di reti. Per poter aggiungere risorse cloud a VMware Cloud Director, è necessario aggiungere risorse di vSphere.

Per informazioni sulle reti di virtual data center dell'organizzazione, consultare [Capitolo 6 Gestione dei virtual data center dell'organizzazione](#).

Per informazioni sulle reti di virtual data center dell'organizzazione, vedere il capitolo *Gestione delle reti di virtual data center dell'organizzazione* in *VMware Cloud Director Tenant Portal Guide*.

VMware Cloud Director 9.7 include l'SDDC o l'istanza di vCenter Server dedicata come risorsa cloud che incapsula un'intera installazione di vCenter Server. Il provider può creare e abilitare un'istanza di vCenter Server dedicata, pubblicarla nei tenant, nonché creare e abilitare proxy in componenti diversi dell'ambiente di vSphere sottostante. Per creare, pubblicare nei tenant e gestire le istanze e i proxy dell'istanza di vCenter Server dedicata, è possibile utilizzare il Service Provider Admin Portal o vCloud OpenAPI. Consultare [Capitolo 9 Gestione di istanze di vCenter Server dedicate](#) o *Guida introduttiva a VMware Cloud Director OpenAPI* in <https://code.vmware.com>.

Virtual data center del provider

Un virtual data center (VDC) del provider unisce le risorse di calcolo e memoria dei pool di risorse di un vCenter Server alle risorse di storage di uno o più criteri di storage di una singola istanza

di vCenter Server. Per le risorse di rete, un VDC del provider può utilizzare NSX Data Center for vSphere oppure NSX-T Data Center.

- È possibile creare e gestire un VDC del provider supportato da un'istanza di vCenter Server collegata e dalla relativa istanza di NSX Manager associata utilizzando Service Provider Admin Portal o l'API di vCloud.
- È possibile creare e gestire un VDC del provider supportato da un'istanza di vCenter Server collegata e da un'istanza di NSX-T Manager utilizzando Service Provider Admin Portal o l'API di vCloud.

Un sistema VMware Cloud Director tipico include più VDC del provider configurati in modo da soddisfare i requisiti di vari livelli di servizio. Ciascun VDC del provider dispone di un pool di risorse primario. È possibile aggiungere e rimuovere pool di risorse non primari dall'istanza di vCenter Server di supporto. Non è possibile rimuovere il pool di risorse primario.

Creazione di un virtual data center del provider

Per rendere le risorse di calcolo, memoria e storage di vSphere disponibili per VMware Cloud Director, è necessario creare un virtual data center (VDC) del provider.

Prima che un'organizzazione possa iniziare la distribuzione di macchine virtuali o la creazione di cataloghi, l'**amministratore di sistema** deve creare un VDC del provider e i VDC dell'organizzazione che ne utilizzano le risorse. La relazione tra i VDC del provider e i VDC dell'organizzazione che supportano è una decisione amministrativa. La decisione può essere basata sull'ambito delle offerte di servizi, sulla capacità e sulla distribuzione geografica dell'infrastruttura di vSphere, nonché su altre considerazioni simili. Poiché un VDC del provider limita la capacità e i servizi di vSphere disponibili per i tenant, gli **amministratori di sistema** creano in genere VDC del provider che forniscono classi di servizio diverse in base alla misurazione di prestazioni, capacità e funzionalità. Il provisioning dei tenant può quindi essere eseguito mediante VDC dell'organizzazione che forniscono classi di servizio specifiche definite dalla configurazione del VDC del provider di supporto.

Prima di creare un VDC del provider, è consigliabile valutare il set di funzionalità di vSphere che si intende offrire ai tenant. Alcune di queste funzionalità possono essere implementate nel pool di risorse primario del VDC del provider. Altre potrebbero richiedere la creazione di pool di risorse aggiuntivi in base a cluster vSphere appositamente configurati e la loro aggiunta al VDC come descritto in [Aggiunta di un pool di risorse a un virtual data center del provider](#).

La gamma di versioni di ESXi installate negli host del cluster che supporta un pool di risorse determina il set di sistemi operativi guest e le versioni dell'hardware virtuale disponibili per le macchine virtuali distribuite nei VDC dell'organizzazione supportati dal VDC del provider.

Prerequisiti

- Accedere a Service Provider Admin Portal come **amministratore di sistema**.

- Verificare di aver creato il pool di risorse primarie di destinazione con capacità disponibile in un cluster configurato per l'utilizzo di DRS automatizzati. È possibile utilizzare un pool di risorse per un solo VDC del provider. Per creare un pool di risorse, è possibile utilizzare vSphere Client.

Se si intende utilizzare un pool di risorse che fa parte di un cluster che utilizza vSphere HA (High Availability), è necessario conoscere la modalità di calcolo delle dimensioni degli slot in vSphere HA. Per informazioni sulle dimensioni degli slot e sulla personalizzazione del comportamento di vSphere HA, vedere la documentazione *Disponibilità di vSphere*.

- Se si utilizza NSX Data Center for vSphere per le risorse di rete del VDC del provider:

- Verificare che l'istanza di vCenter Server che contiene il pool di risorse primario di destinazione sia collegata e disponga di una chiave di licenza NSX Data Center for vSphere.
- Impostare l'infrastruttura VXLAN in NSX Manager. Vedere la relativa *guida all'amministrazione di NSX*.

Se in questo VDC del provider si desidera utilizzare un pool di reti VXLAN personalizzato anziché il pool di reti VXLAN predefinito, creare il pool di reti ora. Vedere [Creazione di un pool di reti supportato da una zona di trasporto NSX Data Center for vSphere](#).

- Se si utilizza NSX-T Data Center per le risorse di rete del VDC del provider:
 - [Aggiunta di una rete esterna supportata da un router logico di livello 0 NSX-T Data Center](#)
 - [Creazione di un pool di reti supportato da una zona di trasporto NSX-T Data Center](#)

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider**.
- 3 Fare clic su **Nuovo**.
- 4 Se è presente una distribuzione multisito di VMware Cloud Director, dal menu a discesa **Sito**, selezionare il sito a cui si desidera aggiungere questa istanza di VDC del provider e fare clic su **Avanti**.

- 5 Immettere un nome e, facoltativamente, una descrizione per il VDC del provider.

È possibile utilizzare queste caselle di testo per indicare le funzionalità di vSphere disponibili per i VDC dell'organizzazione supportati dal VDC del provider, ad esempio **vSphere HA** o i **criteri di storage con il supporto delle operazioni di I/O al secondo**.

- 6 (Facoltativo) Per disabilitare il VDC del provider al momento della creazione, disattivare l'interruttore **Stato**.

Non è possibile utilizzare le risorse di elaborazione e storage di un VDC disabilitato per la creazione di VDC dell'organizzazione.

- 7 Fare clic su **Avanti**.

- 8 Per fornire pool di risorse per il VDC del provider, selezionare un'istanza di vCenter Server e fare clic su **Avanti**.

In questa pagina sono elencate le istanze di vCenter Server registrate in VMware Cloud Director. Fare clic su un'istanza di vCenter Server per visualizzare i pool di risorse disponibili.

- 9 Selezionare un pool di risorse che funga da pool di risorse primario per il VDC del provider.

È possibile utilizzare un pool di risorse per un VDC del provider. Quando si aggiunge un pool di risorse a un VDC del provider, il pool di risorse e la relativa catena principale non possono essere selezionati da altri VDC del provider.

- 10 Selezionare la versione dell'hardware virtuale più recente che si desidera venga supportata dal VDC del provider e fare clic su **Avanti**.

Il sistema determina la versione dell'hardware virtuale più recente supportata da tutti gli host del cluster che supporta il pool di risorse e la propone come predefinita nel menu a discesa **Versione hardware supportata più recente**. È possibile utilizzare la versione dell'hardware predefinita oppure selezionarne una precedente dal menu. La versione specificata diventa la versione dell'hardware virtuale più recente disponibile per una macchina virtuale distribuita in un VDC dell'organizzazione supportato dal VDC del provider. Se si seleziona una versione dell'hardware virtuale precedente, l'utilizzo di alcuni sistemi operativi guest potrebbe non essere supportato dalle macchine virtuali interessate. Dopo aver creato il VDC del provider con la versione dell'hardware selezionata, è possibile solo aggiornare la versione e non effettuarne il downgrade.

Nota La versione dell'hardware disponibile per il VDC del provider dipende dalla versione più recente disponibile dell'host ESXi nel cluster di destinazione. Se la versione hardware più recente supportata dell'host ESXi non è disponibile per la selezione, verificare in vSphere Client che la compatibilità predefinita per la creazione della macchina virtuale nel data center sia impostata su **Usa impostazione data center e versione host**. È inoltre possibile configurare l'impostazione di compatibilità predefinita sulla versione hardware più recente desiderata per il cluster.

La versione dell'hardware della macchina virtuale più recente supportata in VMware Cloud Director 10.1.0 è la versione 15. La versione hardware 15 è disponibile quando viene abilitata nell'istanza di vCenter Server a livello di cluster o di data center.

- 11 Selezionare uno o più criteri di storage per il VDC del provider e fare clic su **Avanti**.

Nell'elenco sono presenti tutti i criteri di storage di vSphere supportati dal pool di risorse selezionato.

12 Configurare il pool di reti per questo VDC del provider.

Ogni VDC del provider deve disporre di un pool di reti. È possibile fare in modo che il sistema ne crei uno con un ambito predefinito oppure utilizzare una VXLAN personalizzata in base a un pool di NSX Data Center for vSphere o Geneve specifico basato su una zona di trasporto di NSX-T Data Center.

Opzione	Descrizione
Creare un pool di reti VXLAN predefinito	Il sistema crea un pool di VXLAN per questo VDC del provider.
Selezionare un pool di reti VXLAN dall'elenco	È possibile selezionare un pool di reti da un elenco in modo da utilizzare un pool di VXLAN personalizzato basato su una zona di trasporto NSX specifica.
Selezionare un pool di reti Geneve e NSX-T Manager	È possibile selezionare un pool di reti in un elenco in modo da utilizzare un pool VXLAN personalizzato supportato da una zona di trasporto NSX-T Data Center.

13 Verificare le opzioni selezionate e fare clic su **Fine** per creare il VDC del provider.

Operazioni successive

È possibile aggiungere pool di risorse secondari per consentire al VDC del provider di fornire funzionalità specializzate, ad esempio cluster edge, gruppi di affinità e host con configurazioni speciali che potrebbero essere richieste da alcune organizzazioni. Vedere [Aggiunta di un pool di risorse a un virtual data center del provider](#).

Reti esterne

Una rete esterna di VMware Cloud Director fornisce un'interfaccia di uplink che connette reti e macchine virtuali del sistema a una rete esterna al sistema, ad esempio una VPN, una Intranet aziendale o Internet. Solo un **amministratore di sistema** può creare una rete esterna.

Se nel sistema sono registrate più istanze di vCenter Server, è possibile creare più reti esterne, ognuna supportata da un router logico di livello 0 o da una rete vSphere.

VMware Cloud Director supporta le reti esterne IPv4 e IPv6.

Nota L'intervallo di indirizzi IP definito quando si crea la rete esterna viene assegnato a un gateway edge o alle macchine virtuali che sono connesse direttamente a questa rete. Per questo motivo, gli indirizzi IP non devono essere utilizzati al di fuori di VMware Cloud Director.

Reti esterne supportate da reti vSphere

Le reti esterne possono essere supportate da una singola rete vSphere o da più reti vSphere.

- Reti esterne supportate da una singola istanza di vSphere.

Per fornire a ciascun cliente della rete esterna un set di indirizzi IP non sovrapposti nella rete vSphere, l'**amministratore di sistema** deve configurare manualmente gli intervalli IP nella VLAN sottostante.

- Reti esterne supportate da più reti vSphere.

Una rete esterna può essere supportata da più reti vSphere. Questo approccio può semplificare la gestione degli indirizzi IP in VMware Cloud Director. È possibile modificare le proprietà di una rete esterna per modificarne gli elementi sottostanti della rete.

Questo tipo di rete ha diversi vincoli.

- La rete può avere al massimo una rete vSphere sottostante su ciascuna istanza VMware Cloud Director registrata nel sistema.
- Tutti i commutatori delle reti sottostanti devono essere dello stesso tipo, ovvero commutatori distribuiti o commutatori standard di vSphere.

Reti esterne supportate da un router logico di livello 0

Una rete esterna può essere supportata da un router logico di livello 0 NSX-T Data Center.

Nota Le reti esterne supportate dai gateway di livello 0 di VRF-lite in NSX-T Data Center non sono supportate. Per ulteriori informazioni sui gateway VRF (Virtual Routing and Forwarding), vedere *Guida all'amministrazione di NSX-T Data Center*.

Aggiunta di una rete esterna supportata da risorse di vSphere

Quando si aggiunge una rete esterna, è possibile registrare le risorse di rete di vSphere che devono essere utilizzate da VMware Cloud Director. È possibile creare reti VDC dell'organizzazione da connettere a una rete esterna.

È possibile aggiungere una rete esterna IPv4 o IPv6. Una rete esterna IPv6 supporta le subnet IPv4 e IPv6 e una rete esterna IPv4 supporta le subnet IPv4 e IPv6.

Prerequisiti

Verificare che un gruppo di porte di vSphere sia disponibile con o senza trunking VLAN. Gruppi di porte flessibili con binding di porta statico garantiscono prestazioni ottimali.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra, fare clic su **Reti esterne** e su **Nuovo**.
- 3 Selezionare **Risorse vSphere**, quindi selezionare il tipo di gruppi di porte che devono supportare la rete e fare clic su **Avanti**.
- 4 Immettere un nome e, facoltativamente, una descrizione per la nuova rete esterna.
- 5 Selezionare i gruppi di porte che devono supportare la rete esterna e fare clic su **Avanti**.

- 6 Configurare almeno una subnet e fare clic su **Avanti**.
 - a Per aggiungere una subnet, fare clic su **Aggiungi**.
 - b Immettere le impostazioni CIDR (Classless Inter-Domain Routing) della rete.
Utilizzare il formato *network_gateway_IP_address/subnet_prefix_length*, ad esempio **192.167.1.1/24**.
 - c (Facoltativo) Immettere le impostazioni DNS.
 - d Configurare un pool di IP statici aggiungendo almeno un intervallo di IP o un indirizzo IP.
 - e Fare clic su **OK**.
 - f (Facoltativo) Per aggiungere un'altra subnet, ripetere questo passaggio.
- 7 Controllare le impostazioni di rete, quindi fare clic su **Fine**.

Operazioni successive

È possibile creare una rete VDC dell'organizzazione da connettere a una rete esterna.

Aggiunta di una rete esterna supportata da un router logico di livello 0 NSX-T Data Center

Per registrare risorse di rete di NSX-T Data Center utilizzabili da VMware Cloud Director, aggiungere una rete esterna supportata da un router logico di livello 0.

Procedura

- 1 Creare un router logico di livello 0.
 - Creare il router di livello 0 in NSX-T Manager.
 - a Accedere con privilegi di amministratore all'istanza di NSX-T Manager.
 - b Fare clic su **Rete**, su **Gateway di livello 0** e quindi su **Aggiungi gateway di livello 0**.
 - c Immettere un nome per il router di livello 0.
 - d Selezionare una modalità High Availability.

Nota Per impostazione predefinita, viene utilizzata la modalità Attiva-Attiva. In modalità Attiva-Attiva, il carico del traffico viene bilanciato tra tutti i membri. In modalità Attiva-Standby, il traffico viene elaborato da un membro attivo scelto. Se il membro attivo non riesce, un nuovo membro diventa attivo.

 - e Nel menu a discesa selezionare un cluster edge NSX-T esistente che supporti questo router logico di livello 0 e fare clic su **Salva**.
 - Creare il router logico di livello 0 utilizzando l'API dei criteri di NSX.
- 2 Accedere al VMware Cloud Director Service Provider Admin Portal.
- 3 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 4 Nel riquadro a sinistra, fare clic su **Reti esterne** e su **Nuovo**.

- 5 Selezionare **Risorse NSX-T (router di livello 0)**, quindi selezionare un'istanza di NSX-T Manager registrata che supporti la rete e fare clic su **Avanti**.
- 6 Immettere un nome e, facoltativamente, una descrizione per la nuova rete esterna.
- 7 Selezionare un router di livello 0 per connettersi alla rete esterna e fare clic su **Avanti**.
- 8 Configurare almeno una subnet e fare clic su **Avanti**.
 - a Per aggiungere una subnet, fare clic su **Aggiungi**.
 - b Immettere le impostazioni CIDR (Classless Inter-Domain Routing) della rete.
 - c (Facoltativo) Immettere le impostazioni DNS.
 - d Configurare un pool di IP statici aggiungendo almeno un intervallo di IP o un indirizzo IP.
 - e Fare clic su **OK**.
 - f (Facoltativo) Per aggiungere un'altra subnet, ripetere la procedura dal passaggio [8.a](#) al passaggio [8.e](#).
- 9 Controllare le impostazioni di rete, quindi fare clic su **Fine**.

Operazioni successive

Utilizzare il router di livello 0 per creare un uplink alla rete esterna.

Pool di reti

Un pool di reti è un gruppo di reti indifferenziate disponibili in un VDC dell'organizzazione per creare reti di vApp e determinati tipi di reti VDC dell'organizzazione.

Un pool di reti è supportato dalle risorse di rete di vSphere come ID VLAN o gruppi di porte, tramite risorse di NSX Data Center for vSphere o risorse di NSX-T Data Center.

VMware Cloud Director utilizza i pool di reti per creare reti VDC dell'organizzazione interne e instradate da NAT e tutte le reti di vApp. Il traffico di rete su ogni rete di un pool è isolato al livello del layer 2 rispetto alle altre reti.

Ogni VDC dell'organizzazione in VMware Cloud Director può includere un solo pool di reti. Più VDC dell'organizzazione possono condividere lo stesso pool di reti. Il pool di reti di un VDC dell'organizzazione fornisce le reti create per soddisfare la quota di rete di un VDC dell'organizzazione.

Pool di rete VXLAN

Ogni VDC del provider supportato da NSX Data Center for vSphere include un pool di reti VXLAN.

Quando si crea un VDC del provider supportato da NSX Data Center for vSphere, è possibile associare tale VDC del provider a un pool di reti VXLAN esistente oppure creare un pool di reti VXLAN per il VDC del provider.

Al pool di reti VXLAN appena creato viene assegnato un nome derivato dal nome del VDC del provider in cui è contenuto. Il nome viene aggiunto al pool al momento della creazione. Non è possibile eliminare o modificare il pool di reti. Se si rinomina il VDC del provider, il pool di reti VXLAN viene rinominato automaticamente.

Nota Per garantire prestazioni di rete ottimali nell'infrastruttura, creare un pool di reti VXLAN e associarlo a tutti i VDC del provider al momento della loro creazione.

Le reti VXLAN di VMware Cloud Director si basano sullo standard VXLAN IETF e offrono diversi vantaggi.

- Reti logiche che si estendono a livello del layer 3
- Reti logiche che si estendono su più rack su un singolo livello layer 2
- Contenimento delle trasmissioni
- Prestazioni superiori
- Maggior portata (fino a 16 milioni di indirizzi di rete)

Per maggiori informazioni sulle reti VXLAN in un ambiente VMware Cloud Director, consultare la *guida all'amministrazione di NSX*.

Creazione di un pool di reti supportato da una zona di trasporto NSX Data Center for vSphere

Per registrare una zona di trasporto di NSX Data Center for vSphere utilizzabile da VMware Cloud Director, aggiungere un pool di reti con supporto VXLAN.

Prerequisiti

Creare una zona di trasporto NSX Data Center for vSphere in un'istanza di vCenter Server qualsiasi registrata in VMware Cloud Director. Vedere la *guida all'amministrazione di NSX*.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **Pool di reti** e fare clic su **Nuovo**.
- 3 Digitare un nome e, facoltativamente, una descrizione per il nuovo pool di reti, quindi fare clic su **Avanti**.
- 4 Selezionare **Con supporto VXLAN** e fare clic su **Avanti**.
- 5 Selezionare un'istanza di vCenter Server per specificare la zona di trasporto VXLAN che deve essere utilizzata da questo pool di reti e fare clic su **Avanti**.
- 6 Selezionare una zona di trasporto NSX Data Center for vSphere che deve supportare il nuovo pool di reti e fare clic su **Avanti**.

Nota Per creare un pool di reti universale per la rete inter-VDC, selezionare una zona di trasporto di tipo UNIVERSAL_VXLAN.

- 7 Controllare le impostazioni del pool di reti, quindi fare clic su **Fine**.

Operazioni successive

Creare una rete VDC dell'organizzazione supportata dal pool di reti o associare il pool di reti a un VDC dell'organizzazione e creare reti vApp.

Pool di reti Geneve

Ogni VDC del provider supportato da NSX-T Data Center include un pool di reti Geneve.

Geneve è lo standard di virtualizzazione delle reti che fornisce la funzione di overlay in NSX-T Data Center.

Quando si crea un VDC del provider supportato da NSX-T Data Center, è possibile associare tale VDC del provider a un pool di reti Geneve esistente oppure creare un pool di reti Geneve per il VDC del provider.

Le reti Geneve di VMware Cloud Director offrono una serie di vantaggi.

- Reti logiche che si estendono a livello del layer 3
- Reti logiche che si estendono su più rack su un singolo livello layer 2
- Contenimento delle trasmissioni
- Prestazioni superiori
- Maggior portata (fino a 16 milioni di indirizzi di rete)

Creazione di un pool di reti supportato da una zona di trasporto NSX-T Data Center

Per registrare una zona di trasporto NSX-T Data Center utilizzabile da VMware Cloud Director, è possibile creare un pool di reti con supporto Geneve.

Prerequisiti

Creare una zona di trasporto NSX-T Data Center con supporto overlay. Per ulteriori informazioni sulla creazione della zona di trasporto e Generic Network Virtualization Encapsulation, denominato overlay di Geneve, vedere la *documentazione del prodotto NSX-T Data Center*.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **Pool di reti** e fare clic su **Nuovo**.
- 3 Digitare un nome e, facoltativamente, una descrizione per il nuovo pool di reti, quindi fare clic su **Avanti**.
- 4 Selezionare **Con supporto Geneve** e fare clic su **Avanti**.
- 5 Selezionare un'istanza di NSX-T Manager per fornire la zona di trasporto per questo pool di reti e fare clic su **Avanti**.
- 6 Selezionare una zona di trasporto NSX-T e fare clic su **Avanti**.
- 7 Controllare le impostazioni del pool di reti, quindi fare clic su **Fine**.

Operazioni successive

Creare una rete VDC dell'organizzazione supportata dal pool di reti o associare il pool di reti a un VDC dell'organizzazione e creare reti vApp.

Creazione di un pool di reti supportato da ID VLAN

Per registrare gli ID VLAN di vSphere utilizzabili da VMware Cloud Director, è necessario aggiungere un pool di reti con supporto VLAN. Un pool di reti con supporto VLAN offre sicurezza, scalabilità e prestazioni per le reti VDC dell'organizzazione.

Prerequisiti

Verificare che in vSphere siano disponibili un intervallo di ID VLAN e un commutatore distribuito vSphere. Gli ID VLAN devono essere ID validi configurati nel commutatore fisico al quale sono connessi i server ESXi.

Attenzione Le VLAN devono essere isolate al livello del layer 2. Il mancato isolamento delle VLAN può causare un'interruzione della connessione di rete.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **Pool di reti** e fare clic su **Nuovo**.
- 3 Digitare un nome e, facoltativamente, una descrizione per il nuovo pool di reti, quindi fare clic su **Avanti**.
- 4 Selezionare **Con supporto VLAN**, quindi fare clic su **Avanti**.
- 5 Selezionare un'istanza di vCenter Server per specificare il commutatore virtuale distribuito che deve essere utilizzato da questo pool di reti e fare clic su **Avanti**.
- 6 Immettere un intervallo di ID VLAN e fare clic su **Avanti**.
- 7 Selezionare un commutatore distribuito per il pool di reti e fare clic su **Avanti**.
- 8 Controllare le impostazioni del pool di reti, quindi fare clic su **Fine**.

Operazioni successive

Creare una rete VDC dell'organizzazione supportata dal pool di reti o associare il pool di reti a un VDC dell'organizzazione e creare reti vApp.

Creazione di un pool di reti supportato da gruppi di porte di vSphere

Per registrare gruppi di porte di vSphere utilizzabili da VMware Cloud Director, aggiungere un pool di reti supportato da gruppi di porte. Diversamente dagli altri tipi di pool di reti, un pool

di reti supportato da gruppi di porte non richiede un commutatore distribuito di vSphere e può supportare gruppi di porte associati ad adattatori distribuiti di terze parti.

Attenzione I gruppi di porte devono essere isolati da tutti gli altri gruppi di porte al layer 2, fisicamente o mediante tag VLAN. Il mancato isolamento dei gruppi di porte può causare un'interruzione della connessione di rete.

Prerequisiti

Verificare che nell'ambiente vSphere siano disponibili uno o più gruppi di porte. I gruppi di porte devono essere disponibili in ogni host ESXi nel cluster e ogni gruppo di porte deve utilizzare solo una singola rete VLAN. Sono supportati gruppi di porte con o senza trunking VLAN.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **Pool di reti** e fare clic su **Nuovo**.
- 3 Digitare un nome e, facoltativamente, una descrizione per il nuovo pool di reti, quindi fare clic su **Avanti**.
- 4 Selezionare **Con supporto di gruppi di porte** e fare clic su **Avanti**.
- 5 Selezionare un'istanza di vCenter Server che fornisca i gruppi di porte che devono essere utilizzati da questo pool di reti e fare clic su **Avanti**.
- 6 Selezionare uno o più gruppi di porte e fare clic su **Avanti**.
È possibile creare una rete per ogni gruppo di porte.
- 7 Controllare le impostazioni del pool di reti, quindi fare clic su **Fine**.

Operazioni successive

Creare una rete VDC dell'organizzazione supportata dal pool di reti o associare il pool di reti a un VDC dell'organizzazione e creare reti vApp.

Visualizzazione delle istanze di vCenter Server

È possibile visualizzare un elenco delle istanze di vCenter Server in tutti i siti dell'installazione di VMware Cloud Director. È possibile vedere come VMware Cloud Director utilizza ciascuna istanza di vCenter Server.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.

Risultati

Viene visualizzato un elenco di tutte le istanze di vCenter Server associate. L'elenco contiene le informazioni seguenti per ciascuna istanza di vCenter Server.

	Descrizione
Nome	Il nome dell'istanza di vCenter Server in VMware Cloud Director.
Stato	Lo stato di vCenter Server può essere normale, con avviso e critico.
Stato	Abilitato o disabilitato. Vedere Abilitazione o disabilitazione di un'istanza di vCenter Server .
Connessione	Connesso o meno a VMware Cloud Director. Vedere Riconnessione di un'istanza di vCenter Server .
Host VC	Nome di dominio completo dell'istanza di vCenter Server.
Versione	La versione di vCenter Server.
Utilizzo	Le istanze di vCenter Server dedicate hanno abilitato l'accesso al tenant. Il provider può utilizzare pool di risorse diversi dell'istanza di vCenter Server condivisa in più VDC del provider e quindi allocare tali pool di risorse a tenant diversi. Vedere Capitolo 9 Gestione di istanze di vCenter Server dedicate .
Integrità cluster	Aggregazione dell'integrità di tutti i cluster nell'istanza di vCenter Server. Quando si aggrega l'aggregazione del cluster, viene visualizzata l'integrità dell'ultimo cluster meno integro.
Cluster	Numero di cluster nell'istanza di vCenter Server.
Macchine virtuali	Numero di macchine virtuali nell'istanza di vCenter Server.
Macchine virtuali in esecuzione	Numero di macchine virtuali in esecuzione nell'istanza di vCenter Server.
CPU	Quantità di CPU virtuale utilizzata attivamente come percentuale della CPU di vCenter Server totale disponibile.
Memoria	Quantità di memoria virtuale utilizzata attivamente come percentuale della memoria di vCenter Server totale disponibile.
Storage	Quantità di storage virtuale utilizzato attivamente come percentuale dello storage di vCenter Server disponibile totale.

Modifica delle impostazioni di vCenter Server

Se le informazioni della connessione per un'istanza di vCenter Server collegata cambiano o si desidera modificarne il nome e la descrizione in VMware Cloud Director, è possibile modificare le impostazioni dell'istanza.

È possibile modificare le impostazioni configurate in fase di aggiunta dell'istanza di vCenter Server. Vedere [Aggiunta dell'istanza di vCenter Server](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel riquadro a sinistra fare clic su **vCenter** e quindi sul nome dell'istanza di vCenter Server che si desidera modificare.
- 3 Nell'angolo superiore destro della sezione **Informazioni su vCenter**, fare clic su **Modifica**.
- 4 Modificare le impostazioni di vCenter Server e fare clic su **Salva**.

Operazioni successive

Se sono state modificate le informazioni della connessione, è necessario eseguire la procedura [Riconnessione di un'istanza di vCenter Server](#).

Abilitazione o disabilitazione di un'istanza di vCenter Server

Prima di eseguire una manutenzione o annullare la registrazione di un'istanza di vCenter Server, è necessario disabilitare l'istanza di vCenter Server di destinazione. Per fornire le relative risorse ai virtual data center in VMware Cloud Director, è necessario abilitare l'istanza di vCenter Server.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'istanza di vCenter Server di destinazione e scegliere **Abilita** o **Disabilita**.
- 4 Per confermare, fare clic su **OK**.

Riconnessione di un'istanza di vCenter Server

Se un'istanza di vCenter Server è disconnessa o se sono state modificate le impostazioni di connessione, è possibile provare a reimpostare la connessione.

Nota Mentre viene stabilita la nuova connessione, l'istanza di vCenter Server non è disponibile per alcuna operazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'istanza di vCenter Server di destinazione e fare clic su **Riconnetti**.

- 4 Per confermare, fare clic su **OK**.

Aggiornamento di un'istanza di vCenter Server

Per aggiornare le informazioni nel database di VMware Cloud Director relative alle risorse di vCenter Server sottostanti, è necessario aggiornare l'istanza di vCenter Server.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'istanza di vCenter Server di destinazione e fare clic su **Aggiorna**.
- 4 Per confermare, fare clic su **OK**.

Aggiornamento dei criteri di storage di un'istanza di vCenter Server

Per aggiornare le informazioni nel database di VMware Cloud Director sui criteri di storage della macchina virtuale nell'ambiente vSphere sottostante, è necessario aggiornare i criteri di storage dell'istanza di vCenter Server.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'istanza di vCenter Server di destinazione e fare clic su **Aggiorna criteri**.
- 4 Per confermare, fare clic su **OK**.

Annullamento della registrazione di un'istanza di vCenter Server

Per interrompere l'utilizzo delle risorse di un'istanza di vCenter Server, è possibile rimuovere questa istanza di vCenter Server dall'installazione di VMware Cloud Director.

Prerequisiti

- Disabilitare l'istanza di vCenter Server. Vedere [Abilitazione o disabilitazione di un'istanza di vCenter Server](#).
- Eliminare tutti i virtual data center del provider che utilizzano pool di risorse di questa istanza di vCenter Server. Vedere [Eliminazione di un virtual data center del provider](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'istanza di vCenter Server di destinazione e fare clic su **Annulla registrazione**.
- 4 Per confermare, fare clic su **OK**.

Modifica delle impostazioni di NSX Manager

Se le informazioni della connessione per un'istanza di NSX Manager registrata cambiano o si desidera modificarne il nome e la descrizione in VMware Cloud Director, è possibile modificare le impostazioni dell'istanza.

È possibile modificare le impostazioni configurate in fase di aggiunta dell'istanza di NSX Manager. Vedere [\(Facoltativo\) Aggiunta dell'istanza di NSX Manager associata](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel riquadro a sinistra fare clic su **vCenter** e quindi sul nome dell'istanza di vCenter Server associata all'istanza di NSX Manager di destinazione.
- 3 Nell'angolo superiore destro della sezione **Informazioni su NSX-V Manager**, fare clic su **Modifica**.
- 4 Modificare il nome host e le credenziali dell'amministratore di NSX Manager e fare clic su **Salva**.
- 5 (Facoltativo) Per abilitare la rete inter-VDC per i virtual data center supportati da questa istanza di vCenter Server, attivare l'opzione, quindi immettere le proprietà della macchina virtuale di controllo e un nome per l'ambito del provider di rete.

Le proprietà della macchina virtuale di controllo vengono utilizzate per la distribuzione di un'appliance nell'istanza di NSX Manager per i componenti della rete inter-VDC, come un router universale.

Parametro	Descrizione
Percorso pool di risorse	Il percorso gerarchico di un pool di risorse specifico nell'istanza di vCenter Server, a partire dal cluster <i>Cluster/Resource_Pool_Parent/Target_Resource</i> . Ad esempio TestbedCluster1/mgmt-rp . In alternativa, è possibile immettere l'ID di riferimento oggetto gestito del pool di risorse. Ad esempio, resgroup-1476 .
Nome archivio dati	Nome dell'archivio dati che ospiterà i file dell'appliance, ad esempio shared-disk-1 .

Parametro	Descrizione
Interfaccia di gestione	Il nome della rete in vCenter Server o gruppo di porte utilizzato per l'interfaccia di gestione HA DLR, ad esempio TestbedPG1 .
Ambito del provider di rete	Corrisponde al dominio di errore di rete nelle topologie di rete dei gruppi di data center. ad esempio boston-fault1 . Per informazioni sulla gestione dei gruppi inter-VDC, vedere <i>VMware Cloud Director Tenant Portal Guide</i> .

Modifica delle impostazioni di NSX-T Manager

Se le informazioni della connessione per un'istanza di NSX-T Manager registrata cambiano o si desidera modificarne il nome e la descrizione in VMware Cloud Director, è possibile modificare le impostazioni dell'istanza.

È possibile modificare le impostazioni configurate in fase di aggiunta dell'istanza di vCenter Server. Vedere [Registrazione di un'istanza di NSX-T Manager](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel riquadro a sinistra fare clic su **NSX-T Manager** e quindi sul nome dell'istanza di NSX-T Manager che si desidera modificare.
- 3 Nell'angolo superiore destro della scheda **Generale**, fare clic su **Modifica**.
- 4 Modificare le impostazioni di NSX-T Manager e fare clic su **Salva**.

Eliminazione di un'istanza di NSX-T Manager

Per interrompere l'utilizzo delle risorse di un'istanza di NSX-T Manager, è possibile rimuovere questa istanza di vCenter Server dall'installazione di VMware Cloud Director.

Prerequisiti

Eliminare tutti i virtual data center del provider che utilizzano risorse di questa istanza di NSX-T Manager. Vedere [Eliminazione di un virtual data center del provider](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel riquadro sinistro fare clic su **NSX-T Manager**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'istanza di NSX-T Manager che si desidera rimuovere e fare clic su **Elimina**.
- 4 Per confermare, fare clic su **Elimina**.

Configurazione e gestione di distribuzioni multisito

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.

Quando si associano due siti di VMware Cloud Director, si abilita l'amministrazione dei siti come singola entità. Si abilita inoltre l'associazione delle organizzazioni di tali siti. Quando un'organizzazione fa parte di un'associazione, gli utenti dell'organizzazione possono utilizzare il VMware Cloud Director Tenant Portal per accedere alle risorse dell'organizzazione che si trovano in qualsiasi sito membro, anche se ciascuna organizzazione membro e le relative risorse si trovano in locale nel sito che occupano.

Nota Per associare siti, è necessario utilizzare l'API di VMware Cloud Director. I siti devono avere la stessa versione dell'API di VMware Cloud Director oppure la versione immediatamente precedente o successiva. Ad esempio, è possibile associare un sito VMware Cloud Director 10.0 (API versione 33.0) con un sito VMware Cloud Director versione 9.7, 10.0 o 10.1, rispettivamente con le versioni API 32.0, 33.0 o 34.0.

Dopo aver associato due siti, è possibile utilizzare l'API di VMware Cloud Director o VMware Cloud Director Tenant Portal per associare le organizzazioni che occupano tali siti. Vedere *Guida alla programmazione dell'API di VMware Cloud Director* e *VMware Cloud Director Tenant Portal Guide*.

Un sito o un'organizzazione può creare un numero illimitato di associazioni con un peer, ma ciascuna associazione include esattamente due membri. Ciascun sito od organizzazione deve disporre della propria chiave privata. I membri di un'associazione stabiliscono una relazione di attendibilità attraverso lo scambio di chiavi pubbliche che vengono utilizzate per verificare le richieste firmate inviate da un membro all'altro.

Ciascun sito di un'associazione viene definito dall'ambito di un gruppo di server VMware Cloud Director (un gruppo di server che condivide un database di VMware Cloud Director). Ciascuna organizzazione di un'associazione occupa un singolo sito. L'amministratore dell'organizzazione controlla l'accesso agli asset di ogni sito membro da parte di utenti e gruppi dell'organizzazione.

Oggetti Site e associazioni di siti

Il processo di installazione o aggiornamento crea un oggetto `site` che rappresenta il gruppo di server VMware Cloud Director locale. Un amministratore di sistema la cui autorità si estende a più gruppi di server VMware Cloud Director può configurare tali gruppi di server come un'associazione di siti di VMware Cloud Director.

Associazioni di organizzazioni

Una volta completata l'associazione del sito, gli amministratori dell'organizzazione di qualsiasi sito membro possono iniziare ad associare le rispettive organizzazioni.

Nota Non è possibile associare un'organizzazione `System` a un'organizzazione `tenant`.
L'organizzazione `System` in qualsiasi sito può essere associata solo all'organizzazione `System` in un altro sito.

Identità di utenti e gruppi

Le associazioni di siti e organizzazioni devono accettare di utilizzare lo stesso provider di identità. Le identità di utenti e gruppi per tutte le organizzazioni nell'associazione devono essere gestite tramite questo provider di identità.

Ad eccezione dell'organizzazione `System`, che deve utilizzare il provider di identità integrato di VMware Cloud Director, le associazioni sono libere di scegliere il provider di identità più adatto alle loro esigenze.

Controllo dell'accesso al sito per utenti e gruppi dell'organizzazione

Gli amministratori dell'organizzazione possono configurare il proprio provider di identità in modo che generi token di accesso di utenti o gruppi che siano validi in tutti i siti membri oppure solo in un sottoinsieme di siti membri. Mentre le identità di utenti e gruppi devono essere le stesse in tutte le organizzazioni membro, i diritti di utenti e gruppi sono limitati dai ruoli assegnati a tali utenti e gruppi in ogni organizzazione membro. L'assegnazione di un ruolo a un utente o un gruppo è locale rispetto all'organizzazione membro, così come gli eventuali ruoli personalizzati che vengono creati.

Requisiti di bilanciamento del carico

L'implementazione efficace di una distribuzione multisito richiede la configurazione di un bilanciamento del carico che distribuisca le richieste in arrivo in un endpoint istituzionale, come `https://vcloud.example.com`, agli endpoint per ciascun membro dell'associazione dei siti (ad esempio, `https://us.vcloud.example.com` e `https://uk.vcloud.example.com`). Se un sito dispone di più celle, è inoltre necessario configurare un bilanciamento del carico che distribuisca le richieste in arrivo a tutte le celle, in modo che una richiesta a `https://us.vcloud.example.com` possa essere gestita da `https://cell1.us.vcloud.example.com`, `https://cell2.us.vcloud.example.com` e così via.

Stato di un membro dell'associazione

Dopo avere creato un'associazione di siti o organizzazioni, il sistema locale recupera periodicamente lo stato di ciascun membro dell'associazione remota e aggiorna tale stato nel database VMware Cloud Director del sito locale. Lo stato del membro è visibile nell'elemento `Status` di un elemento `SiteAssociationMember` o `OrgAssociationMember`. Questo elemento può avere uno dei tre valori seguenti:

ACTIVE

L'associazione è stata stabilita da entrambe le parti e la comunicazione con la parte remota è riuscita.

ASYMMETRIC

L'associazione è stata stabilita nel sito locale, ma il sito remoto non ha ancora risposto con un'azione corrispondente.

UNREACHABLE

È stata creata un'associazione da entrambe le parti, ma il sito remoto non è al momento raggiungibile in rete.

Questo processo, definito "heartbeat", viene eseguito con l'identità dell'utente del sistema multisito, un account utente VMware Cloud Director locale creato nell'organizzazione System durante l'installazione di VMware Cloud Director. Nonostante questo account sia membro dell'organizzazione System, non dispone di diritti di amministratore di sistema, ma di un diritto singolo, ovvero `Multisite: System Operations`, che fornisce le autorizzazioni per creare una richiesta dell'API di VMware Cloud Director che recuperi lo stato del membro remoto di un'associazione di siti.

Elenchi di risorse multisito

Se si utilizzano distribuzioni di VMware Cloud Director in più posizioni, è possibile visualizzare gli elenchi di risorse che includono informazioni sugli oggetti di tutti i siti connessi.

Per facilitare la navigazione attraverso vSphere e le risorse cloud dal Service Provider Admin Portal, a partire dalla versione 9.7, VMware Cloud Director include elenchi di risorse multisito. A partire dalla versione 10.0, VMware Cloud Director supporta gli elenchi di risorse multisito che includono le organizzazioni.

È possibile accedere agli elenchi di risorse tramite i menu **Risorse vSphere** e **Risorse cloud**.

È possibile accedere a informazioni dettagliate sugli oggetti provenienti da siti diversi e creare oggetti sia nel sito locale sia in siti remoti.

Gli elenchi di risorse multisito di vSphere sono supportati per le istanze di vCenter Server, le istanze di NSX-T Manager, i pool di risorse, gli archivi dati, gli host, i commutatori distribuiti, i gruppi di porte, gli elementi bloccati e i criteri di storage.

Gli elenchi di risorse cloud multisito sono supportati per organizzazioni, VDC dell'organizzazione, modelli di VDC dell'organizzazione, VDC del provider, celle cloud, gateway edge, reti esterne, pool di reti e criteri di dimensionamento delle macchine virtuali.

Gestione dei virtual data center del provider

4

Dopo avere creato un virtual data center del provider, è possibile modificarne le proprietà, disabilitarlo o eliminarlo, nonché gestirne i criteri di storage e i pool di risorse.

Per creare un virtual data center del provider, è necessario utilizzare Service Provider Admin Portal o l'API di vCloud. Per informazioni sull'utilizzo di Service Provider Admin Portal, vedere [Creazione di un virtual data center del provider](#). Per informazioni sull'utilizzo dell'API di vCloud, vedere *Guida alla programmazione dell'API di VMware Cloud Director*.

Questo capitolo include i seguenti argomenti:

- [Abilitazione o disabilitazione di un virtual data center del provider](#)
- [Eliminazione di un virtual data center del provider](#)
- [Modifica delle impostazioni generali di un virtual data center del provider](#)
- [Unione di virtual data center del provider](#)
- [Visualizzazione dei virtual data center dell'organizzazione di un virtual data center del provider](#)
- [Visualizzazione degli archivi dati in un virtual data center del provider](#)
- [Visualizzazione delle reti esterne in un virtual data center del provider](#)
- [Gestione dei criteri di storage della macchina virtuale in un virtual data center del provider](#)
- [Gestione dei pool di risorse in un virtual data center del provider](#)
- [Modifica dei metadati per un virtual data center del provider](#)

Abilitazione o disabilitazione di un virtual data center del provider

Per disabilitare tutti i virtual data center esistenti dell'organizzazione che utilizzano le risorse di un virtual data center del provider, è possibile disabilitare tale virtual data center del provider. Non è possibile creare virtual data center dell'organizzazione che utilizzino le risorse di un virtual data center del provider disabilitato.

Le vApp in esecuzione su macchine virtuali continuano a essere eseguite nei virtual data center dell'organizzazione esistenti supportati da questo virtual data center del provider, ma non è possibile creare o avviare ulteriori vApp o macchine virtuali.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider**.
- 3 Fare clic sul pulsante di opzione accanto al nome del virtual data center del provider di destinazione e scegliere **Abilita** o **Disabilita**.
- 4 Per confermare, fare clic su **OK**.

Eliminazione di un virtual data center del provider

Per rimuovere le risorse di un virtual data center del provider da VMware Cloud Director, è possibile eliminare il virtual data center del provider.

Le risorse sottostanti in vSphere rimangono inalterate.

Prerequisiti

- Disabilitare il virtual data center del provider di destinazione. Vedere [Abilitazione o disabilitazione di un virtual data center del provider](#).
- Eliminare tutti i virtual data center dell'organizzazione che utilizzano le risorse di questo virtual data center del provider. Vedere [Eliminazione di un virtual data center dell'organizzazione](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider**.
- 3 Fare clic sul pulsante di opzione accanto al nome del virtual data center del provider che si desidera rimuovere e fare clic su **Elimina**.
- 4 Per confermare, fare clic su **OK**.

Modifica delle impostazioni generali di un virtual data center del provider

È possibile modificare il nome e la descrizione di un virtual data center del provider. Se il pool di risorse di supporto supporta una versione hardware virtuale superiore, è possibile aggiornare l'hardware virtuale più recente supportato da un virtual data center del provider.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC del provider** e fare clic sul nome del virtual data center del provider che si desidera modificare.
- 3 Nell'angolo superiore destro della scheda **Configura > Generale**, fare clic su **Modifica**.
- 4 (Facoltativo) Modificare il nome e la descrizione del virtual data center del provider.

- 5 (Facoltativo) Nel menu a discesa selezionare la versione hardware più recente supportata da questo virtual data center del provider, quindi fare clic su **Salva**.

La versione più recente che è possibile selezionare è determinata dagli host ESXi nel pool di risorse che supporta il virtual data center del provider.

Nota È possibile aggiornare solo la versione dell'hardware supportata da un virtual data center del provider. Non è possibile eseguire il downgrade della versione dell'hardware. La versione dell'hardware della macchina virtuale più recente supportata in VMware Cloud Director 10.1.0 è la versione 15. La versione hardware 15 è disponibile quando viene abilitata nell'istanza di vCenter Server a livello di cluster o di data center.

- 6 Fare clic su **Salva**.

Unione di virtual data center del provider

Per combinare le risorse di due virtual data center del provider, è possibile unire questi ultimi in un singolo virtual data center del provider.

Prerequisiti

- I virtual data center del provider di destinazione appartengono allo stesso data center di vCenter Server.
- I virtual data center del provider di destinazione contengono solo virtual data center dell'organizzazione elastici.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider**.
- 3 Fare clic sul pulsante di opzione accanto al nome del virtual data center del provider che si desidera espandere e fare clic su **Unisci**.
- 4 Fare clic sul pulsante di opzione accanto al nome del virtual data center del provider con cui unire le risorse e fare clic su **Unisci**.

Visualizzazione dei virtual data center dell'organizzazione di un virtual data center del provider

È possibile visualizzare un elenco dei virtual data center dell'organizzazione che utilizzano risorse da un virtual data center del provider.

Procedura


- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.

3 Fare clic sulla scheda **VDC dell'organizzazione**.

Risultati

Viene visualizzato l'elenco dei virtual data center dell'organizzazione che utilizzano le risorse di questo virtual data center del provider. Per ogni VDC dell'organizzazione, l'elenco include informazioni sulla condizione, lo stato, il modello di allocazione, l'organizzazione, l'istanza di vCenter Server, il numero di reti, il numero di vApp, il numero di criteri di storage e il numero di pool di risorse.

Operazioni successive

- È possibile passare alla vista dei virtual data center dell'organizzazione nella VMware Cloud Director Tenant Portal facendo clic sull'icona **pop-out**  accanto al nome del virtual data center dell'organizzazione di destinazione.
- Facendo clic sul pulsante di opzione accanto al nome di un virtual data center dell'organizzazione, è possibile eseguire operazioni di gestione simili alle operazioni descritte in [Capitolo 6 Gestione dei virtual data center dell'organizzazione](#).

Visualizzazione degli archivi dati in un virtual data center del provider

È possibile visualizzare i dettagli relativi agli archivi dati che forniscono la capacità di storage a un virtual data center del provider.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Archivi dati**.

Viene visualizzato l'elenco di tutti i datastore presenti nel virtual data center del provider. L'elenco contiene le informazioni seguenti per ciascun archivio dati.

Titolo	Descrizione
Nome	Nome dell'archivio dati
Stato	Abilitato o disabilitato
Tipo	Tipo di file system utilizzato dall'archivio dati. Può essere VMFS (Virtual Machine File System) o NFS (Network File System).
Utilizzato	Lo spazio di archivio dati occupato dai file delle macchine virtuali, compresi i file di registro, le snapshot e i dischi virtuali. Quando viene accesa una macchina virtuale, lo spazio di storage utilizzato comprende anche i file di registro.

Titolo	Descrizione
Provisioning effettuato	Lo spazio dell'archivio dati riservato alle macchine virtuali. Se sono presenti macchine virtuali che utilizzano il thin provisioning, parte dello spazio può non essere utilizzato, quindi tale spazio rimane a disposizione di altre macchine virtuali. Se viene utilizzato il thin provisioning, questo valore potrebbe essere maggiore della capacità effettiva dell'archivio dati.
Storage richiesto	<p>Storage di cui è stato effettuato il provisioning utilizzato solo dagli oggetti di VMware Cloud Director nell'archivio dati, tra cui:</p> <ul style="list-style-type: none"> ■ Macchine virtuali con provisioning effettuato in VMware Cloud Director ■ Voci di catalogo (modelli e file multimediali) ■ NSX Edge ■ Requisiti di swapping della memoria utilizzata e non utilizzata per le macchine virtuali <p>Questo valore non include lo storage richiesto per le macchine virtuali shadow o per i dischi intermedi nella struttura di un clone collegato.</p>
vCenter Server	Istanza di vCenter Server associata all'archivio dati.

Visualizzazione delle reti esterne in un virtual data center del provider

È possibile visualizzare un elenco delle reti esterne accessibili per un virtual data center del provider.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Reti esterne**.

Risultati

È possibile visualizzare un elenco delle reti esterne disponibili con le informazioni relative alle impostazioni CIDR del gateway e all'utilizzo del pool di IP.

Gestione dei criteri di storage della macchina virtuale in un virtual data center del provider

È possibile aggiungere, abilitare, disabilitare e rimuovere i criteri di storage della macchina virtuale da un virtual data center del provider. È possibile inoltre aggiungere, modificare ed eliminare metadati per un criterio di storage in un virtual data center del provider.

Abilitazione della crittografia della macchina virtuale nei criteri di storage di un virtual data center del provider

È possibile aggiungere un criterio di storage abilitato per la crittografia in un VDC del provider. È possibile crittografare macchine virtuali e dischi associando una macchina virtuale o un disco a un criterio di storage che disponga della funzionalità di 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. 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.

Abilitazione della crittografia delle macchine virtuali

Per crittografare le macchine virtuali in VMware Cloud Director, è necessario configurare almeno un server di gestione chiavi (KMS) nell'istanza di vCenter Server e associare macchine virtuali e dischi a un criterio di storage che disponga della funzionalità di crittografia della macchina virtuale.

- 1 In vCenter Server, aggiungere un cluster KMS. Un'istanza di vCenter Server può includere più cluster KMS. Per informazioni sulla configurazione di un cluster di server di gestione chiavi, vedere l'argomento [Configurazione del cluster del server di gestione chiavi](#) nella *vSphere Guida alla sicurezza*.
- 2 In vCenter Server, abilitare la crittografia in un criterio di storage. Vedere l'argomento [Creazione di un criterio di storage di crittografia](#) nella *vSphere Guida alla sicurezza*.
- 3 In VMware Cloud Director Service Provider Admin Portal, aggiungere il criterio abilitato per la crittografia a un VDC del provider. Vedere [Aggiunta di un criterio di storage della macchina virtuale in un virtual data center del provider](#).
- 4 In VMware Cloud Director Service Provider Admin Portal, aggiungere il criterio abilitato per la crittografia a un VDC dell'organizzazione. Vedere [Aggiunta di un criterio di storage della macchina virtuale a un virtual data center dell'organizzazione](#).
- 5 In VMware Cloud Director Tenant Portal, i tenant possono associare la macchina virtuale o il disco a un criterio di storage in cui sia abilitata la crittografia della macchina virtuale.
- 6 Per decrittografare una macchina virtuale o un disco, i tenant possono associare la macchina virtuale o il disco a un criterio di storage in cui la crittografia non sia abilitata.

Limitazioni della crittografia della macchina virtuale

Le seguenti azioni non sono supportate in VMware Cloud Director 10.1.

- 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. Gli **autori di vApp** possono visualizzare lo stato di crittografia delle macchine virtuali e dei dischi. Per ulteriori informazioni su questi ruoli e diritti, vedere [Ruoli predefiniti e relativi diritti](#).

È possibile visualizzare tutte le funzionalità di storage nella colonna **Funzionalità** in **Risorse > Risorse vSphere > Criteri di storage**. In questa colonna vengono visualizzate la crittografia della macchina virtuale, l'associazione basata su tag, vSAN e le operazioni IOPS che limitano le capacità di storage. Per visualizzare l'elenco completo delle capacità di storage, espandere la riga facendo clic sulla freccia a sinistra del nome del criterio di storage.

Le informazioni sulla capacità di storage possono essere visualizzate anche nella scheda **Criteri di storage** di un VDC del provider.

Aggiunta di un criterio di storage della macchina virtuale in un virtual data center del provider

È possibile aggiungere un criterio di storage della macchina virtuale in un virtual data center del provider, quindi configurare i virtual data center dell'organizzazione supportati da questo virtual data center del provider in modo che supportino il criterio di storage aggiunto.

Prerequisiti

- L'amministratore di vSphere ha creato il criterio di storage della macchina virtuale di destinazione. Per informazioni sulla gestione basata sui criteri di storage (SPBM), consultare la documentazione relativa allo *storage vSphere*.
- [Aggiornamento dei criteri di storage di un'istanza di vCenter Server](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Nella scheda **Criteri di storage**, fare clic su **Aggiungi**.
- 4 Selezionare uno o più criteri di storage da aggiungere e fare clic su **Aggiungi**.

Se si seleziona * (**qualsiasi**), VMware Cloud Director aggiunge e rimuove dinamicamente gli archivi dati quando vengono aggiunti o rimossi dai cluster dell'archivio dati del virtual data center del provider.

Operazioni successive

Configurare i virtual data center dell'organizzazione supportati dal virtual data center del provider per supportare il criterio di storage. Vedere [Aggiunta di un criterio di storage della macchina virtuale a un virtual data center dell'organizzazione](#).

Abilitazione o disabilitazione di un criterio di storage della macchina virtuale in un virtual data center del provider

Quando si disabilita un criterio di storage della macchina virtuale in un virtual data center del provider, i virtual data center dell'organizzazione non possono più utilizzare il criterio di storage della macchina virtuale.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Criteri di storage**.

- 4 Fare clic sul pulsante di opzione accanto al criterio di storage della macchina virtuale di destinazione e scegliere **Abilita** o **Disabilita**.
- 5 Per confermare, fare clic su **OK**.

Eliminazione di un criterio di storage della macchina virtuale da un virtual data center del provider

È possibile eliminare un criterio di storage della macchina virtuale da un virtual data center del provider.

Prerequisiti

Disabilitare il criterio di storage della macchina virtuale di destinazione. Vedere [Abilitazione o disabilitazione di un criterio di storage della macchina virtuale in un virtual data center del provider](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Criteri di storage**.
- 4 Fare clic sul pulsante di opzione accanto al criterio di storage della macchina virtuale di destinazione e fare clic su **Rimuovi**.
- 5 Per confermare, fare clic su **Rimuovi**.

Modifica dei metadati per un criterio di storage della macchina virtuale in un virtual data center del provider

È possibile aggiungere, modificare ed eliminare metadati per un criterio di storage in un virtual data center del provider.

Utilizzando i metadati degli oggetti, è possibile associare coppie *name=value* definite dall'utente a un criterio di storage su un virtual data center del provider. È possibile utilizzare i metadati degli oggetti nelle espressioni di filtro delle query dell'API di vCloud.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Criteri di storage**.
- 4 Fare clic sul pulsante di opzione accanto al criterio di storage della macchina virtuale di destinazione e fare clic su **Metadati**.
- 5 Fare clic su **Modifica**.

- 6 (Facoltativo) Per aggiungere una coppia chiave-valore, fare clic su **Aggiungi**, immettere un nome e un valore e selezionare un tipo per la nuova coppia chiave-valore.
- 7 (Facoltativo) Per modificare una coppia chiave-valore, immettere un nuovo nome e un valore e selezionare un nuovo tipo per la coppia chiave-valore.
- 8 (Facoltativo) Per rimuovere una coppia chiave-valore, a destra della riga corrispondente, fare clic sull'icona **Elimina**.
- 9 Fare clic su **Salva** e fare clic su **OK**.

Abilitazione dell'impostazione delle operazioni di I/O al secondo

È possibile abilitare l'impostazione delle operazioni di I/O al secondo (IOPS) per un criterio di storage in modo che i tenant possano impostare limiti di IOPS per disco.

Le prestazioni di lettura/scrittura gestite nei dispositivi di storage fisico e nei dischi virtuali sono espresse in unità denominate IOPS, che misurano le operazioni di lettura/scrittura al secondo. Per limitare le prestazioni di I/O, un criterio di storage del VDC del provider che include dispositivi di storage con l'allocazione IOPS abilitata deve supportare un criterio di storage del VDC dell'organizzazione. In seguito, un tenant può configurare i dischi che lo utilizzano per richiedere un livello specifico di prestazioni di I/O. Un profilo di storage configurato con il supporto IOPS fornisce il valore IOPS predefinito a tutti i dischi che lo utilizzano. Ciò include dischi che non sono configurati per richiedere un valore IOPS specifico. Un disco rigido configurato per richiedere un valore IOPS specifico non può utilizzare un criterio di storage il cui valore IOPS massimo sia inferiore al valore richiesto o un profilo di storage che non sia configurato con il supporto IOPS.

Nota La velocità effettiva di I/O delle macchine virtuali è una combinazione di dimensioni di blocco e IOPS. Se le macchine virtuali utilizzano dimensioni di blocco diverse, la loro velocità effettiva sarà diversa, anche se il limite del numero di IOPS è lo stesso. Per ulteriori informazioni sulla gestione delle risorse di I/O di storage, vedere la guida *Gestione delle risorse di vSphere*.

- 1 In vCenter Server, aggiungere capacità IOPS a uno o più archivi dati.
- 2 In vCenter Server, creare un criterio di storage che utilizzi gli archivi dati con capacità IOPS aggiuntive.
- 3 Utilizzando l'API di VMware Cloud Director Service Provider Admin Portal o VMware Cloud Director, aggiungere il criterio di storage a uno o più VDC del provider.
- 4 Utilizzando l'API di Service Provider Admin Portal o VMware Cloud Director, pubblicare il criterio di storage in uno o più VDC dell'organizzazione.
- 5 Utilizzando l'API di VMware Cloud Director, aggiornare il criterio di storage del VDC dell'organizzazione per abilitare la limitazione del numero di IOPS e impostare il valore massimo di IOPS, il valore predefinito di IOPS e così via.

È possibile abilitare la limitazione del numero di IOPS in un criterio di storage esistente.

- 1 In vCenter Server, aggiungere capacità IOPS a tutti gli archivi dati associati al criterio di storage che si desidera modificare.

- 2 Utilizzando il VMware Cloud Director Service Provider Admin Portal o l'API di VMware Cloud Director, verificare che il criterio di storage del VDC del provider corrispondente indichi che la capacità IOPS è diversa da zero.
- 3 Utilizzando l'API di VMware Cloud Director, aggiornare il criterio di storage del VDC dell'organizzazione per abilitare la limitazione del numero di IOPS e impostare il valore massimo di IOPS, il valore predefinito di IOPS e così via.

Quando si abilita la limitazione del numero di IOPS per il criterio di storage di un VDC dell'organizzazione, i tenant possono utilizzare il VMware Cloud Director Tenant Portal per impostare i limiti di IOPS per disco.

Gestione dei pool di risorse in un virtual data center del provider

È possibile aggiungere, abilitare, disabilitare e scollegare i pool di risorse secondari da un virtual data center del provider. Non è possibile disabilitare o scollegare il pool di risorse primario in un virtual data center del provider.

Aggiunta di un pool di risorse a un virtual data center del provider

È possibile aggiungere uno o più pool di risorse secondari a un virtual data center del provider, in modo da espandere i virtual data center dell'organizzazione Pay-As-You-Go e Pool di allocazioni.

Quando sono supportate da più pool di risorse, le risorse di calcolo possono espandersi per includere più macchine virtuali.

È possibile aggiungere pool di risorse supportati da cluster di vSphere configurati in modo ottimale per l'hosting di istanze di NSX Edge che dispongono di uplink VLAN. VMware Cloud Director può utilizzare metadati per indicare che il sistema deve collocare i gateway edge del VDC dell'organizzazione in pool di risorse supportati da tali cluster. Per ulteriori informazioni, consultare l'articolo della Knowledge Base di VMware all'indirizzo <https://kb.vmware.com/kb/2151398>.

Prerequisiti

L'amministratore di vSphere ha creato il pool di risorse secondario di destinazione nell'istanza di vCenter Server che supporta il pool di risorse primario del virtual data center del provider.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Nella scheda **Pool di risorse**, fare clic su **Aggiungi**.
- 4 Selezionare uno o più pool di risorse da aggiungere e fare clic su **Aggiungi**.

Risultati

VMware Cloud Director aggiunge il pool di risorse per il virtual data center del provider rendendo elastici tutti i virtual data center dell'organizzazione Pay-As-You-Go e Pool di allocazioni supportati dal virtual data center del provider.

VMware Cloud Director aggiunge anche un pool di risorse del VDC di sistema al di sotto del nuovo pool di risorse. Questo pool di risorse viene utilizzato per la creazione di risorse di sistema come macchine virtuali e macchine virtuali NSX Edge che fungono da modello per i cloni collegati.

Importante Non modificare o eliminare il pool di risorse del VDC di sistema.

Abilitazione o disabilitazione di un pool di risorse in un virtual data center del provider

Quando si disabilita un pool di risorse, le risorse di memoria ed elaborazione del pool di risorse non possono più essere utilizzate dal virtual data center del provider

I processi già in corso non interrompono l'utilizzo delle risorse del pool di risorse disabilitato.

Nota Non è possibile disabilitare il pool di risorse primario in un virtual data center del provider.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Pool di risorse**.
- 4 Fare clic sul pulsante di opzione accanto al pool di risorse di destinazione e scegliere **Abilita** o **Disabilita**.
- 5 Per confermare, fare clic su **OK**.

Scollegamento di un pool di risorse da un virtual data center del provider

Se un virtual data center del provider dispone di più di un pool di risorse, è possibile scollegare un pool di risorse dal virtual data center del provider. Non è possibile scollegare il pool di risorse primario dal virtual data center del provider.

Prerequisiti

- Disabilitare il pool di risorse di destinazione nel virtual data center del provider. Vedere [Abilitazione o disabilitazione di un pool di risorse in un virtual data center del provider](#).
- Ridistribuire le reti interessate dal pool di risorse disabilitato.
- Ridistribuire i gateway Edge interessati dal pool di risorse disabilitato.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Pool di risorse**.
- 4 Selezionare il pulsante di opzione accanto al pool di risorse di destinazione e fare clic su **Scollega**.
- 5 Per confermare, fare clic su **OK**.

Modifica dei metadati per un virtual data center del provider

È possibile aggiungere, modificare ed eliminare i metadati per un virtual data center del provider.

Utilizzando i metadati degli oggetti, è possibile associare coppie *nome=valore* a un virtual data center del provider. È possibile utilizzare i metadati degli oggetti nelle espressioni di filtro delle query API di vCloud.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Nell'angolo superiore destro della scheda **Configura > Metadati**, fare clic su **Modifica**.
- 4 (Facoltativo) Per aggiungere una coppia chiave-valore, fare clic su **Aggiungi**, immettere un nome e un valore e selezionare un tipo per la nuova coppia chiave-valore.
- 5 (Facoltativo) Per modificare una coppia chiave-valore, immettere un nuovo nome e un valore e selezionare un nuovo tipo per la coppia chiave-valore.
- 6 (Facoltativo) Per rimuovere una coppia chiave-valore, a destra della riga corrispondente, fare clic sull'icona **Elimina**.
- 7 Fare clic su **Salva** e fare clic su **OK**.

Gestione delle organizzazioni

5

VMware Cloud Director Service Provider Admin Portal consente di creare, configurare e gestire organizzazioni VMware Cloud Director.

Utilizzare VMware Cloud Director Service Provider Admin Portal per gestire le organizzazioni, impostare i criteri per determinare come gli utenti utilizzano le risorse allocate a un'organizzazione e gestire la pubblicazione e la condivisione dei cataloghi.

Questo capitolo include i seguenti argomenti:

- [Informazioni generali sui lease](#)
- [Creazione di un'organizzazione](#)
- [Abilitazione o disabilitazione di un'organizzazione](#)
- [Eliminazione di un'organizzazione](#)
- [Configurazione dei cataloghi di un'organizzazione](#)
- [Configurazione dei criteri di un'organizzazione](#)
- [Migra storage tenant](#)

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.

Creazione di un'organizzazione

È possibile creare una nuova organizzazione da VMware Cloud Director Service Provider Admin Portal.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.

a Dal riquadro sinistro, selezionare **Organizzazioni**.

Viene mostrato l'elenco delle organizzazioni esistenti in una visualizzazione griglia.

- 2 Fare clic su **Nuovo**.

Si apre la finestra di dialogo **Nuova organizzazione**.

- 3 Immettere i valori seguenti.

Opzione	Descrizione
Nome organizzazione	L'identificatore univoco che costituisce l'URL per accedere al portale tenant dell'organizzazione.
Nome completo organizzazione	Il nome completo dell'organizzazione.
Descrizione	Descrizione facoltativa dell'organizzazione.

- 4 Fare clic sul pulsante **Crea** per completare la creazione.

Abilitazione o disabilitazione di un'organizzazione

La disabilitazione di un'organizzazione impedisce agli utenti di effettuare l'accesso all'organizzazione e termina le sessioni degli utenti attualmente connessi. Le vApp in esecuzione nell'organizzazione non vengono interrotte.

Un **amministratore di sistema** può allocare risorse, aggiungere reti e così via, anche dopo la disabilitazione di un'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.

a Dal riquadro sinistro, selezionare **Organizzazioni**.

Viene mostrato l'elenco delle organizzazioni esistenti in una visualizzazione griglia.

- 2 Fare clic sul pulsante di opzione accanto al nome dell'organizzazione, quindi fare clic su **Abilita** o **Disabilita**.

Eliminazione di un'organizzazione

Eliminare un'organizzazione per rimuoverla definitivamente da VMware Cloud Director.

Prerequisiti

Prima di poter eliminare un'organizzazione, è necessario disabilitarla ed eliminare tutti i virtual data center, i modelli, i file multimediali e le vApp dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - a Dal riquadro sinistro, selezionare **Organizzazioni**.
Viene mostrato l'elenco delle organizzazioni esistenti in una visualizzazione griglia.
- 2 Fare clic sul pulsante di opzione accanto al nome dell'organizzazione, quindi fare clic su **Elimina**.
- 3 Per confermare, fare clic su **Sì**.

Configurazione dei cataloghi di un'organizzazione

È possibile configurare il modo in cui un'organizzazione condivide i suoi cataloghi di servizi.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - a Dal riquadro sinistro, selezionare **Organizzazioni**.
Viene mostrato l'elenco delle organizzazioni esistenti in una visualizzazione griglia.
- 2 Selezionare un'organizzazione e nella scheda **Configura** selezionare **Catalogo**.
- 3 Per modificare le impostazioni di condivisione e pubblicazione, fare clic su **Modifica**.

Opzione	Descrizione
Condivisione	Consente agli amministratori dell'organizzazione di condividere i cataloghi dell'organizzazione con altre organizzazioni in questa istanza di VMware Cloud Director. Se non si seleziona quest'opzione, gli amministratori dell'organizzazione sono ancora in grado di condividere i cataloghi all'interno dell'organizzazione.
Consenti la pubblicazione su cataloghi esterni	Consente agli amministratori dell'organizzazione di pubblicare i cataloghi nelle organizzazioni esterne a questa istanza di VMware Cloud Director.
Consenti la sottoscrizione a cataloghi esterni	Consente agli amministratori dell'organizzazione di sottoscrivere cataloghi esterni di questa istanza di VMware Cloud Director.

Configurazione dei criteri di un'organizzazione

I lease, le quote e i limiti impongono dei vincoli sull'utilizzo delle risorse di storage e di elaborazione da parte degli utenti di un'organizzazione. È possibile modificare tali impostazioni per impedire che gli utenti esauriscano o monopolizzino le risorse di un'organizzazione.

Prerequisiti

Vedere [Informazioni generali sui lease](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.

a Dal riquadro sinistro, selezionare **Organizzazioni**.

Viene mostrato l'elenco delle organizzazioni esistenti in una visualizzazione griglia.

- 2 Selezionare un'organizzazione e fare clic sulla scheda **Criteri**.
- 3 Fare clic su **Modifica** per modificare lease, quote, limiti delle risorse e criteri delle password per l'organizzazione.
- 4 Configurare i lease delle vApp con le seguenti impostazioni.

Opzione	Descrizione
Lease di runtime massimo	Indica per quanto tempo è possibile eseguire le vApp prima che vengano arrestate automaticamente.
Azione scadenza runtime	Modalità di elaborazione delle vApp in esecuzione scadute. La sospensione di una vApp comporta anche la sospensione di tutte le relative macchine virtuali e mantiene lo stato corrente scrivendo la memoria sul disco. Disattiva consente di arrestare immediatamente tutte le relative macchine virtuali e vApp secondarie.
Lease dello storage massimo	Indica per quanto tempo le vApp arrestate risultano disponibili prima di essere eliminate automaticamente.
Pulizia dello storage	Indica come vengono elaborate le vApp dopo che sono state arrestate e pulite.

- 5 Configurare i lease dei modelli di vApp con le seguenti impostazioni.

Opzione	Descrizione
Lease dello storage massimo	Indica per quanto tempo i modelli di vApp risultano disponibili prima di essere eliminati automaticamente.
Pulizia dello storage	Indica il modo in cui vengono elaborati i modelli di vApp dopo che sono stati puliti.

- 6 Configurare le quote con le impostazioni seguenti.

Opzione	Descrizione
Quota di tutte le macchine virtuali	Numero totale di macchine virtuali disponibili che un utente può archiviare in questa organizzazione.
Quota macchine virtuali in esecuzione	Numero totale di macchine virtuali che un utente può accendere in questa organizzazione.

7 Configurare i limiti con le impostazioni seguenti.

Opzione	Descrizione
Numero di operazioni che utilizzano molte risorse per utente	Digitare il numero massimo di operazioni simultanee che utilizzano molte risorse per utente o selezionare Eredita limite di sistema .
Numero di operazioni che utilizzano molte risorse da inserire in coda per utente	Digitare il numero massimo di operazioni che utilizzano molte risorse da inserire in coda per utente o selezionare Eredita limite di sistema .
Numero di operazioni che utilizzano molte risorse per organizzazione	Digitare il numero massimo di operazioni simultanee che utilizzano molte risorse per organizzazione o selezionare Eredita limite di sistema .
Numero di operazioni che utilizzano molte risorse da inserire in coda per organizzazione	Digitare il numero massimo di operazioni che utilizzano molte risorse da inserire in coda per organizzazione o selezionare Eredita limite di sistema .
Numero di connessioni simultanee per macchina virtuale	Digitare il numero massimo di connessioni simultanee della console per macchina virtuale o selezionare Eredita limite di sistema .
Numero di virtual data center per organizzazione	Digitare il numero massimo di virtual data center per organizzazione o selezionare Eredita quota di sistema .

8 Configurare i criteri delle password con le seguenti impostazioni.

Opzione	Descrizione
Blocco account abilitato	Abilita il blocco degli account utente dopo un determinato numero di tentativi di accesso non validi.
Login non validi prima del blocco	Numero di tentativi di accesso non validi prima che l'account utente venga bloccato.
Intervallo blocco account	Periodo durante il quale un account utente bloccato non può accedere.

Migra storage tenant

È possibile migrare tutte le vApp, i dischi indipendenti e gli elementi del catalogo di una o più organizzazioni da uno o più archivi dati ad altri archivi dati.

Prima di rimuovere un archivio dati, è necessario migrare tutti gli elementi contenuti nell'archivio dati in un nuovo archivio dati. È inoltre possibile effettuare la migrazione di un'organizzazione in un nuovo archivio dati con una capacità di storage maggiore o che utilizza una tecnologia di storage più recente, come VMware vSAN.

Importante La migrazione dello storage tenant è un'operazione che richiede l'utilizzo di molte risorse e che può durare molto tempo, in particolare nel caso in cui siano presenti molti asset di cui effettuare la migrazione. Per ulteriori informazioni sulla migrazione dello storage tenant, vedere <https://kb.vmware.com/kb/2151086>.

Prerequisiti

- Determinare i criteri di storage utilizzati dai VDC delle organizzazioni di destinazione. Vedere [Aggiunta di un criterio di storage della macchina virtuale a un virtual data center dell'organizzazione](#).

- Per ogni criterio di storage contenente un archivio dati di origine di cui si desidera eseguire la migrazione, verificare che sia presente almeno un archivio dati di destinazione verso cui eseguire la migrazione. È possibile creare archivi dati di destinazione o utilizzare quelli esistenti. Per ulteriori informazioni su come determinare gli archivi dati nei criteri di storage utilizzati dalle organizzazioni di destinazione, vedere la documentazione relativa allo *storage vSphere*.

Procedura

- 1 Accedere a VMware Cloud Director Service Provider Admin Portal come **amministratore di sistema** o con un ruolo che disponga del diritto **Organizzazione: Migra storage tenant**.
- 2 Avviare la procedura guidata **Migra storage tenant**.
 - In **Risorse cloud**, selezionare **Organizzazioni** e fare clic su **Migra storage tenant**.
 - In **Risorse vSphere**, selezionare **Archivi dati** e fare clic su **Migra storage tenant**.
- 3 Selezionare una o più organizzazioni con elementi di storage di cui si desidera eseguire la migrazione e fare clic su **Avanti**.
- 4 Selezionare uno o più archivi dati di origine di cui eseguire la migrazione e fare clic su **Avanti**.
Nella procedura guidata viene visualizzato l'elenco di tutti gli archivi dati presenti nel sistema.
- 5 Selezionare uno o più archivi dati di destinazione e fare clic su **Avanti**.
- 6 Rivedere i contenuti della pagina **Pronto per il completamento** e fare clic su **Fine** per avviare la migrazione.

Gestione dei virtual data center dell'organizzazione

6

Per fornire risorse a un'organizzazione, è possibile creare uno o più virtual data center per tale organizzazione. Dopo aver creato un virtual data center dell'organizzazione, è possibile modificarne le proprietà, disabilitarlo o eliminarlo e gestirne le impostazioni del modello di allocazione, di storage e di rete.

Questo capitolo include i seguenti argomenti:

- Informazioni sui modelli di allocazione
- Informazioni sul dimensionamento delle macchine virtuali e sui criteri di posizionamento delle macchine virtuali
- Creazione di un virtual data center dell'organizzazione
- Abilitazione o disabilitazione di un virtual data center dell'organizzazione
- Eliminazione di un virtual data center dell'organizzazione
- Modifica del nome e della descrizione del virtual data center dell'organizzazione
- Modifica delle impostazioni del modello di allocazione di un virtual data center dell'organizzazione
- Modifica delle impostazioni di storage di un virtual data center dell'organizzazione
- Modifica delle impostazioni di rete di un virtual data center dell'organizzazione
- Configurazione di servizi di rete inter-VDC
- Modifica dei metadati per un virtual data center dell'organizzazione
- Visualizzazione dei pool di risorse di un virtual data center dell'organizzazione
- Gestione del firewall distribuito in un virtual data center dell'organizzazione

Informazioni sui modelli di allocazione

Un modello di allocazione determina come e quando le risorse di calcolo e di memoria del virtual data center (VDC) del provider allocate vengono sottoposte a commit nel VDC dell'organizzazione.

Nella tabella seguente sono illustrate le impostazioni di distribuzione delle risorse di vSphere a livello della macchina virtuale (VM) o del pool di risorse in base al modello di allocazione del VDC dell'organizzazione.

	Modello di allocazione Flex	Modello di pool di allocazioni elastico	Modello di pool di allocazioni non elastico	Modello Pay-As-You-Go	Modello del pool di prenotazioni
Elastico	Basato sulla configurazione del VDC dell'organizzazione.	Sì	No	Sì	No
Velocità vCPU	Se in un criterio di dimensionamento della macchina virtuale non è definito alcun limite della CPU della macchina virtuale, la velocità di vCPU potrebbe influire sul limite della CPU della macchina virtuale nel VDC.	Influisce sul numero di vCPU in esecuzione nel VDC dell'organizzazione.	Non applicabile	Influisce sul limite della CPU della macchina virtuale	Non applicabile
Limite della CPU del pool di risorse	Limite della CPU del VDC dell'organizzazione ripartito in base al numero di macchine virtuali nel pool di risorse.	Allocazione CPU del VDC dell'organizzazione	Allocazione CPU del VDC dell'organizzazione	Illimitato	Allocazione CPU del VDC dell'organizzazione
Prenotazione CPU del pool di risorse	La prenotazione della CPU del VDC dell'organizzazione è ripartita in base al numero di vCPU nel pool di risorse. La prenotazione della CPU del VDC dell'organizzazione è uguale all'allocazione della CPU del VDC dell'organizzazione moltiplicata per la garanzia della CPU.	Somma delle macchine virtuali attive e corrisponde alla garanzia della CPU moltiplicata per la velocità della vCPU e per il numero di vCPU.	Allocazione CPU del VDC dell'organizzazione moltiplicata per la garanzia della CPU	Nessuna, espandibile	Allocazione CPU del VDC dell'organizzazione
Limite di memoria del pool di risorse	Il limite di memoria del VDC dell'organizzazione è ripartito in base al numero di macchine virtuali nel pool di risorse.	Illimitato	Allocazione RAM del VDC dell'organizzazione	Illimitato	Allocazione RAM del VDC dell'organizzazione

	Modello di allocazione Flex	Modello di pool di allocazioni elastico	Modello di pool di allocazioni non elastico	Modello Pay-As-You-Go	Modello del pool di prenotazioni
Prenotazione della memoria del pool di risorse	La prenotazione della RAM del VDC dell'organizzazione è ripartita in base al numero di macchine virtuali nel pool di risorse. La prenotazione della RAM del VDC dell'organizzazione è uguale all'allocazione della RAM del VDC dell'organizzazione moltiplicata per la garanzia della RAM.	Somma della garanzia della RAM moltiplicata per la vRAM di tutte le macchine virtuali attivate nel pool di risorse. La prenotazione della RAM del pool di risorse è espandibile.	Allocazione della RAM del VDC dell'organizzazione moltiplicata per la garanzia della RAM	Nessuna, espandibile	Allocazione RAM del VDC dell'organizzazione
Limite CPU della macchina virtuale	Basato sul criterio di dimensionamento della macchina virtuale.	Illimitato	Illimitato	Velocità di vCPU per il numero di vCPU	Ad hoc
Prenotazione CPU della macchina virtuale	Basato sul criterio di dimensionamento della macchina virtuale.	0	0	È uguale alla velocità della CPU moltiplicata per la velocità della vCPU e per il numero di vCPU.	Ad hoc
Limite RAM della macchina virtuale	Basato sul criterio di dimensionamento della macchina virtuale.	Illimitato	Illimitato	vRAM	Ad hoc
Prenotazione RAM della macchina virtuale	Basato sul criterio di dimensionamento della macchina virtuale.	0	È uguale alla vRAM moltiplicata per la garanzia della RAM più il sovraccarico della RAM.	È uguale alla vRAM moltiplicata per la garanzia della RAM più il sovraccarico della RAM.	Ad hoc

Conversione di un modello di allocazione VDC legacy in un modello di allocazione Flex

È possibile aggiungere un criterio di dimensionamento della macchina virtuale e del posizionamento di una macchina virtuale a un VDC con un modello di pool di allocazione elastico, un modello di pool di allocazione non elastico, un modello pay-as-you-go o un modello di pool di prenotazioni. Se il criterio di posizionamento della macchina virtuale o di dimensionamento della macchina virtuale non è compatibile con il modello di allocazione del VDC esistente, è possibile decidere di convertire il VDC in un VDC dell'organizzazione Flex.

Conformità del criterio della macchina virtuale

La conversione del VDC legacy non causa la mancata conformità della macchina virtuale. Se un amministratore modifica i valori di elaborazione della macchina virtuale o l'appartenenza al gruppo di macchine virtuali di una macchina virtuale direttamente nell'istanza di vCenter Server, una macchina virtuale può diventare non conforme al dimensionamento della macchina virtuale o al criterio di posizionamento della macchina virtuale assegnato. Una macchina virtuale può anche diventare non conforme se un utente con i privilegi necessari modifica la prenotazione della macchina virtuale e limita i valori utilizzando l'API di vCloud. Se è presente una macchina virtuale non conforme, l'interfaccia utente di VMware Cloud Director Tenant Portal visualizza un messaggio di avviso. Il tenant può visualizzare informazioni dettagliate sulla causa della mancata conformità e può rendere la macchina virtuale nuovamente conforme, il che riapplica i criteri alla macchina virtuale.

Utilizzo consigliato per i modelli di allocazione

Ogni modello di allocazione può essere utilizzato per diversi livelli di controllo e gestione delle prestazioni.

La seguente tabella contiene informazioni sull'utilizzo consigliato per ciascun modello di allocazione.

Modello di allocazione	Utilizzo consigliato
Modello di allocazione Flex	Con il modello di allocazione Flex è possibile raggiungere un controllo delle prestazioni con granularità fine a livello del carico di lavoro. Con il modello di allocazione Flex, gli amministratori di sistema di VMware Cloud Director possono gestire l'elasticità dei singoli VDC dell'organizzazione. Il modello di allocazione Flex utilizza la gestione basata su criteri dei carichi di lavoro. Con il modello di allocazione Flex, i provider di cloud possono avere un maggiore controllo sull'overhead della memoria in un VDC dell'organizzazione e possono imporre un utilizzo della capacità di burst rigoroso per i tenant.
Modello di allocazione del pool di allocazioni	Utilizzare il modello di allocazione del pool di allocazioni per carichi di lavoro stabili e duraturi, in cui i tenant sottoscrivono un consumo di risorse di calcolo fisso e i provider di cloud possono prevedere e gestire la capacità delle risorse di calcolo. Il modello di allocazione del pool di allocazioni è ottimale per carichi di lavoro con requisiti di prestazioni diversi. Con il modello di allocazione del pool di allocazioni, tutti i carichi di lavoro condividono le risorse allocate dai pool di risorse di vCenter Server. Indipendentemente dal fatto che l'elasticità sia abilitata o disabilitata, i tenant ricevono una quantità limitata di risorse di calcolo. Con il modello di allocazione del pool di allocazioni, i provider di cloud abilitano o disabilitano l'elasticità a livello di sistema e l'impostazione viene applicata a tutti i VDC dell'organizzazione del pool di allocazioni. Se si utilizza l'allocazione del pool di allocazioni non elastico, il VDC dell'organizzazione prenota preventivamente il pool di risorse VDC e i tenant possono eseguire l'overcommit di vCPU ma non possono eseguire l'overcommit della memoria. Se si utilizza l'allocazione del pool elastico, il VDC dell'organizzazione non prenota preventivamente risorse di calcolo e la capacità può estendersi in più cluster. I provider di cloud gestiscono l'overcommit delle risorse di calcolo fisiche e i tenant non possono eseguire l'overcommit di vCPU e memoria.
Pay-As-You-Go	Utilizzare il modello Pay-As-You-Go quando non è necessario allocare risorse di calcolo in vCenter Server in anticipo. La prenotazione, il limite e le condivisioni vengono applicati in ogni carico di lavoro che i tenant distribuiscono nel VDC. Con il modello di allocazione Pay-As-You-Go, ogni carico di lavoro nel VDC dell'organizzazione riceve la stessa percentuale delle risorse di calcolo configurate prenotate. VMware Cloud Director considera uguale la velocità della CPU di ogni vCPU per ogni carico di lavoro ed è possibile definire la velocità della CPU solo a livello di VDC dell'organizzazione. Dal punto di vista delle prestazioni, poiché non è possibile modificare le impostazioni di prenotazione dei carichi di lavoro individuali, ogni carico di lavoro riceve la stessa preferenza. Il modello di allocazione Pay-As-You-Go è ottimale per i tenant che richiedono che in un stesso VDC dell'organizzazione siano in esecuzione carichi di lavoro con requisiti di prestazioni diversi. A causa dell'elasticità, il modello Pay-As-You-Go è adatto per carichi di lavoro generici di breve durata che fanno parte delle applicazioni con ridimensionamento automatico. Con il modello Pay-As-You-Go, i tenant possono rispondere a picchi nella richiesta di risorse di calcolo in un VDC dell'organizzazione.
Pool di prenotazioni	Utilizzare il modello di allocazione del pool di prenotazioni quando è necessario un controllo a granularità fine sulle prestazioni dei carichi di lavoro in esecuzione nel VDC dell'organizzazione. Dal punto di vista del provider di cloud , il modello di allocazione del pool di prenotazioni richiede un'allocazione anticipata di tutte le risorse di calcolo in vCenter Server. Il modello di allocazione del pool di prenotazioni non è elastico. Il modello di allocazione del pool di prenotazioni è ottimale per i carichi di lavoro eseguiti nell'hardware dedicato a un tenant specifico. In questi casi, gli utenti del tenant possono gestire l'uso e l'overcommit delle risorse di calcolo.

Modello di allocazione Flex

A partire da VMware Cloud Director 9.7, gli **amministratori di sistema** possono creare i virtual data center (VDC) dell'organizzazione utilizzando il modello di allocazione Flex. Grazie alla combinazione di criteri di dimensionamento della macchina virtuale e allocazione Flex, gli **amministratori di sistema** possono controllare il consumo di CPU e RAM sia a livello del VDC

sia a livello della singola macchina virtuale. Il modello di allocazione Flex supporta tutte le configurazioni di allocazione disponibili nei modelli di allocazione esistenti.

In VMware Cloud Director 10.0 e versioni successive, tutti i VDC dell'organizzazione non Flex possono essere convertiti in VDC Flex.

Quando si crea un VDC dell'organizzazione Flex, gli **amministratori di sistema** controllano i seguenti parametri del VDC dell'organizzazione:

Parametro	Descrizione
Elasticity	Abilitare o disabilitare la funzionalità del pool elastico.
Include VM Memory Overhead	Includere o escludere l'overhead della memoria in questo VDC. Quando è impostato su true, potrebbe non essere possibile utilizzare la capacità completa del VDC perché l'overhead della memoria di ogni macchina virtuale attivata viene preso anche dalla capacità disponibile del VDC. Se impostato su false, l'overhead della memoria viene preso dal VDC del provider e non dalla capacità allocata del VDC.
CPU allocation	La quantità di CPU allocata a questo VDC in MHz o GHz. L'allocazione della CPU definisce la capacità della CPU del VDC. La CPU totale utilizzata da tutte le macchine virtuali in esecuzione nel VDC non può superare questo valore.
CPU limit	Il limite della CPU definisce la quota della CPU di un VDC. Nella maggior parte dei casi, il limite della CPU è uguale alla capacità CPU allocata del VDC. A volte potrebbe essere necessario non allocare alcuna CPU al VDC, come nel modello pay-as-you-go. In questo caso, è necessario impostare una quota sul consumo complessivo della CPU impostando l'allocazione della CPU su zero e il limite della CPU su un valore diverso da zero. È inoltre possibile utilizzare questa impostazione per consentire una quota di CPU illimitata. Se viene scelta un'impostazione illimitata, i pool di risorse di supporto del VDC in vCenter Server ottengono una CPU illimitata.
CPU resources guaranteed	La percentuale di allocazione della CPU riservata fisicamente al VDC.
vCPU speed	La velocità della vCPU predefinita per le macchine virtuali nel VDC.
Memory allocation	La quantità di memoria allocata a questo VDC in MB o GB. Questo parametro definisce la capacità di memoria totale del VDC. La memoria totale configurata da tutte le macchine virtuali in esecuzione nel VDC non può superare questo valore.
Memory resources guaranteed	La percentuale di allocazione di memoria fisicamente riservata per il VDC.
Maximum number of VMs	Il numero massimo di macchine virtuali nel VDC.

L'**amministratore di sistema di VMware Cloud Director** può configurare un VDC dell'organizzazione Flex in modo che sia elastico o non elastico. Quando nei VDC dell'organizzazione Flex la funzionalità del pool elastico è abilitata, il VDC dell'organizzazione si estende e utilizza tutti i pool di risorse associati al relativo VDC del provider. In VMware Cloud Director 9.7, se si converte un VDC dell'organizzazione non elastico in un VDC dell'organizzazione elastico, non è possibile convertire nuovamente lo stesso VDC dell'organizzazione in un VDC non elastico.

Il modello di allocazione Flex supporta le funzionalità dei criteri di dimensionamento della macchina virtuale senza i vincoli degli altri modelli di allocazione. Nel modello di allocazione Flex, l'allocazione delle risorse di calcolo della macchina virtuale dipende dai criteri di dimensionamento della macchina virtuale. Se non si definisce un criterio di dimensionamento della macchina virtuale per un VDC dell'organizzazione, l'allocazione delle risorse di calcolo dipende dal modello di allocazione del VDC dell'organizzazione. Utilizzando la combinazione del modello di allocazione Flex e dei criteri di dimensionamento della macchina virtuale dell'organizzazione, un singolo VDC dell'organizzazione può ospitare macchine virtuali che utilizzano la configurazione comune per tutti gli altri modelli di allocazione. Per ulteriori informazioni, vedere [Informazioni sul dimensionamento delle macchine virtuali e sui criteri di posizionamento delle macchine virtuali](#).

Per creare un VDC dell'organizzazione Flex, è possibile utilizzare VMware Cloud Director Service Provider Admin Portal o l'API vCloud. Per ulteriori informazioni sull'API vCloud, vedere *Guida alla programmazione dell'API di VMware Cloud Director*.

Modello di allocazione del pool di allocazioni

Con il modello di allocazione del pool di allocazioni, una percentuale delle risorse allocate dal virtual data center (VDC) del provider viene sottoposta a commit nel VDC dell'organizzazione. È possibile specificare la percentuale per CPU e memoria. Questa percentuale è conosciuta come fattore di garanzia di percentuale e consente di eseguire l'overcommit delle risorse.

L'amministratore di sistema può configurare un VDC dell'organizzazione del pool di allocazioni in modo che sia elastico o non elastico. L'elasticità è un'impostazione globale che influisce su tutti i VDC dell'organizzazione del pool di allocazioni. Vedere [Modifica delle impostazioni generali del sistema](#).

Per impostazione predefinita, i VDC dell'organizzazione del pool di allocazioni hanno un pool di allocazioni elastico abilitato. Per impostazione predefinita, il pool di allocazioni elastico è abilitato nei sistemi aggiornati da VMware Cloud Director 5.1 che dispongono di VDC dell'organizzazione del pool di allocazioni con macchine virtuali estese su più pool di risorse.

Quando per i VDC del pool di allocazioni è abilitata la funzionalità del pool di allocazioni elastico, il VDC dell'organizzazione utilizza e si estende su tutti i pool di risorse associati al relativo VDC del provider. Di conseguenza, la frequenza di vCPU è adesso un parametro obbligatorio per un pool di allocazioni.

Impostare la frequenza di vCPU e il fattore di garanzia di percentuale in modo che sia possibile distribuire macchine virtuali sufficienti nel VDC dell'organizzazione senza che la CPU costituisca un fattore di impedimento.

Quando viene creata una macchina virtuale, il motore di posizionamento la colloca nel pool di risorse del VDC del provider più compatibile con i requisiti della macchina virtuale. Per questo VDC dell'organizzazione viene creato un pool di sottorisorse nel pool di risorse del VDC del provider e la macchina virtuale viene posizionata in tale pool di risorse secondarie.

Quando la macchina virtuale viene attivata, il motore di posizionamento controlla il pool di risorse del VDC del provider per verificare che sia ancora in grado di attivare la macchina virtuale. In caso contrario, il motore di posizionamento trasferisce la macchina virtuale a un pool di risorse del VDC del provider più risorse sufficienti a eseguire la macchina virtuale. Se non esiste già, viene creato un pool di sottorisorse per il VDC dell'organizzazione.

Il pool di sottorisorse è configurato con risorse sufficienti per eseguire la nuova macchina virtuale. La prenotazione della memoria del pool di sottorisorse viene aumentata del valore che si ottiene moltiplicando la dimensione della memoria configurata per la macchina virtuale per il fattore di garanzia di percentuale per il VDC dell'organizzazione. La prenotazione della CPU del pool di sottorisorse viene aumentata del valore che si ottiene moltiplicando il numero di vCPU configurate per la macchina virtuale per il numero di vCPU specificate a livello del VDC dell'organizzazione per il fattore di garanzia di percentuale per la CPU impostata a livello del VDC dell'organizzazione. Se è abilitata la funzionalità del pool di allocazioni elastico, il limite di memoria del pool di sottorisorse viene aumentato in base alla dimensione della memoria configurata per la macchina virtuale, mentre il limite di CPU del pool di sottorisorse viene aumentato del valore che si ottiene moltiplicando il numero di vCPU con cui è configurata la macchina virtuale per la frequenza di vCPU specificata a livello del VDC dell'organizzazione. La macchina virtuale viene riconfigurata per impostare la memoria e la prenotazione di CPU su zero e il motore di posizionamento la colloca in un pool di risorse del VDC del provider.

Con il modello del pool di allocazioni elastico, i limiti vengono monitorati e gestiti solo da VMware Cloud Director. Se la funzionalità elastica è disabilitata, viene impostato anche il limite del pool di risorse.

Il vantaggio del modello basato su pool di allocazioni è che la macchina virtuale può sfruttare le risorse di una macchina virtuale non utilizzata sullo stesso pool di sottorisorse. Questo modello consente di sfruttare le nuove risorse aggiunte al VDC del provider.

In rari casi, durante l'attivazione, a causa della mancanza di risorse nel pool originale, una macchina virtuale può essere trasferita dal pool di risorse a cui è stata assegnata al momento della creazione a un pool di risorse diverso. La modifica dei file della macchina virtuale a un nuovo pool di risorse può richiedere un costo minore.

Quando la funzionalità del pool di allocazioni elastico è disabilitata, il comportamento dei VDC dell'organizzazione del pool di allocazioni è simile al modello del pool di allocazioni di VMware Cloud Director 1.5. In questo modello, la frequenza di vCPU non è configurabile. L'overcommit è controllato mediante l'impostazione della percentuale di risorse garantite.

Per impostazione predefinita, nel VDC del pool di allocazioni, le impostazioni di prenotazione, limite e condivisione delle macchine virtuali vengono recuperate dalle impostazioni del VDC. Per creare o riconfigurare una macchina virtuale con impostazioni di allocazione delle risorse personalizzate per CPU e memoria, è possibile utilizzare l'API vCloud. Vedere *Guida alla programmazione dell'API di VMware Cloud Director*.

Modello di allocazione Pay-As-You-Go

Con il modello di allocazione pay-as-you-go, le risorse vengono sottoposte a commit solo quando gli utenti creano vApps nel VDC dell'organizzazione. È possibile specificare una percentuale di risorse da garantire per consentire l'overcommit delle risorse. È inoltre possibile rendere elastico il VDC di un'organizzazione Pay-As-You-Go aggiungendo più pool di risorse al relativo VDC del provider.

Le risorse sottoposte a commit nell'organizzazione vengono applicate a livello della macchina virtuale.

Quando una macchina virtuale è accesa, se il pool di risorse originale non è in grado di ospitare la macchina virtuale, il motore di posizionamento controlla il pool di risorse e assegna la macchina virtuale a un altro pool di risorse. Se per il pool di risorse non è disponibile alcun pool di sottorisorse, VMware Cloud Director ne crea uno con limite infinito e classificazione zero. La classificazione della macchina virtuale viene impostata sul relativo limite e moltiplicata per le risorse di cui è stato effettuato il commit, quindi il motore della macchina virtuale la posiziona in un pool di risorse del VDC del provider.

Il vantaggio del modello Pay-As-You-Go è che consente l'utilizzo delle nuove risorse aggiunte al VDC del provider.

In rari casi, durante l'attivazione, a causa della mancanza di risorse nel pool originale, una macchina virtuale può passare dal pool di risorse a cui era stata assegnata inizialmente a un pool di risorse diverso. Lo spostamento dei file del disco della macchina virtuale in un nuovo pool di risorse può richiedere un costo minore.

Nel modello pay-as-you-go non vengono riservate risorse in anticipo quindi, se queste non sono sufficienti, una macchina virtuale potrebbe non avviarsi. Le macchine virtuali che adottano questo modello non possono sfruttare le risorse delle macchine virtuali inutilizzate appartenenti allo stesso pool di sottorisorse, poiché le risorse sono impostate a livello della macchina virtuale.

Per impostazione predefinita, in un VDC Pay-As-You-Go, le impostazioni di prenotazione, limite e condivisione delle macchine virtuali vengono recuperate dalle impostazioni del VDC. Per creare o riconfigurare una macchina virtuale con impostazioni di allocazione delle risorse personalizzate per CPU e memoria, è possibile utilizzare l'API vCloud. Vedere *Guida alla programmazione dell'API di VMware Cloud Director*.

Modello di allocazione del pool di prenotazioni

Con il modello di allocazione del pool di prenotazioni, tutte le risorse allocate vengono immediatamente sottoposte a commit nel VDC dell'organizzazione. Gli utenti dell'organizzazione possono controllare l'overcommit specificando le impostazioni di prenotazione, limite e priorità per le singole macchine virtuali.

Poiché questo modello prevede solo un pool di risorse e un pool di sottorisorse, il motore di posizionamento non riassegna il pool di risorse di una macchina virtuale quando questa viene avviata. Il limite e la classificazione della macchina virtuale non sono modificati.

Con il modello basato su pool di prenotazioni, le risorse sono sempre disponibili quando necessario. Il modello consente inoltre di controllare in modo molto preciso la classificazione, il limite e le condivisioni, così da utilizzare in modo ottimizzato le risorse riservate con un'attenta pianificazione. Per informazioni sulla configurazione delle impostazioni di allocazione delle risorse della macchina virtuale nei virtual data center del pool di prenotazioni, vedere *vCloud Air - Guida per gli utenti di Virtual Private Cloud OnDemand*.

In questo modello, la prenotazione avviene sempre presso il cluster principale. Se le risorse per creare un virtual data center dell'organizzazione sul cluster principale sono insufficienti, l'operazione non viene conclusa con successo.

Questo modello, inoltre, non è elastico e gli utenti dell'organizzazione potrebbero impostare condivisioni, classificazioni e limiti non ottimali sulle macchine virtuali, il che comporterebbe l'utilizzo non ottimale delle risorse.

Informazioni sul dimensionamento delle macchine virtuali e sui criteri di posizionamento delle macchine virtuali

È possibile controllare l'allocazione e il posizionamento delle risorse della macchina virtuale in un cluster o un host specifico utilizzando i criteri di dimensionamento e i criteri di posizionamento della macchina virtuale.

VMware Cloud Director 10.0 introduce i concetti di criterio di posizionamento della macchina virtuale e di criterio di dimensionamento della macchina virtuale.

Gli **amministratori di sistema** di VMware Cloud Director creano e gestiscono i criteri di dimensionamento della macchina virtuale a livello globale e possono pubblicare singoli criteri individuali in uno o più VDC dell'organizzazione. I criteri di posizionamento della macchina virtuale vengono creati e gestiti per ciascun VDC del provider, perché un criterio di posizionamento della macchina virtuale ha come ambito il livello del VDC del provider. Quando si pubblica un criterio in un VDC dell'organizzazione, il criterio diventa disponibile per gli utenti dell'organizzazione. Quando si creano e si gestiscono macchine virtuali nel VDC dell'organizzazione, i tenant possono assegnare alle macchine virtuali i criteri disponibili. I tenant e gli utenti nel VDC dell'organizzazione non possono esaminare la configurazione specifica di un criterio di posizionamento o dimensionamento della macchina virtuale.

I criteri di posizionamento e dimensionamento della macchina virtuale sono un meccanismo che consente ai provider di cloud di definire e offrire livelli di servizio differenziati, ad esempio un profilo con utilizzo intensivo della CPU o un profilo con utilizzo della memoria elevato. Se si pubblicano più criteri di dimensionamento e posizionamento della macchina virtuale in un VDC dell'organizzazione, gli utenti del tenant possono scegliere tra tutti i criteri personalizzati e il criterio predefinito durante la creazione e la gestione delle macchine virtuali nel VDC

dell'organizzazione. Il criterio predefinito del sistema viene generato automaticamente per ogni VDC. Gli **Amministratori di sistema** possono eliminare il criterio predefinito del sistema nel VDC e contrassegnare un altro criterio personalizzato come predefinito. Il criterio predefinito non definisce alcun valore e consente tutte le configurazioni della macchina virtuale.

Criterio di posizionamento della macchina virtuale

Un criterio di posizionamento della macchina virtuale definisce il posizionamento di una macchina virtuale in un host o in un gruppo di host. Si tratta di un meccanismo che consente agli **amministratori del provider di cloud** di creare un gruppo di host con nome all'interno di un VDC del provider. Il gruppo di host con nome è un sottoinsieme di host all'interno dei cluster VDC del provider che può essere selezionato in base a qualsiasi criterio, ad esempio i livelli di prestazioni o la licenza. Un criterio di posizionamento della macchina virtuale definisce regole di affinità per l'host della macchina virtuale che incidono direttamente sul posizionamento dei carichi di lavoro del tenant. Gli amministratori definiscono o espongono gruppi di host con nome utilizzando gruppi di macchine virtuali in vCenter Server. Un gruppo di macchine virtuali ha un'affinità diretta con un gruppo di host e rappresenta il gruppo di host con cui ha affinità.

È possibile definire il criterio di posizionamento della macchina virtuale a livello di VDC del provider. Un criterio di posizionamento della macchina virtuale include i seguenti attributi:

- Nome (deve essere univoco nel VDC del provider)
- Descrizione
- Un set di uno o più gruppi di macchine virtuali selezionati dai cluster sottostanti nel VDC del provider. È possibile selezionare un gruppo di macchine virtuali per cluster

Un criterio di posizionamento della macchina virtuale è facoltativo durante la creazione di una macchina virtuale e un tenant può assegnare solo un criterio di posizionamento della macchina virtuale a una macchina virtuale.

Quando un tenant crea una macchina virtuale nel VDC dell'organizzazione e seleziona il criterio di posizionamento della macchina virtuale, VMware Cloud Director aggiunge la macchina virtuale al gruppo di macchine virtuali a cui si fa riferimento nel criterio. Di conseguenza, VMware Cloud Director crea la macchina virtuale nell'host appropriato.

Un criterio di posizionamento della macchina virtuale può avere zero o un gruppo di macchine virtuali da ciascun cluster. Ad esempio, il criterio di posizionamento della macchina virtuale *oracle_license* può comprendere i gruppi di macchine virtuali *oracle_license1* e *oracle_license2*, dove il gruppo di macchine virtuali *oracle_license1* appartiene al cluster *oracle_cluster1* e il gruppo di macchine virtuali *oracle_license2* appartiene al cluster *oracle_cluster2*.

Quando si assegna un criterio di posizionamento della macchina virtuale a una macchina virtuale, il motore di posizionamento aggiunge questa macchina virtuale al gruppo di macchine virtuali corrispondente del cluster in cui si trova. Ad esempio, se si decide di distribuire una macchina virtuale nel cluster *oracle_cluster1* e si assegna il criterio di posizionamento della macchina virtuale *oracle_license* a questa macchina virtuale, il motore di posizionamento aggiunge la macchina virtuale al gruppo di macchine virtuali *oracle_license1*.

Criterio di dimensionamento della macchina virtuale

Un criterio di dimensionamento della macchina virtuale definisce l'allocazione delle risorse di calcolo per le macchine virtuali all'interno di un VDC dell'organizzazione. L'allocazione di risorse di calcolo include l'allocazione di CPU memoria, le prenotazioni, i limiti e le condivisioni.

Con i criteri di dimensionamento della macchina virtuale, gli **amministratori di sistema** di VMware Cloud Director possono controllare i seguenti aspetti del consumo di risorse di calcolo a livello di macchina virtuale:

- Numero di vCPU e velocità di clock delle vCPU
- Quantità di memoria allocata alla macchina virtuale
- Prenotazione, limite e condivisioni di memoria e CPU
- Configurazioni aggiuntive.

Il parametro API `extraConfigs` rappresenta una mappatura tra coppie chiave-valore che vengono applicate come valori di configurazione aggiuntivi in una macchina virtuale. È possibile creare un criterio con configurazioni aggiuntive solo utilizzando l'API di vCloud. Le configurazioni aggiuntive esistenti vengono visualizzate nell'interfaccia utente Service Provider Admin Portal in **Configurazioni aggiuntive** nella vista dettagliata del criterio di dimensionamento della macchina virtuale.

È possibile definire i criteri di dimensionamento della macchina virtuale a livello globale. Per ulteriori informazioni sugli attributi dei criteri di dimensionamento della macchina virtuale, vedere [Attributi dei criteri di dimensionamento della macchina virtuale](#).

VMware Cloud Director genera un criterio di dimensionamento della macchina virtuale predefinito per tutti i VDC. Il criterio di dimensionamento della macchina virtuale predefinito contiene solo un nome e una descrizione e tutti gli attributi del criterio rimanenti sono vuoti.

È inoltre possibile definire un altro criterio di dimensionamento della macchina virtuale come criterio predefinito per un VDC dell'organizzazione. Il criterio di dimensionamento della macchina virtuale predefinito controlla l'allocazione e il consumo di risorse delle macchine virtuali create dai tenant nel VDC dell'organizzazione, a meno che un tenant non assegni un altro criterio di dimensionamento della macchina virtuale specifico alla macchina virtuale.

Per limitare il numero massimo di risorse di calcolo che i tenant possono allocare a singole macchine virtuali in un VDC dell'organizzazione, i provider di cloud possono definire un criterio di dimensionamento della macchina virtuale massimo. Quando viene assegnato a un VDC dell'organizzazione, il criterio di dimensionamento della macchina virtuale massimo agisce come un limite superiore per la configurazione della risorsa di calcolo per tutte le macchine

virtuali nel VDC dell'organizzazione. Il criterio di dimensionamento della macchina virtuale massimo non è disponibile per gli utenti del tenant durante la creazione di una macchina virtuale. Quando si definisce un criterio di dimensionamento della macchina virtuale come criterio massimo, VMware Cloud Director copia internamente il contenuto del criterio e utilizza il contenuto copiato come criterio di dimensionamento della macchina virtuale massimo. Di conseguenza, il VDC dell'organizzazione non dipende dal criterio di dimensionamento della macchina virtuale utilizzato inizialmente.

Utilizzando criteri di dimensionamento della macchina virtuale, i provider di cloud possono limitare il consumo di risorse di calcolo per tutte le macchine virtuali in un VDC dell'organizzazione ad esempio a tre dimensioni predefinite, come *Dimensione piccola*, *Dimensione media* e *Dimensione grande*. Il flusso di lavoro è il seguente.

- 1 Un **amministratore di sistema** crea tre criteri di dimensionamento della macchina virtuale con i seguenti attributi:

Nome	Attributi
Dimensione piccola	<ul style="list-style-type: none"> ■ Descrizione: criterio della macchina virtuale di piccole dimensioni ■ Nome: Dimensione piccola ■ Memoria: 1024 ■ Numero di vCPU: 1
Dimensione media	<ul style="list-style-type: none"> ■ Descrizione: criterio della macchina virtuale di medie dimensioni ■ Nome: Dimensione media ■ Memoria: 2048 ■ Numero di vCPU: 2
Dimensione grande	<ul style="list-style-type: none"> ■ Descrizione: criterio della macchina virtuale di grandi dimensioni ■ Nome: Dimensione grande ■ Memoria: 4096 ■ Numero di vCPU: 4

- 2 Pubblicare i nuovi criteri di dimensionamento della macchina virtuale in un VDC dell'organizzazione.
- 3 Facoltativamente, definire uno dei criteri di dimensionamento della macchina virtuale come criterio di dimensionamento della macchina virtuale predefinito per il VDC dell'organizzazione.

Di seguito sono elencate le operazioni dei criteri disponibili per i provider di cloud:

- Per definire il posizionamento di una macchina virtuale in un host o in un gruppo di host, creare un criterio di posizionamento. Vedere [Creazione di un criterio di posizionamento della macchina virtuale](#).
- Per controllare l'allocazione di risorse di calcolo fisico per i carichi di lavoro del tenant, creare un criterio di ridimensionamento. Vedere [Creazione di un criterio di dimensionamento della macchina virtuale](#).

- Pubblicare un criterio di posizionamento o dimensionamento della macchina virtuale in uno o più VDC dell'organizzazione. Vedere [Aggiunta di un criterio di posizionamento della macchina virtuale a un VDC dell'organizzazione](#)
- Impostare un criterio di posizionamento o dimensionamento della macchina virtuale come predefinito.
- Modificare un criterio di posizionamento della macchina virtuale e un criterio di dimensionamento della macchina virtuale. È possibile modificare solo il nome e la descrizione del criterio nell'interfaccia utente di VMware Cloud Director.
- Annullare la pubblicazione di un criterio di posizionamento o dimensionamento della macchina virtuale da un VDC dell'organizzazione.
- Eliminare un criterio di posizionamento o dimensionamento della macchina virtuale. Consultare [Eliminazione di un criterio di posizionamento della macchina virtuale](#) e [Eliminazione di un criterio di dimensionamento della macchina virtuale](#).

Gli utenti che dispongono del diritto **ORG_VDC_MANAGE_COMPUTE_POLICIES** possono creare, aggiornare e pubblicare i criteri di posizionamento e dimensionamento della macchina virtuale.

Nella tabella seguente sono elencate le operazioni dei criteri di dimensionamento e posizionamento della macchina virtuale per gli utenti dei tenant.

Tabella 6-1. Operazioni dei criteri di dimensionamento e posizionamento della macchina virtuale per gli utenti dei tenant

Operazione	Descrizione
Assegnare un criterio alla macchina virtuale durante la creazione di una macchina virtuale.	<p>Gli utenti del tenant autorizzati a creare macchine virtuali in un VDC dell'organizzazione possono facoltativamente assegnare criteri di posizionamento e dimensionamento della macchina virtuale alle macchine virtuali utilizzando il VMware Cloud Director Tenant Portal. Di conseguenza, i parametri definiti nel criterio di dimensionamento della macchina virtuale controllano il consumo di CPU e memoria della macchina virtuale. L'assegnazione di un criterio di posizionamento o dimensionamento della macchina virtuale non è un requisito per i tenant durante la creazione di una macchina virtuale. Se un tenant non seleziona in modo esplicito un criterio di dimensionamento della macchina virtuale da assegnare a una macchina virtuale, a questa viene applicato il dimensionamento della macchina virtuale predefinito.</p> <p>Se non si crea alcun criterio di posizionamento della macchina virtuale, l'opzione del criterio di posizionamento della macchina virtuale non è visibile per i tenant. Se il tenant seleziona un criterio di posizionamento con informazioni di dimensionamento, l'opzione del criterio di dimensionamento della macchina virtuale diventa nascosto al tenant. È possibile creare un criterio di posizionamento della macchina virtuale con informazioni di dimensionamento solo utilizzando l'API di vCloud.</p> <p>Se è presente un solo criterio di dimensionamento della macchina virtuale, l'opzione del criterio di ridimensionamento della macchina virtuale non è visibile per i tenant.</p> <p>Quando l'amministratore di sistema imposta gli attributi Conteggio vCPU, Core per socket e Memoria in un criterio di dimensionamento della macchina virtuale, se un tenant seleziona il criterio, questi valori vengono visualizzati, ma non sono modificabili.</p>
Assegnare un criterio a una macchina virtuale esistente.	<p>Gli utenti tenant autorizzati a gestire le macchine virtuali in un VDC dell'organizzazione possono assegnare o modificare i criteri di dimensionamento e posizionamento della macchina virtuale per una macchina virtuale esistente utilizzando il VMware Cloud Director Tenant Portal. Quando un tenant modifica il criterio di posizionamento della macchina virtuale, la macchina virtuale viene spostata in un nuovo host in base alle regole di affinità dell'host della macchina virtuale definita nel nuovo criterio di posizionamento della macchina virtuale. Quando un tenant modifica un criterio di dimensionamento della macchina virtuale, il sistema riconfigura la macchina virtuale in modo che utilizzi le risorse di calcolo come specificato nel nuovo criterio di dimensionamento della macchina virtuale.</p>

Il flusso di lavoro per lavorare con il posizionamento della macchina virtuale e i criteri di dimensionamento della macchina virtuale è il seguente.

- 1 Un **amministratore di sistema** crea uno o più criteri di posizionamento della macchina virtuale. Vedere [Creazione di un criterio di posizionamento della macchina virtuale](#).
- 2 Un **amministratore di sistema** crea uno o più criteri di dimensionamento della macchina virtuale. Vedere [Creazione di un criterio di dimensionamento della macchina virtuale](#).

Il nome di un criterio di dimensionamento della macchina virtuale è univoco in un singolo sito VMware Cloud Director. Il nome di un criterio di posizionamento della macchina virtuale è univoco all'interno dell'ambito VDC del provider del criterio.
- 3 Un **amministratore di sistema** pubblica i criteri di posizionamento e dimensionamento della macchina virtuale in uno o più VDC dell'organizzazione. Vedere [Aggiunta di un criterio di posizionamento della macchina virtuale a un VDC dell'organizzazione](#).

La pubblicazione di un criterio di posizionamento della macchina virtuale lo rende disponibile per gli utenti dei tenant nei VDC dell'organizzazione durante la creazione e la modifica della macchina virtuale.

- 4 Quando si crea o si aggiorna una macchina virtuale, i tenant possono utilizzare l'API di vCloud o il VMware Cloud Director Tenant Portal per assegnare un criterio di dimensionamento della macchina virtuale e un criterio di posizionamento della macchina virtuale a una macchina virtuale.

Attributi dei criteri di dimensionamento della macchina virtuale

Quando si crea un criterio di dimensionamento della macchina virtuale, è possibile specificare un sottoinsieme di tutti gli attributi disponibili. L'unico attributo obbligatorio è il nome del criterio di dimensionamento della macchina virtuale.

In un criterio di dimensionamento della macchina virtuale sono presenti due tipi di parametri.

- Configurazione del dimensionamento della macchina virtuale individuale: preconfigurare la RAM specificata, il numero di vCPU e i core per socket per le macchine virtuali in base al criterio corrente.
- Vincoli sulle risorse massime: preconfigurare una limitazione per il consumo di memoria e CPU da parte di una singola macchina virtuale in base al criterio corrente.

Nella tabella seguente sono elencati tutti gli attributi che è possibile definire in un criterio di dimensionamento della macchina virtuale.

Tabella 6-2. Attributi dei criteri di calcolo del VDC

Attributo del criterio di calcolo del VDC	Parametro API	Descrizione
Name	name	Parametro obbligatorio utilizzato come identificatore per il criterio di dimensionamento della macchina virtuale.
Description	description	Rappresenta una breve descrizione del criterio di dimensionamento della macchina virtuale.
vCPU Speed	cpuSpeed	Definisce la velocità della vCPU di un core in MHz o GHz.
vCPU Count	cpuCount	Definisce il numero di vCPU configurate per una macchina virtuale. Questa è una configurazione dell'hardware della macchina virtuale. Quando un tenant assegna il criterio di dimensionamento della macchina virtuale a una macchina virtuale, questo conteggio diventa il numero di vCPU configurato per la macchina virtuale.
Cores Per Socket	coresPerSocket	Numero di core per socket per una macchina virtuale. Questa è una configurazione dell'hardware della macchina virtuale. Il numero di vCPU definito nel criterio di dimensionamento della macchina virtuale deve essere divisibile per il numero di core per socket. Se il numero di vCPU non è divisibile per il numero di core per socket, il numero di core per socket diventa non valido.

Tabella 6-2. Attributi dei criteri di calcolo del VDC (continua)

Attributo del criterio di calcolo del VDC	Parametro API	Descrizione
CPU Reservation Guarantee	cpuReservationGuarantee	<p>Definisce quante delle risorse della CPU di una macchina virtuale sono prenotate.</p> <p>La CPU allocata per una macchina virtuale è uguale al numero di vCPU moltiplicato per la velocità di vCPU in MHz.</p> <p>Il valore dell'attributo è compreso tra 0 e 1. Se la garanzia della prenotazione della CPU ha valore 0, non è definita alcuna prenotazione della CPU. Il valore 1 definisce il 100% della CPU prenotata.</p>
CPU Limit	cpuLimit	<p>Definisce il limite della CPU in MHz o GHz per una macchina virtuale.</p> <p>Se non è definito nel criterio di calcolo del VDC, il limite della CPU è uguale alla velocità della CPU moltiplicata per il numero di vCPU.</p>
CPU Shares	cpuShares	<p>Definisce il numero di condivisioni di CPU per una macchina virtuale.</p> <p>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 CPU rispetto a un'altra macchina virtuale, può consumare una quantità doppia della CPU in questione nel caso in cui entrambe le macchine virtuali competano per le risorse.</p> <p>Se non sono definite nel criterio di calcolo del VDC, alla macchina virtuale vengono applicate le condivisioni normali.</p>
Memory	memory	<p>Definisce la memoria configurata per una macchina virtuale in MB o GB. Questa è una configurazione dell'hardware della macchina virtuale.</p> <p>Quando un tenant assegna il criterio di dimensionamento della macchina virtuale a una macchina virtuale, questa riceve la quantità di memoria definita da questo attributo.</p>
Memory Reservation Guarantee	memoryReservationGuarantee	<p>Definisce la quantità di memoria prenotata configurata per una macchina virtuale.</p> <p>Il valore dell'attributo è compreso tra 0 e 100%.</p>
Memory Limit	memoryLimit	<p>Definisce il limite di memoria in MB o GB per una macchina virtuale.</p> <p>Se non è definito nel criterio di dimensionamento della macchina virtuale, il limite di memoria è uguale alla memoria allocata per la macchina virtuale.</p>
Memory Shares	memoryShares	<p>Definisce il numero di condivisioni di memoria per una macchina virtuale.</p> <p>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 memoria rispetto a un'altra macchina virtuale, può consumare una quantità doppia della memoria in questione nel caso in cui entrambe le macchine virtuali competano per le risorse.</p> <p>Se non sono definite nel criterio di calcolo del VDC, alla macchina virtuale vengono applicate le condivisioni normali.</p>
Extra Configuration	extraConfigs	<p>Rappresenta una mappatura tra coppie chiave-valore che vengono applicate come valori di configurazione aggiuntivi in una macchina virtuale.</p> <p>È possibile creare un criterio con configurazioni aggiuntive solo tramite l'API di vCloud. Le configurazioni aggiuntive esistenti vengono visualizzate nell'interfaccia utente Service Provider Admin Portal in Configurazioni aggiuntive nella vista dettagliata del criterio di dimensionamento della macchina virtuale.</p>

Creazione di un criterio di posizionamento della macchina virtuale

Un criterio di posizionamento della macchina virtuale è un criterio di calcolo del VDC che contiene un riferimento a un criterio del VDC del provider. È possibile utilizzare un criterio di posizionamento della macchina virtuale per definire il posizionamento di una macchina virtuale in un host specifico, un gruppo di host o un cluster.

Prerequisiti

- Verificare che nell'ambiente sia presente almeno un VDC del provider.
- Verificare che nell'ambiente sia presente almeno un gruppo di macchine virtuali.

Un gruppo di macchine virtuali è una raccolta di macchine virtuali che è possibile collegare a un gruppo di host con affinità positive o negative. Tramite una regola di affinità positiva è possibile determinare il posizionamento di un gruppo di macchine virtuali in un host specifico. La regola di anti-affinità o di affinità negativa posiziona un gruppo di macchine virtuali in host diversi, impedendo che tutte le macchine virtuali smettano di funzionare contemporaneamente se un singolo host non funziona. È possibile creare un gruppo di macchine virtuali tramite l'interfaccia utente di vCenter Server o l'API di VMware Cloud Director.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider**.
- 3 Selezionare un VDC del provider nell'elenco.
- 4 Fare clic sulla scheda **Criteri posizionamento macchina virtuale**, quindi su **Nuovo**.
- 5 (Facoltativo) Nella pagina **Che cos'è il criterio di posizionamento della macchina virtuale** della procedura guidata, selezionare la casella di controllo per interrompere la visualizzazione delle informazioni sul criterio di posizionamento della macchina virtuale.
- 6 Fare clic su **Avanti**.
- 7 Immettere un nome per il criterio di posizionamento della macchina virtuale e, facoltativamente, una descrizione.
- 8 Selezionare i gruppi di macchine virtuali o i gruppi di macchine virtuali logiche a cui si desidera collegare la macchina virtuale e fare clic su **Avanti**.

Quando si seleziona più di un gruppo logico, se un tenant applica questo criterio a una macchina virtuale, la macchina virtuale diventa un membro di tutti i gruppi di macchine virtuali inclusi nei gruppi di macchine virtuali logiche selezionati. La macchina virtuale è condizionata da una combinazione di tutte le affinità che si applicano alle macchine virtuali in questi gruppi.

È possibile creare un gruppo di macchine virtuali logiche inline selezionando un gruppo di macchine virtuali per cluster. Questo gruppo di macchine virtuali logiche non ha un nome e può essere utilizzato solo per il criterio di posizionamento della macchina virtuale selezionato.

- 9 Controllare le impostazioni del criterio di posizionamento della macchina virtuale e fare clic su **Fine**.

Operazioni successive

- [Creazione di un criterio di dimensionamento della macchina virtuale](#).
- [Aggiunta di un criterio di posizionamento della macchina virtuale a un VDC dell'organizzazione](#).

Aggiunta di un criterio di posizionamento della macchina virtuale a un VDC dell'organizzazione

Quando si crea un criterio di posizionamento della macchina virtuale, non è visibile per i tenant. È possibile pubblicare un criterio di posizionamento della macchina virtuale in un VDC dell'organizzazione per renderlo disponibile ai tenant.

La pubblicazione di un criterio di posizionamento della macchina virtuale in un VDC dell'organizzazione rende il criterio visibile ai tenant. Il tenant può selezionare il criterio quando crea una nuova macchina virtuale standalone o una macchina virtuale da un modello, la modifica, l'aggiunge a una vApp e crea una vApp da un modello di vApp. Non è possibile eliminare un criterio di posizionamento della macchina virtuale disponibile per i tenant.

Prerequisiti

- Verificare che nel proprio ambiente sia presente almeno un VDC dell'organizzazione. Vedere [Creazione di un virtual data center dell'organizzazione](#).
- Verificare di disporre di almeno un criterio di posizionamento della macchina virtuale. Vedere [Creazione di un criterio di posizionamento della macchina virtuale](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare un VDC dell'organizzazione e fare clic sulla scheda **Criteri posizionamento macchina virtuale**.
- 4 Fare clic su **Aggiungi**.
- 5 Selezionare i criteri di posizionamento della macchina virtuale che si desidera aggiungere al VDC dell'organizzazione e fare clic su **OK**.

Operazioni successive

- Selezionare un criterio e fare clic su **Rimuovi** per annullare la pubblicazione del criterio.
- Selezionare un criterio di posizionamento della macchina virtuale e fare clic su **Imposta come predefinito** per fare in modo che il criterio venga visualizzato come scelta predefinita per i

tenant durante la creazione di una macchina virtuale e di una vApp e durante la modifica della macchina virtuale. Se per un VDC dell'organizzazione è stato pubblicato più di un criterio di posizionamento della macchina virtuale, il tenant può selezionare un criterio diverso da quello predefinito.

Eliminazione di un criterio di posizionamento della macchina virtuale

Se un criterio di posizionamento della macchina virtuale non viene pubblicato nei tenant, è possibile eliminarlo dal VDC del provider.

Prerequisiti

- Verificare che nell'ambiente sia presente almeno un criterio di posizionamento della macchina virtuale.
- Verificare che il criterio di posizionamento della macchina virtuale non venga aggiunto a un VDC dell'organizzazione. Non è possibile eliminare i criteri di posizionamento della macchina virtuale disponibili per i tenant.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider**.
- 3 Selezionare un VDC del provider nell'elenco.
- 4 Fare clic sulla scheda **Criteri di posizionamento macchina virtuale** e selezionare un criterio di posizionamento della macchina virtuale.
- 5 Fare clic su **Elimina**.

Creazione di un criterio di dimensionamento della macchina virtuale

È possibile creare un criterio di dimensionamento della macchina virtuale per rendere disponibile ai tenant vincoli di consumo di CPU e memoria predefiniti che possono essere applicati a macchine virtuali individuali in un VDC dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, fare clic su **Criteri di dimensionamento macchina virtuale**.
- 3 Fare clic su **Nuovo**.
- 4 Immettere un nome per il criterio di dimensionamento della macchina virtuale e, facoltativamente, una descrizione.
- 5 Fare clic su **Avanti**.
- 6 Nella pagina **CPU**, selezionare le impostazioni di allocazione della CPU che si desidera applicare al criterio e fare clic su **Avanti**.

- 7 Selezionare le impostazioni di allocazione della memoria che si desidera applicare al criterio e fare clic su **Avanti**.
- 8 Controllare le impostazioni del criterio di dimensionamento della macchina virtuale e fare clic su **Fine**.

Operazioni successive

- Dopo aver creato un criterio di dimensionamento della macchina virtuale, è possibile modificare solo il nome e la descrizione del criterio di dimensionamento della macchina virtuale. Vedere [Modifica di un criterio di dimensionamento della macchina virtuale](#).
- [Aggiunta di un criterio di dimensionamento della macchina virtuale a un VDC dell'organizzazione](#).
- [Creazione di un criterio di posizionamento della macchina virtuale](#).

Aggiunta di un criterio di dimensionamento della macchina virtuale a un VDC dell'organizzazione

Quando si crea un criterio di dimensionamento della macchina virtuale, esso non è visibile per i tenant. È possibile pubblicare un criterio di dimensionamento della macchina virtuale in un VDC dell'organizzazione per renderlo disponibile ai tenant.

La pubblicazione di un criterio di dimensionamento della macchina virtuale in un VDC dell'organizzazione rende il criterio visibile per i tenant. Il tenant può selezionare il criterio quando crea una nuova macchina virtuale standalone o una macchina virtuale da un modello, la modifica, l'aggiunge a una vApp e crea una vApp da un modello di vApp. Non è possibile eliminare un criterio di dimensionamento della macchina virtuale disponibile per i tenant.

Prerequisiti

- Verificare che nel proprio ambiente sia presente almeno un VDC dell'organizzazione. Vedere [Creazione di un virtual data center dell'organizzazione](#).
- Verificare di disporre di almeno un criterio di dimensionamento della macchina virtuale. Vedere [Creazione di un criterio di dimensionamento della macchina virtuale](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare un VDC dell'organizzazione e fare clic sulla scheda **Criteri di dimensionamento macchina virtuale**.
- 4 Fare clic su **Aggiungi**.
- 5 Selezionare i criteri di dimensionamento della macchina virtuale che si desidera aggiungere al VDC dell'organizzazione e fare clic su **OK**.

Operazioni successive

- Selezionare un criterio e fare clic su **Rimuovi** per annullare la pubblicazione del criterio.
- Selezionare un criterio di dimensionamento della macchina virtuale e fare clic su **Imposta come predefinito** per fare in modo che il criterio venga visualizzato come scelta predefinita per i tenant durante la creazione di una macchina virtuale e di una vApp e la modifica della macchina virtuale. Se per un VDC dell'organizzazione è stato pubblicato più di un criterio di dimensionamento della macchina virtuale, il tenant può selezionare un criterio diverso da quello predefinito.

Modifica di un criterio di dimensionamento della macchina virtuale

Dopo aver creato un criterio di dimensionamento della macchina virtuale, è possibile modificarne solo il nome e la descrizione. La modifica dei parametri della CPU e della memoria non è supportata.

Prerequisiti

- Verificare che nel proprio ambiente sia presente almeno un VDC dell'organizzazione. Vedere [Creazione di un virtual data center dell'organizzazione](#).
- Verificare di disporre di almeno un criterio di dimensionamento della macchina virtuale. Vedere [Creazione di un criterio di dimensionamento della macchina virtuale](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, fare clic su **Criteri di dimensionamento macchina virtuale**.
- 3 Fare clic sul nome del criterio di dimensionamento della macchina virtuale che si desidera modificare.
- 4 Per modificare il nome e la descrizione del criterio, fare clic su **Modifica**.
- 5 Fare clic su **Salva**.

Operazioni successive

[Aggiunta di un criterio di dimensionamento della macchina virtuale a un VDC dell'organizzazione](#)

Eliminazione di un criterio di dimensionamento della macchina virtuale

È possibile eliminare i criteri di dimensionamento della macchina virtuale che non sono pubblicati nei tenant.

Prerequisiti

- Verificare che nell'ambiente sia presente almeno un criterio di dimensionamento della macchina virtuale.

- Verificare che il criterio di dimensionamento della macchina virtuale non venga aggiunto a un VDC dell'organizzazione. Non è possibile eliminare i criteri di dimensionamento della macchina virtuale disponibili per i tenant.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, fare clic su **Criteri di dimensionamento macchina virtuale**.
- 3 Selezionare un criterio di dimensionamento della macchina virtuale e fare clic su **Elimina**.

Creazione di un virtual data center dell'organizzazione

Per allocare risorse a un'organizzazione, è necessario creare un virtual data center dell'organizzazione. Un virtual data center dell'organizzazione ottiene le proprie risorse da un virtual data center del provider. Un'organizzazione può disporre di più virtual data center dell'organizzazione.

Prerequisiti

Creare un virtual data center del provider. Vedere [Creazione di un virtual data center del provider](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra, fare clic su **VDC dell'organizzazione** e su **Nuovo**.
- 3 Immettere un nome e, facoltativamente, una descrizione per il nuovo virtual data center dell'organizzazione.
- 4 (Facoltativo) Per disabilitare il nuovo virtual data center dell'organizzazione al momento della creazione, disattivare l'interruttore **Abilitare il VDC dell'organizzazione**.

Gli utenti non possono distribuire vApp in un virtual data center dell'organizzazione disabilitato.

- 5 Fare clic su **Avanti**.
- 6 Selezionare il pulsante di opzione accanto al nome dell'organizzazione in cui si desidera aggiungere questo virtual data center e fare clic su **Avanti**.
- 7 Selezionare il pulsante di opzione accanto al nome del virtual data center del provider da cui si desidera che il virtual data center dell'organizzazione ottenga risorse di elaborazione e storage, quindi fare clic su **Avanti**.

L'elenco dei virtual data center del provider include tutti i virtual data center del provider abilitati nel sito con informazioni sulle risorse disponibili. L'elenco delle reti include informazioni sulle reti disponibili per il virtual data center del provider selezionato.

- 8 Selezionare un modello di allocazione per questo virtual data center dell'organizzazione e fare clic su **Avanti**.

Opzione	Descrizione
Pool di allocazioni	Una percentuale delle risorse allocate dal virtual data center del provider viene sottoposta a commit nel virtual data center dell'organizzazione. È possibile specificare la percentuale per CPU e memoria.
Pay-As-You-Go	Le risorse vengono sottoposte a commit solo se gli utenti creano vApp nel virtual data center dell'organizzazione.
Pool di prenotazioni	Tutte le risorse allocate vengono immediatamente sottoposte a commit nel virtual data center dell'organizzazione.
Flex	È possibile controllare il consumo di risorse sia a livello del VDC sia a livello della singola macchina virtuale. Il modello di allocazione Flex supporta le funzionalità dei criteri di calcolo del VDC dell'organizzazione. Il modello di allocazione Flex supporta tutte le configurazioni di allocazione disponibili negli altri modelli di allocazione.

- 9 Configurare le impostazioni di allocazione per il modello di allocazione selezionato e fare clic su **Avanti**.

Opzione	Descrizione	Modello di allocazione
Elasticità	Abilitare o disabilitare la funzionalità del pool elastico. Un VDC dell'organizzazione elastico include e utilizza tutti i pool di risorse associati al rispettivo VDC provider.	Flex
Includi overhead della memoria della macchina virtuale	Includere o escludere l'overhead della memoria.	Flex
Allocazione CPU	La quantità massima di CPU che si desidera allocare alle macchine virtuali in esecuzione nel virtual data center dell'organizzazione.	<ul style="list-style-type: none"> ■ Pool di allocazioni ■ Pool di prenotazioni ■ Flex
Consenti l'aumento delle risorse CPU	Per fornire risorse CPU illimitate a questo virtual data center dell'organizzazione, attivare questo interruttore.	Pool di prenotazioni
Quota CPU	La quantità massima di consumo di CPU per questo virtual data center dell'organizzazione.	<ul style="list-style-type: none"> ■ Pay-As-You-Go ■ Flex
Risorse CPU garantite	La percentuale di risorse CPU che si desidera garantire a una macchina virtuale in esecuzione in questo virtual data center dell'organizzazione. È possibile controllare l'overcommit di risorse CPU garantendone meno del 100%. Per un modello di allocazione del pool di allocazioni, la garanzia di percentuale determina anche la percentuale di allocazione della CPU di cui viene eseguito il commit per questo virtual data center dell'organizzazione.	<ul style="list-style-type: none"> ■ Pool di allocazioni ■ Pay-As-You-Go ■ Flex
Velocità vCPU	La velocità della vCPU. Alle macchine virtuali in esecuzione nel virtual data center dell'organizzazione verrà assegnata questa quantità di GHz per ogni vCPU.	<ul style="list-style-type: none"> ■ Pay-As-You-Go ■ Flex

Opzione	Descrizione	Modello di allocazione
Allocazione memoria	La quantità massima di memoria che si desidera allocare alle macchine virtuali in esecuzione nel virtual data center dell'organizzazione.	<ul style="list-style-type: none"> ■ Pool di allocazioni ■ Pool di prenotazioni
Quota memoria	La quantità massima di consumo di memoria per questo virtual data center dell'organizzazione.	<ul style="list-style-type: none"> ■ Pay-As-You-Go ■ Flex
Risorse di memoria garantite	La percentuale di risorse della memoria che si desidera garantire alle macchine virtuali in esecuzione nel virtual data center dell'organizzazione. È possibile eseguire l'overcommit delle risorse garantendone meno del 100%. Per un modello di allocazione del pool di allocazioni, la garanzia di percentuale determina anche la percentuale di allocazione della memoria impegnata per questo virtual data center dell'organizzazione.	<ul style="list-style-type: none"> ■ Pool di allocazioni ■ Pay-As-You-Go ■ Flex
Numero massimo di macchine virtuali	Il numero massimo di macchine virtuali che possono essere presenti nel virtual data center dell'organizzazione.	<ul style="list-style-type: none"> ■ Pool di allocazioni ■ Pay-As-You-Go ■ Pool di prenotazioni ■ Flex

- 10 Configurare le impostazioni di storage per questo virtual data center dell'organizzazione e fare clic su **Avanti**.

L'elenco contiene i criteri di storage abilitati nel virtual data center del provider di origine.

- a Selezionare le caselle di controllo di uno o più criteri di storage che si desidera aggiungere a questo virtual data center dell'organizzazione.
- b (Facoltativo) Per limitare la quantità di capacità di storage allocata per un criterio di storage selezionato, selezionare **Limitato** nel menu a discesa nella cella **Tipo di allocazione** e immettere la capacità massima nella cella **Storage allocato**.
- c (Facoltativo) Per modificare il criterio di storage predefinito, nel menu a discesa **Criterio di creazione istanze predefinito**, selezionare il criterio di storage predefinito di destinazione.

VMware Cloud Director utilizza il criterio di storage predefinito per tutte le operazioni di provisioning delle macchine virtuali in cui il criterio di storage non viene specificato a livello del modello di vApp o della macchina virtuale.
- d (Facoltativo) Per abilitare il thin provisioning per le macchine virtuali nel virtual data center dell'organizzazione, attivare l'interruttore **Thin provisioning**.
- e (Facoltativo) Per disabilitare il provisioning rapido per le macchine virtuali nel virtual data center dell'organizzazione, disattivare l'interruttore **Provisioning rapido**.

- 11 Configurare le impostazioni del pool di reti per questo virtual data center dell'organizzazione e fare clic su **Avanti**.

VMware Cloud Director utilizza il pool di reti per creare reti di vApp e reti del virtual data center dell'organizzazione interne.

- Per ignorare l'aggiunta di un pool di reti in questa fase, disattivare l'interruttore **Utilizza pool di reti**.

- Per configurare un pool di reti, selezionare il pulsante di opzione accanto al nome del pool di reti di destinazione e immettere la quota per questo virtual data center dell'organizzazione.

La quota è il numero massimo di reti di cui è stato eseguito il provisioning nel virtual data center dell'organizzazione supportato da questo pool di reti. Non deve superare il numero di reti disponibili per il pool di reti selezionato.

12 Controllare la pagina **Pronto per il completamento** e fare clic su **Fine**.

Abilitazione o disabilitazione di un virtual data center dell'organizzazione

Per impedire a ulteriori vApp e macchine virtuali di utilizzare risorse di elaborazione e storage da un virtual data center dell'organizzazione, è possibile disabilitare il virtual data center dell'organizzazione. Le vApp in esecuzione su macchine virtuali continueranno a essere eseguite, ma non sarà possibile creare o avviare altre vApp o macchine virtuali.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere **Abilita** o **Disabilita**.
- 4 Per confermare, fare clic su **OK**.

Eliminazione di un virtual data center dell'organizzazione

Per rimuovere tutte le risorse di un virtual data center dell'organizzazione dall'organizzazione, è possibile eliminare il virtual data center dell'organizzazione. Questa operazione non influisce sulle risorse nel virtual data center del provider di origine.

Importante Questa operazione consente di rimuovere definitivamente il virtual data center dell'organizzazione e tutte le relative macchine virtuali, vApp, reti di virtual data center dell'organizzazione e gateway edge.

Prerequisiti

Se si desidera mantenere determinate macchine virtuali, vApp, modelli di vApp o file multimediali appartenenti al virtual data center dell'organizzazione di destinazione, è possibile spostarli in un altro virtual data center dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.

- 3 Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione che si desidera rimuovere e fare clic su **Elimina**.
- 4 Se il virtual data center dell'organizzazione contiene risorse, ad esempio macchine virtuali, vApp, reti di virtual data center dell'organizzazione e gateway edge, per confermarne la rimozione, selezionare la casella di controllo per ogni tipo di risorsa.
- 5 Per confermare, fare clic su **Elimina**.

Modifica del nome e della descrizione del virtual data center dell'organizzazione

Con l'aumentare delle dimensioni dell'installazione di VMware Cloud Director, può essere necessario assegnare un nome più significativo o una descrizione più precisa a un virtual data center esistente dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Nell'angolo superiore destro della scheda **Generale**, fare clic su **Modifica**.
- 4 Immettere un nuovo nome e una nuova descrizione, quindi fare clic su **Salva**.

Modifica delle impostazioni del modello di allocazione di un virtual data center dell'organizzazione

Non è possibile modificare il modello di allocazione di un virtual data center dell'organizzazione, ma è possibile modificare le impostazioni di allocazione per il modello di allocazione specificate durante la procedura di creazione del virtual data center dell'organizzazione.

È possibile modificare le impostazioni di allocazione per il modello di allocazione configurato durante la creazione del virtual data center dell'organizzazione. Vedere [Passaggio 9](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Nell'angolo superiore destro della scheda **Allocazione**, fare clic su **Modifica**.
- 4 Modificare le impostazioni del modello di allocazione e fare clic su **Salva**.

Modifica delle impostazioni di storage di un virtual data center dell'organizzazione

È possibile modificare le impostazioni di storage configurate durante la creazione del virtual data center dell'organizzazione.

Abilitazione della crittografia della macchina virtuale nei criteri di storage di un virtual data center dell'organizzazione

È possibile aggiungere un criterio di storage abilitato per la crittografia in un VDC dell'organizzazione. È possibile crittografare macchine virtuali e dischi associando una macchina virtuale o un disco a un criterio di storage che disponga della funzionalità di 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. 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 del provider dispone di un criterio di storage in cui è abilitata la crittografia della macchina virtuale, è possibile aggiungere il criterio abilitato per la crittografia in un VDC dell'organizzazione. Consultare [Abilitazione della crittografia della macchina virtuale nei criteri di storage di un virtual data center del provider](#) e [Aggiunta di un criterio di storage della macchina virtuale a un virtual data center dell'organizzazione](#). Quindi, utilizzando VMware Cloud Director Tenant Portal, i tenant possono essere associati a una macchina virtuale o a un disco con un criterio di storage in cui sia abilitata la crittografia della macchina virtuale.

Limitazioni della crittografia della macchina virtuale

Le seguenti azioni non sono supportate in VMware Cloud Director 10.1.

- 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. Gli **autori di vApp** possono visualizzare lo stato di crittografia delle macchine virtuali e dei dischi. Per ulteriori informazioni su questi ruoli e diritti, vedere [Ruoli predefiniti e relativi diritti](#).

È possibile visualizzare tutte le funzionalità di storage nella colonna **Funzionalità** in **Risorse > Risorse vSphere > Criteri di storage**. In questa colonna vengono visualizzate la crittografia della macchina virtuale, l'associazione basata su tag, vSAN e le operazioni IOPS che limitano le capacità di storage. Per visualizzare l'elenco completo delle capacità di storage, espandere la riga facendo clic sulla freccia a sinistra del nome del criterio di storage.

Le informazioni sulla capacità di storage possono essere visualizzate anche nella scheda **Storage** di un VDC dell'organizzazione.

Modifica delle impostazioni di provisioning delle macchine virtuali di un virtual data center dell'organizzazione

È possibile modificare le impostazioni del thin provisioning e del fast provisioning delle macchine virtuali configurate durante la creazione del virtual data center dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Nell'angolo superiore destro della scheda **Storage**, fare clic su **Modifica**.
- 4 (Facoltativo) Modificare l'impostazione del thin provisioning.
 - Per disabilitare il thin provisioning per le macchine virtuali nel virtual data center dell'organizzazione, disattivare l'interruttore **Thin provisioning**.
 - Per abilitare il thin provisioning per le macchine virtuali nel virtual data center dell'organizzazione, attivare l'interruttore **Thin provisioning**.
- 5 (Facoltativo) Modificare l'impostazione del provisioning rapido.
 - Per abilitare il provisioning rapido per le macchine virtuali nel virtual data center dell'organizzazione, attivare l'interruttore **Provisioning rapido**.

- Per disabilitare il provisioning rapido per le macchine virtuali nel virtual data center dell'organizzazione, disattivare l'interruttore **Provisioning rapido**.

6 Fare clic su **Modifica**.

Aggiunta di un criterio di storage della macchina virtuale a un virtual data center dell'organizzazione

È possibile configurare un virtual data center dell'organizzazione per supportare un criterio di storage della macchina virtuale aggiunto in precedenza al virtual data center del provider di supporto.

Prerequisiti

Il criterio di storage della macchina virtuale di destinazione è stato aggiunto al virtual data center del provider di origine. Vedere [Aggiunta di un criterio di storage della macchina virtuale in un virtual data center del provider](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Storage**, quindi su **Aggiungi**.

È possibile visualizzare un elenco dei criteri di storage aggiuntivi disponibili nel virtual data center del provider di origine.
- 4 Selezionare le caselle di controllo di uno o più criteri di storage da aggiungere e fare clic su **Aggiungi**.

Modifica del criterio di storage predefinito in un virtual data center dell'organizzazione

È possibile modificare il criterio di storage predefinito configurato durante la creazione di un virtual data center dell'organizzazione.

VMware Cloud Director utilizza il criterio di storage predefinito per tutte le operazioni di provisioning delle macchine virtuali in cui il criterio di storage non viene specificato a livello del modello di vApp o della macchina virtuale.

Prerequisiti

- Il criterio di storage predefinito di destinazione viene aggiunto al virtual data center dell'organizzazione. Vedere [Aggiunta di un criterio di storage della macchina virtuale a un virtual data center dell'organizzazione](#).
- Il criterio di storage predefinito di destinazione è abilitato nel virtual data center dell'organizzazione. Vedere [Abilitazione o disabilitazione di un criterio di storage in un virtual data center dell'organizzazione](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Storage**.
- 4 Fare clic sul pulsante di opzione accanto al nome del criterio di storage predefinito di destinazione e quindi su **Imposta come predefinito**.
- 5 Per confermare, fare clic su **OK**.

Modifica del limite di un criterio di storage in un virtual data center dell'organizzazione

È possibile modificare il limite della capacità di storage allocata configurata per un criterio di storage durante la creazione di un virtual data center dell'organizzazione.

È possibile impostare la capacità di storage allocata come illimitata o configurare una quantità massima di capacità di storage allocata per un criterio di storage in un virtual data center dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Storage**.
- 4 Fare clic sul pulsante di opzione accanto al nome del criterio di storage di destinazione e fare clic su **Modifica limite**.
- 5 Configurare l'impostazione del limite per questo criterio di storage.
 - Per impostare un limite, selezionare il pulsante di opzione superiore e immettere la quantità massima di risorse di storage per questo criterio di storage nel virtual data center dell'organizzazione.
 - Per impostare nessun limite, selezionare il pulsante di opzione **Illimitato**.
- 6 Fare clic su **Modifica**.

Modifica dei metadati per un criterio di storage della macchina virtuale in un virtual data center dell'organizzazione

È possibile aggiungere, modificare ed eliminare metadati per un criterio di storage in un virtual data center dell'organizzazione.

Utilizzando i metadati degli oggetti, è possibile associare coppie di *name=value* definite dall'utente a un criterio di storage in un virtual data center dell'organizzazione. È possibile utilizzare i metadati degli oggetti nelle espressioni di filtro delle query API di vCloud.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Storage**.
- 4 Fare clic sul pulsante di opzione accanto al nome del criterio di storage di destinazione e fare clic su **Metadati**.
- 5 Fare clic su **Modifica**.
- 6 (Facoltativo) Per aggiungere una coppia chiave-valore, fare clic su **Aggiungi**, immettere un nome e un valore e selezionare un tipo per la nuova coppia chiave-valore.
- 7 (Facoltativo) Per modificare una coppia chiave-valore, immettere un nuovo nome e un valore e selezionare un nuovo tipo per la coppia chiave-valore.
- 8 (Facoltativo) Per rimuovere una coppia chiave-valore, a destra della riga corrispondente, fare clic sull'icona **Elimina**.
- 9 Fare clic su **Salva** e fare clic su **OK**.

Abilitazione o disabilitazione di un criterio di storage in un virtual data center dell'organizzazione

Per impedire che ulteriori vApp e macchine virtuali utilizzino un criterio di storage in un virtual data center dell'organizzazione, è possibile disabilitare questo criterio di storage nel virtual data center dell'organizzazione. Il funzionamento delle vApp in esecuzione e delle macchine virtuali attivate continuerà, ma non sarà possibile crearne o avviarne altre con questo criterio di storage.

Non è possibile disabilitare il criterio di storage predefinito.

Prerequisiti

Se si desidera disabilitare il criterio di storage predefinito, [Modifica del criterio di storage predefinito in un virtual data center dell'organizzazione](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Storage**.

- 4 Fare clic sul pulsante di opzione accanto al nome dell'istanza di di destinazione e scegliere **Abilita** o **Disabilita**.
- 5 Per confermare, fare clic su **OK**.

Eliminazione di un criterio di storage da un virtual data center dell'organizzazione

Per impedire a un virtual data center dell'organizzazione di utilizzare un criterio di storage, è possibile rimuovere il criterio di storage dal virtual data center dell'organizzazione. Il funzionamento delle vApp in esecuzione e delle macchine virtuali attivate continuerà, ma non sarà possibile crearne o avviarne altre con questo criterio di storage.

Prerequisiti

Disabilitare il criterio di storage che si desidera rimuovere. Vedere [Abilitazione o disabilitazione di un criterio di storage in un virtual data center dell'organizzazione](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Storage**.
- 4 Fare clic sul pulsante di opzione accanto al nome del criterio di storage di destinazione e fare clic su **Rimuovi**.
- 5 Per confermare, fare clic su **Rimuovi**.

Modifica delle impostazioni di rete di un virtual data center dell'organizzazione

È possibile modificare il pool di reti da cui le nuove reti vengono sottoposte a provisioning in un virtual data center dell'organizzazione. È inoltre possibile abilitare i virtual data center dell'organizzazione in modo da renderli idonei per le reti inter-VDC.

Un pool di reti è un gruppo di reti indifferenziate che è possibile utilizzare per creare reti di vApp, reti VDC dell'organizzazione instradate e reti vDC dell'organizzazione interne. È possibile modificare il pool di reti per le nuove reti. Le reti esistenti continuano a utilizzare i vecchi pool di reti.

Con i virtual data center dell'organizzazione abilitati per le reti inter-VDC, gli utenti dell'organizzazione con diritti pertinenti possono creare gruppi di data center e reti di livello 2 estese in questi gruppi.

Prerequisiti

Se si desidera abilitare la rete inter-VDC per un virtual data center dell'organizzazione, verificare di aver configurato NSX inter-vCenter nel virtual data center del provider di supporto.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Nell'angolo superiore destro della scheda **Pool di reti**, fare clic su **Modifica**.
È possibile visualizzare il numero di reti utilizzate da questo virtual data center dell'organizzazione.
- 4 (Facoltativo) Configurare le impostazioni del pool di reti per questo virtual data center dell'organizzazione.
 - Se non si desidera un pool di reti per questo virtual data center dell'organizzazione, disattivare l'opzione **Utilizza pool di reti**.
 - Se si desidera configurare un pool di reti per questo virtual data center dell'organizzazione, eseguire i passaggi seguenti:
 - a Attivare l'opzione **Utilizza pool di reti**.
È possibile visualizzare un elenco dei pool di reti disponibili con informazioni sul loro utilizzo, sulle reti disponibili e sulla capacità.
 - b Selezionare il pulsante di opzione accanto al nome del pool di risorse di destinazione.
 - c Configurare la quota per questo pool di reti in questo virtual data center dell'organizzazione.
La quota è il numero massimo di reti di cui è stato eseguito il provisioning. Non deve superare il numero di reti disponibili per il pool di reti selezionato.
- 5 Per abilitare le reti inter-VDC per questo virtual data center dell'organizzazione, attivare l'opzione **Networking VDC incrociato**.
- 6 Fare clic su **Salva**.

Risultati

Nel portale tenant di VMware Cloud Director i virtual data center abilitati per il networking inter-VDC sono presenti nell'elenco dei data center per la creazione di un gruppo di data center. Per informazioni su come creare gruppi di data center, vedere *VMware Cloud Director Tenant Portal Guide*.

Configurazione di servizi di rete inter-VDC

La funzionalità dei servizi di rete inter-VDC consente alle organizzazioni che dispongono di virtual data center supportati da più istanze di vCenter Server di estendere le reti di livello 2 fino a quattro virtual data center. I servizi di rete inter-VDC si basano su NSX tra vCenter e possono essere estesi a più siti di VMware Cloud Director.

La creazione di una rete tra virtual data center richiede NSX Data Center for vSphere.

Con la rete inter-VDC le organizzazioni possono raggruppare fino a quattro virtual data center e configurare uscite e reti di livello 2 estese in ogni gruppo.

I virtual data center inclusi in un gruppo possono appartenere a siti di VMware Cloud Director diversi. Vedere [Configurazione e gestione di distribuzioni multisito](#).

Le organizzazioni possono utilizzare i servizi di rete inter-VDC per implementare soluzioni ad alta disponibilità o architetture di sistemi distribuiti, in cui un'applicazione può essere distribuita tra più virtual data center o siti.

L'**amministratore di sistema** deve configurare l'ambiente NSX tra vCenter sottostante e i server VMware Cloud Director, nonché abilitare i servizi di rete tra virtual data center per ogni virtual data center.

- 1 Configurare una delle istanze di NSX Manager come istanza di NSX Manager primario. Vedere *la guida all'installazione di NSX tra vCenter*.
 - a Distribuire il cluster NSX nell'istanza di NSX Manager primario.
 - b Preparare gli host ESXi nell'istanza di NSX Manager primario.
 - c Configurare VXLAN dall'istanza di NSX Manager primario.
 - d Assegnare il ruolo primario all'istanza di NSX Manager.
 - e Creare un pool per la segmentazione IP per la zona di trasporto universale.
 - f Aggiungere una zona di trasporto universale.
- 2 Configurare il resto delle istanze di NSX Manager come NSX Manager secondari. Vedere *la guida all'installazione di NSX tra vCenter*.
 - a Preparare gli host ESXi in ciascuna istanza di NSX Manager secondario.
 - b Configurare VXLAN da ogni istanza di NSX Manager secondario.
 - c Assegnare il ruolo secondario a ogni istanza di NSX Manager.
 - d Connettere i cluster ESXi alla zona di trasporto universale.
- 3 Configurare le proprietà della macchina virtuale di controllo per ogni istanza di NSX Manager. Vedere [Modifica delle impostazioni di NSX Manager](#).

- 4 Creare un pool di reti con supporto VXLAN utilizzando una zona di trasporto di tipo universale da qualsiasi istanza di vCenter Server. Vedere [Creazione di un pool di reti supportato da una zona di trasporto NSX Data Center for vSphere](#).

Nota Per le distribuzioni multisito, è necessario creare un pool di reti con supporto VXLAN in ciascun sito di VMware Cloud Director.

- 5 Abilitare i servizi di rete inter-VDC in ogni virtual data center dell'organizzazione. Vedere [Modifica delle impostazioni di rete di un virtual data center dell'organizzazione](#).
- 6 Se l'organizzazione dispone di virtual data center multisito, verificare che gli ID di installazione dei vari siti di VMware Cloud Director siano diversi. Se sono presenti siti di VMware Cloud Director configurati con lo stesso ID di installazione, vedere [Rigenerazione degli indirizzi MAC per reti estese multisito](#) nella *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

A questo punto, l'**amministratore dell'organizzazione** può creare e configurare gruppi di data center, uscite e reti estese. Per informazioni sulla gestione dei servizi di rete inter-VDC, vedere *VMware Cloud Director Tenant Portal Guide*.

Modifica dei metadati per un virtual data center dell'organizzazione

È possibile aggiungere, modificare ed eliminare i metadati per un virtual data center dell'organizzazione.

Utilizzando i metadati degli oggetti, è possibile associare a un virtual data center dell'organizzazione coppie `name=value` definite dall'utente a un virtual data center dell'organizzazione. È possibile utilizzare i metadati degli oggetti nelle espressioni di filtro delle query API di vCloud.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Metadati**.
- 4 Fare clic su **Modifica**.
- 5 (Facoltativo) Per aggiungere una coppia chiave-valore, fare clic su **Aggiungi**, immettere un nome e un valore e selezionare un tipo per la nuova coppia chiave-valore.
- 6 (Facoltativo) Per modificare una coppia chiave-valore, immettere un nuovo nome e un valore e selezionare un nuovo tipo per la coppia chiave-valore.
- 7 (Facoltativo) Per rimuovere una coppia chiave-valore, a destra della riga corrispondente, fare clic sull'icona **Elimina**.

8 Fare clic su **Salva** e fare clic su **OK**.

Visualizzazione dei pool di risorse di un virtual data center dell'organizzazione

È possibile visualizzare un elenco dei pool di risorse di vCenter Server utilizzati da un virtual data center dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione** e quindi sul nome del virtual data center dell'organizzazione di destinazione.
- 3 Fare clic sulla scheda **Pool di risorse**.

Risultati

È possibile visualizzare una tabella con i pool di risorse in uso dal virtual data center dell'organizzazione e l'istanza di vCenter Server a cui ciascun pool di risorse appartiene.

Gestione del firewall distribuito in un virtual data center dell'organizzazione

Per fornire la sicurezza di rete di livello 3 e di livello 2 in un virtual data center dell'organizzazione, è possibile abilitare e creare regole per il firewall distribuito su questo virtual data center dell'organizzazione. Con le regole del firewall distribuito, è possibile proteggere il traffico che viaggia tra macchine virtuali in un virtual data center dell'organizzazione.

VMware Cloud Director supporta i servizi firewall distribuiti nei virtual data center dell'organizzazione supportati da NSX Data Center for vSphere.

Per la creazione delle regole del firewall distribuito, è possibile utilizzare vari oggetti di raggruppamento e gruppi di sicurezza. Vedere [Raggruppamento di oggetti personalizzato](#) e [Utilizzo dei gruppi di sicurezza](#).

Per informazioni sulla protezione del traffico da e verso un gateway edge, vedere [Gestione di un firewall del gateway edge NSX Data Center for vSphere](#).

Abilitazione del firewall distribuito in un virtual data center dell'organizzazione

Prima di poter gestire le impostazioni del firewall distribuito in un virtual data center dell'organizzazione, è necessario abilitare il firewall distribuito in tale virtual data center dell'organizzazione.

VMware Cloud Director supporta i servizi firewall distribuiti nei virtual data center dell'organizzazione supportati da NSX Data Center for vSphere.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 4 Nella scheda **Firewall distribuito > Generale**, attivare l'interruttore **Abilita Firewall distribuito**.

Risultati

È possibile visualizzare le regole predefinite del firewall, che consentono il passaggio di tutto il traffico di livello 3 e di livello 2 attraverso il virtual data center dell'organizzazione.

- Nella scheda **Firewall distribuito > Generale**, è possibile visualizzare la regola del firewall distribuito predefinita per il traffico di livello 3, con il nome Regola di permesso predefinita.
- Nella scheda **Firewall distribuito > Ethernet**, è possibile visualizzare la regola del firewall distribuito predefinita per il traffico di livello 2, con il nome Regola di permesso predefinita.

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](#)
- 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 barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.

- 4 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**.

- 5 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.

- 6 Fare clic nella cella **Nome** e digitare un nome.
- 7 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>

8 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>

9 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: <ol style="list-style-type: none"> Selezionare il protocollo del servizio. 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: <ol style="list-style-type: none"> Selezionare uno o più oggetti e aggiungerli al filtro. Fare clic su Mantieni.

10 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.

11 Nella cella **Direzione** della nuova regola, selezionare se la regola si applica al traffico in entrata, a quello in uscita oppure a entrambi.

12 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**.

- 13 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.


- 14 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 barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 4 Per gestire le regole del firewall distribuito, eseguire una delle seguenti azioni:
 - Per disabilitare una regola, fare clic sul segno di spunta verde nella relativa cella **N.**.
Il segno di spunta verde diventa un'icona di disabilitazione di colore rosso. Se la regola è disabilitata e si desidera abilitarla, fare clic sull'icona di disabilitazione 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.
- 5 Fare clic su **Salva modifiche**.

Raggruppamento di oggetti personalizzato

Il software NSX 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**. Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.

Procedura

- 1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ol style="list-style-type: none"> Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. Nel riquadro a sinistra fare clic su VDC dell'organizzazione. Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ol style="list-style-type: none"> Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. Nel riquadro a sinistra fare clic su Gateway edge. Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. Fare clic sulla scheda 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 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**. Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.


Procedura

- 1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ol style="list-style-type: none"> Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. Nel riquadro a sinistra fare clic su VDC dell'organizzazione. Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ol style="list-style-type: none"> Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. Nel riquadro a sinistra fare clic su Gateway edge. Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. Fare clic sulla scheda 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 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 servizi disponibili utilizzando la pagina **Raggruppamento di oggetti**. Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.

Procedura

1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su VDC dell'organizzazione. c Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. d Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su Gateway edge. c Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. d Fare clic sulla scheda 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**. Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.

Procedura

1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su VDC dell'organizzazione. c Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. d Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su Gateway edge. c Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. d Fare clic sulla scheda 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.

Utilizzo dei gruppi di sicurezza

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 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.

- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 4 Fare clic sulla scheda **Raggruppamento di oggetti > Gruppi di sicurezza**.
- 5 Fare clic sul pulsante **Crea** ()
- 6 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.
- 7 (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**.
- 8 (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.
- 9 (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.




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 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 4 Fare clic sulla scheda **Raggruppamento di oggetti > Gruppi di sicurezza**.
- 5 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.
- 6 (Facoltativo) Modificare il nome e la descrizione del gruppo di sicurezza.
- 7 (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**.
- 8 (Facoltativo) Modificare un set di membri dinamici facendo clic sull'icona **Modifica** () accanto al set di membri dinamici che si desidera modificare.
 - a Applicare le modifiche necessarie al set di membri dinamici.
 - b Fare clic su **OK**.
- 9 (Facoltativo) Eliminare un set di membri dinamici facendo clic sull'icona **Elimina** () accanto al set di membri dinamici che si desidera eliminare.

- 10** (Facoltativo) Modificare l'elenco dei membri inclusi facendo clic sull'icona **Modifica**  accanto all'elenco **Includi 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.
 - 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.
- 11** (Facoltativo) Modificare l'elenco dei membri esclusi facendo clic sull'icona **Modifica**  accanto all'elenco **Escludi 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.
 - 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.
- 12** 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 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 4 Fare clic sulla scheda **Raggruppamento di oggetti > Gruppi di sicurezza**.
- 5 Selezionare il gruppo di sicurezza che si desidera eliminare.
- 6 Fare clic sul pulsante **Elimina** ().
- 7 Per confermare l'eliminazione, fare clic su **OK**.

Risultati

Il gruppo di sicurezza viene eliminato.

Utilizzo dei tag di sicurezza

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 barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 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 barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 4 Dall'elenco dei tag di sicurezza, selezionare il tag di sicurezza da 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 barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 4 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**.

5 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 barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 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](#).

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 barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **VDC dell'organizzazione**.
- 3 Selezionare il pulsante di opzione accanto al virtual data center dell'organizzazione di destinazione e selezionare **Gestisci firewall**.
- 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](#)

Gestione dei gateway edge NSX Data Center for vSphere

7

Un gateway edge NSX Data Center for vSphere fornisce a una rete di virtual data center dell'organizzazione instradata la connettività a reti esterne e può offrire servizi come bilanciamento del carico, NAT (Network Address Translation) e firewall. VMware Cloud Director supporta gateway edge IPv4 e IPv6.

A partire da VMware Cloud Director 9.7, il carico di lavoro di elaborazione e il carico di lavoro di rete vengono isolati utilizzando diversi pool di risorse e criteri di storage vSphere. I gateway edge si trovano in cluster edge che è necessario creare in precedenza. Vedere [Utilizzo dei cluster edge di NSX Data Center for vSphere](#).

È possibile migrare i gateway edge preesistenti ai cluster edge corrispondenti ridistribuendo questi gateway edge. Vedere [Ridistribuzione di un gateway edge](#).

Importante A partire dalla versione 9.7, VMware Cloud Director supporta solo gateway edge avanzati. È necessario convertire un gateway edge non avanzato preesistente in un gateway avanzato. Vedere <https://kb.vmware.com/kb/66767>.

Questo capitolo include i seguenti argomenti:

- [Utilizzo dei cluster edge di NSX Data Center for vSphere](#)
- [Aggiunta di un gateway edge NSX Data Center for vSphere](#)
- [Configurazione dei servizi gateway edge NSX Data Center for vSphere](#)
- [Visualizzazione dell'utilizzo delle reti e delle allocazioni IP in un gateway edge](#)
- [Modifica delle proprietà dei gateway edge](#)
- [Ridistribuzione di un gateway edge](#)
- [Eliminazione di un gateway edge](#)
- [Statistiche e registri per un gateway edge](#)
- [Abilitazione dell'accesso a un gateway edge dalla riga di comando SSH](#)

Utilizzo dei cluster edge di NSX Data Center for vSphere

Per isolare i carichi di lavoro di calcolo dai carichi di lavoro di rete, VMware Cloud Director supporta l'oggetto cluster edge. Un cluster edge è composto da un pool di risorse di vSphere e da

un criterio di storage utilizzati solo per i gateway edge del VDC dell'organizzazione. I virtual data center del provider non possono utilizzare le risorse dedicate ai cluster edge e i cluster edge non possono utilizzare le risorse dedicate ai virtual data center del provider.

I cluster edge forniscono un dominio di trasmissione L2 dedicato, che riduce le dispersioni VLAN e garantisce la sicurezza e l'isolamento della rete. Ad esempio, il cluster edge può contenere VLAN aggiuntive per il peering con i router fisici.

È possibile creare un numero qualsiasi di cluster edge. È possibile assegnare un cluster edge a un VDC dell'organizzazione come cluster edge primario o secondario.

- Il cluster edge primario per un VDC dell'organizzazione viene utilizzato per l'appliance edge principale del gateway edge del VDC dell'organizzazione.
- Il cluster edge secondario per un VDC dell'organizzazione viene utilizzato per l'appliance edge di standby quando un gateway edge è in modalità di disponibilità elevata.

VDC dell'organizzazione diversi possono condividere cluster edge o possono avere i propri cluster edge dedicati.

A partire da vCloud Director 9.7, il precedente processo per l'utilizzo dei metadati per il controllo del posizionamento del gateway edge è stato deprecato. Vedere <https://kb.vmware.com/kb/2151398>.

È possibile migrare i gateway edge legacy in cluster edge appena creati ridistribuendo tali gateway edge. Vedere [Ridistribuzione di un gateway edge](#).

Preparazione dell'ambiente per un cluster edge

- 1 In vSphere, creare il pool di risorse per il cluster edge di destinazione.

Se un virtual data center dell'organizzazione utilizza un pool di reti VLAN, il pool di reti VLAN e il cluster edge per questo virtual data center dell'organizzazione devono trovarsi nello stesso commutatore distribuito di vSphere.

- 2 Se un virtual data center dell'organizzazione utilizza un pool di reti VXLAN, in NSX aggiungere il cluster edge alla zona di trasporto VXLAN, quindi sincronizzare il pool di reti VXLAN in VMware Cloud Director.

- 3 In vSphere creare il profilo di storage del cluster edge.

Creazione e gestione di cluster edge

Dopo aver preparato l'ambiente, per creare e gestire i cluster edge, è necessario utilizzare i metodi `EdgeClusters` di VMware Cloud Director OpenAPI. Vedere *Guida introduttiva a VMware Cloud Director OpenAPI* all'indirizzo <https://code.vmware.com>.

La visualizzazione dei cluster edge richiede il diritto **Visualizza cluster edge**. La creazione, l'aggiornamento e l'eliminazione di cluster edge richiedono il diritto di **Gestisci cluster edge**.

Quando si crea un cluster edge, è necessario specificare il nome, il pool di risorse di vSphere e il nome del profilo di storage.

Dopo aver creato un cluster edge, è possibile modificarne il nome e la descrizione. Dopo aver eliminato o spostato i gateway edge che contiene, è possibile eliminare un cluster edge.

Assegnazione di un cluster edge a un VDC dell'organizzazione

Dopo aver creato un cluster edge, è possibile assegnarlo a un VDC dell'organizzazione aggiornando il profilo di rete del VDC dell'organizzazione. È possibile assegnare un cluster edge a un VDC dell'organizzazione come cluster edge primario o secondario.

Se non si assegna un cluster edge secondario, l'appliance edge di standby di un gateway edge in modalità di disponibilità elevata viene distribuita nel cluster edge primario, ma su un host diverso dall'host che esegue l'appliance edge primaria.

Per aggiornare, visualizzare ed eliminare i profili di rete del VDC dell'organizzazione, è necessario utilizzare i metodi `VdcNetworkProfile` di VMware Cloud Director OpenAPI. Vedere *Guida introduttiva a VMware Cloud Director OpenAPI* all'indirizzo <https://code.vmware.com>.

Considerazioni:

- I cluster edge primario e secondario devono trovarsi nello stesso commutatore distribuito di vSphere.
- Se il VDC dell'organizzazione utilizza un pool di reti VXLAN, la zona di trasporto NSX deve occupare i cluster di calcolo ed edge.
- Se il VDC dell'organizzazione utilizza un pool di reti VLAN, i cluster edge e i cluster di calcolo devono essere nello stesso commutatore distribuito di vSphere.

Se si aggiorna di nuovo il cluster edge primario o secondario di un VDC dell'organizzazione, per trasferire un gateway edge esistente nel nuovo cluster, è necessario ridistribuire il gateway edge. Vedere [Ridistribuzione di un gateway edge](#).

Aggiunta di un gateway edge NSX Data Center for vSphere

Un gateway edge NSX Data Center for vSphere fornisce una rete VDC dell'organizzazione instradata con connettività a reti esterne e può fornire servizi come bilanciamento del carico, NAT e firewall.

A partire da VMware Cloud Director 9.7, i gateway edge NSX Data Center for vSphere vengono distribuiti nei cluster edge creati in precedenza e assegnati al VDC dell'organizzazione.

È possibile aggiungere un gateway edge IPv4 o IPv6 che si connette a una o più reti esterne.

Nota I gateway edge IPv6 supportano servizi limitati. I gateway edge IPv6 supportano i firewall edge, i firewall distribuiti e il routing statico.

Prerequisiti

- Per informazioni sui requisiti di sistema per la distribuzione di un gateway edge NSX Data Center for vSphere, consultare *Guida per l'amministratore di NSX*.

- Se si desidera distribuire il gateway edge in un cluster edge dedicato, creare e assegnare un cluster edge al virtual data center dell'organizzazione. Vedere [Utilizzo dei cluster edge di NSX Data Center for vSphere](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra, fare clic su **Gateway edge** e su **Nuovo**.
- 3 Selezionare il virtual data center dell'organizzazione supportato da NSX-V in cui si desidera creare il gateway edge e fare clic su **Avanti**.
- 4 Immettere un nome e, facoltativamente, una descrizione per il nuovo gateway edge.
- 5 Attivare o lasciare disattivata ciascuna impostazione generale del gateway edge.

Impostazione generale	Descrizione
Routing distribuito	Configura il gateway edge per fornire il routing logico distribuito.
Modalità FIPS	Configura il gateway edge per l'utilizzo della modalità NSX FIPS.
High Availability	Abilita il failover automatico in un gateway edge di backup.

- 6 Selezionare la configurazione del gateway edge per le risorse di sistema e fare clic su **Avanti**.

Configurazione	Descrizione
Compatta	Richiede meno memoria e risorse di elaborazione.
Large	Offre capacità e prestazioni migliori rispetto alla configurazione Compatta. Le configurazioni Large e X-Large offrono funzioni di sicurezza identiche.
X-Large	Utilizzata in ambienti che hanno un bilanciamento del carico con un grande numero di sessioni simultanee.
Quad Large	Utilizzata in ambienti a elevata velocità effettiva. Richiede una velocità di connessione elevata.

- 7 Selezionare una o più subnet delle reti esterne a cui il gateway edge può connettersi e fare clic su **Avanti**.

Se è stato assegnato un cluster edge al VDC dell'organizzazione, l'elenco visualizzato contiene le reti esterne accessibili per questo cluster edge.

- 8 (Facoltativo) Configurare una rete come gateway predefinito.
 - a Attivare l'opzione **Configura gateway predefinito**.
 - b Fare clic sul pulsante di opzione accanto al nome della rete esterna di destinazione e sul pulsante di opzione accanto all'indirizzo IP di destinazione.
 - c (Facoltativo) Attivare l'opzione **Utilizza il gateway predefinito per l'inoltro DNS**.
- 9 Fare clic su **Avanti**.

- 10 Attivare o lasciare disattivata ciascuna impostazione avanzata del gateway edge e fare clic su **Avanti**.

Impostazione avanzata	Descrizione
Impostazioni IP	È possibile inserire manualmente un indirizzo IP per ogni subnet nel gateway edge.
Sottoalloca pool IP	È possibile sottoallocare più pool di IP statici dai pool di IP disponibili di ciascuna rete esterna nel gateway edge.
Limiti classificazione	È possibile configurare i limiti di classificazione in entrata e in uscita per ciascuna rete esterna nel gateway edge.

- 11 (Facoltativo) Se sono state abilitate una o più impostazioni avanzate nel [passaggio 10](#), configurare ciascuna impostazione abilitata.

Impostazione avanzata	Passaggi
Impostazioni IP	<p>Per ogni rete nel gateway edge, nella cella Indirizzi IP, immettere un indirizzo IP e fare clic su Avanti.</p> <p>Se non si immette un indirizzo IP per una rete, il sistema assegna un indirizzo IP arbitrario a tale rete.</p>
Sottoalloca pool IP	<ol style="list-style-type: none"> Fare clic sul pulsante di opzione accanto al nome di una rete esterna e fare clic su Modifica. È possibile visualizzare i pool di IP disponibili per questa rete esterna e i pool di IP sottoallocati correnti, se configurati. Modificare i pool di IP sottoallocati per questa rete esterna e fare clic su Salva. È possibile aggiungere indirizzi e intervalli IP dagli intervalli dei pool di IP disponibili. Fare clic su Salva. Il sistema combina gli intervalli IP che si sovrappongono. Fare clic su Avanti. <p>Nota L'allocazione degli indirizzi IP a un gateway edge è un processo in cui il provider assegna la proprietà degli indirizzi IP al gateway. VMware Cloud Director configura automaticamente l'interfaccia del gateway appropriata con gli indirizzi secondari durante il processo di allocazione. Se uno qualsiasi degli indirizzi IP viene utilizzato al di fuori di VMware Cloud Director, può causare conflitti di indirizzi IP.</p>
Limiti classificazione	Per ogni rete esterna nel gateway edge, attivare l'interruttore Abilita , immettere i limiti nelle celle Classificazione in entrata e Classificazione in uscita e fare clic su Avanti .

- 12 Controllare la pagina **Pronto per il completamento** e fare clic su **Fine**.

Configurazione dei servizi gateway edge NSX Data Center for vSphere

In un gateway edge è possibile configurare servizi come DHCP, firewall, Network Address Translation (NAT) e VPN.

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 del firewall distribuito in un virtual data center dell'organizzazione](#).

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 disabilitare o abilitare un firewall del gateway edge.

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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:

- Selezionare il protocollo del servizio.
- Digitare i numeri di porta per la porta di origine e quella di destinazione oppure specificare **qualsiasi**.
- 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic sulla scheda **Firewall**.
- 3 Consente di gestire le regole firewall.
 - Per disabilitare una regola, fare clic sul segno di spunta verde nella relativa cella **N.**. Il segno di spunta verde diventa un'icona di disabilitazione di colore rosso. Se la regola è disabilitata e si desidera abilitarla, fare clic sull'icona di disabilitazione 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**.

Applicazione delle impostazioni del server syslog a un gateway edge NSX Data Center for vSphere

Se è stata abilitata la registrazione per una o più regole del firewall del gateway edge, il gateway edge si connette al server syslog. Se è stato creato un gateway edge prima della configurazione iniziale del server syslog o se sono state modificate le impostazioni del server syslog, è necessario sincronizzare le impostazioni del server syslog per questo gateway edge.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge**.
- 3 Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e quindi su **Sincronizza syslog**.
- 4 Per confermare, fare clic su **OK**.

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 abilitato per il servizio DHCP, 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 disabilitare il servizio DHCP, quindi abilitarlo 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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 .
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.

Opzione	Descrizione
Il lease non ha scadenza	<p>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.</p> <p>Se si seleziona questa opzione, il campo Durata lease viene impostato su Infinito.</p>
Durata lease (secondi)	<p>Intervallo di tempo (in secondi) che indica la durata del lease degli indirizzi IP assegnati dal DHCP ai client.</p> <p>La durata del lease predefinita è un giorno (86400 secondi).</p> <p>Nota Se si seleziona Il lease non ha scadenza, non è possibile specificare una durata del lease.</p>

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.

Opzione	Descrizione
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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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**.

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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	<p>Digitare l'indirizzo IP richiesto oppure selezionare l'indirizzo IP allocato nell'elenco.</p> <p>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.</p>
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	<p>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.</p> <p>I messaggi di ICMP vengono identificati dal campo del tipo. Per impostazione predefinita, il tipo di ICMP è impostato su Qualsiasi.</p>
IP/Intervallo convertito	<p>Digitare l'indirizzo IP o un intervallo di indirizzi IP in cui verranno convertiti gli indirizzi di destinazione dei pacchetti in entrata.</p> <p>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.</p>
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.

Opzione	Descrizione
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 abilitare 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 abilitare 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 avanzata del routing

È possibile configurare le funzionalità di routing statico e dinamico fornite dal software NSX per i gateway edge 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, vedere *Routing* nella documentazione *per l'amministratore di NSX*.

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 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.

Opzione	Descrizione
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>
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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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 ridistribuzione 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

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.


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

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Passare a **Bilanciamento del carico** > **Monitoraggio del servizio**.
- 3 Fare clic sul pulsante **Crea** ().
- 4 Immettere un nome per il monitor del servizio.

5 (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.
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 vengono abilitate o disabilitate.
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>

Esempio: Estensioni supportate per ciascun protocollo**Tabella 7-1. 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.
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 User Agent.
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 7-2. 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=AUTH_PAIR	Specifica nome utente:password nei siti con autenticazione di base.

Tabella 7-3. 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= <i>STRING</i>	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= <i>INTEGER</i>	Chiude la connessione quando viene ricevuto un numero di byte superiore a quello specificato.
delay= <i>INTEGER</i>	Attende il numero di secondi specificato tra l'invio della stringa e il polling di una risposta.
certificate= <i>INTEGER</i> [, <i>INTEGER</i>]	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= <i>DOUBLE</i>	Specifica il tempo di risposta in secondi trascorso il quale viene restituito uno stato di avviso.
critical= <i>DOUBLE</i>	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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.

Opzione	Descrizione
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 <code>host</code> 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.


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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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/configuration-1.5.html>.

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.
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](#).

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](#)

Protezione dell'accesso mediante l'utilizzo di reti VPN

È possibile configurare le funzionalità VPN fornite dal software NSX per i gateway edge 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 dei certificati SSL](#).

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 abilitate 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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 abilitata per impostazione predefinita. È possibile modificare il livello dei messaggi per i quali effettuare 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.
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 abilitare o disabilitare 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.

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 abilitate 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 seleziona Abilita 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 disabilitare l'ottimizzazione TCP per tale rete privata. Inoltre, la rete privata per il server FTP deve essere abilitata e viene visualizzata nella tabella nella schermata sopra la rete privata ottimizzata con 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 abilitato 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 abilita l'ottimizzazione 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	Abilitare o disabilitare la rete privata.

4 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 abilitato o disabilitato.
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 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 abilitato o disabilitato.

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) Disabilitare la riconnessione automatica.

l'opzione **Abilita riconnessione automatica** è abilitata per impostazione predefinita. Se la riconnessione automatica è abilitata, il client VPN SSL riconnette automaticamente gli utenti quando si disconnettono.
- 5 (Facoltativo) Facoltativamente, fare in modo che il client informi gli utenti remoti quando è disponibile un aggiornamento del client.

Questa opzione è disabilitata per impostazione predefinita. Se si abilita 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, in **Risorse**, selezionare **Risorse cloud**.
- b Nel riquadro a sinistra fare clic su **Gateway edge**.
- c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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 Nella scheda **VPN IPsec**, fare clic su **Siti VPN IPsec**.
- 2 Fare clic sul pulsante **Aggiungi** ()
- 3 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. 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 precondivisa in modo da poter aggiornare la chiave condivisa.</p>
Chiave precondivisa	<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>
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.

4 Fare clic su **Mantieni**.

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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](#).

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.

Procedura

1 [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**.

2 [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.

3 [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.

4 [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.

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.
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	Le credenziali dell'utente nel sito peer devono essere uguali alle credenziali sul lato client.
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**.

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.
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 (Facoltativo) Per configurare le opzioni avanzate, fare clic sulla scheda **Avanzato client**.
- 4 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	

- 5 Per abilitare la convalida del certificato del server, fare clic su **Modifica certificato CA** e selezionare il certificato CA appropriato.

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 operazione disabilita 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 disabilitato e i dettagli relativi alla configurazione vengono rimossi dal gateway edge.

Gestione dei certificati SSL

Il software NSX 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.
- 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Nella scheda **Certificati** fare clic su **CSR**.
- 3 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.	

Opzione	Descrizione
Dimensione chiave	Immettere le dimensioni della chiave in bit. Il valore minimo è 2048 bit.
Descrizione	(Facoltativo) Immettere una descrizione per il certificato.

4 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 una 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.

- 2 Nella tabella nella schermata, selezionare la richiesta CSR per cui si sta importando il certificato firmato dall'autorità di certificazione.
- 3 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Nell'elenco, selezionare la richiesta di firma del certificato (CSR) che si desidera utilizzare per questo certificato autofirmato e fare clic su **CSR autofirmato**.
- 3 Digitare il numero di giorni per cui il certificato autofirmato è valido.
- 4 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic su **Certificato CA**.
- 3 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-----.
- 4 (Facoltativo) Digitare una descrizione.
- 5 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic su **CRL**.
- 3 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-----`.
- 4 (Facoltativo) Digitare una descrizione.
- 5 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic su **Certificato di servizio**.

3 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-----.

4 Immettere i dati in formato PEM della chiave privata del certificato.

- 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-----.

5 Immettere una passphrase della chiave privata e confermarla.**6** (Facoltativo) Digitare una descrizione.**7** 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 di oggetti personalizzato

Il software NSX 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**. Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.

Procedura

1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su VDC dell'organizzazione. c Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. d Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su Gateway edge. c Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. d Fare clic sulla scheda 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 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**. Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.

Procedura

1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su VDC dell'organizzazione. c Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. d Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su Gateway edge. c Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. d Fare clic sulla scheda 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 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 servizi disponibili utilizzando la pagina **Raggruppamento di oggetti**.

Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.

Procedura

1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su VDC dell'organizzazione. c Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. d Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su Gateway edge. c Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. d Fare clic sulla scheda 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**. Per aprire questa pagina, è necessario passare alle impostazioni del firewall distribuito del VDC dell'organizzazione o alle impostazioni dei servizi di un gateway edge appartenente al VDC dell'organizzazione.

Procedura

1 Aprire la pagina **Raggruppamento di oggetti**.

Opzione	Azione
Dalle impostazioni del firewall distribuito del VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su VDC dell'organizzazione. c Selezionare il pulsante di opzione accanto al nome del virtual data center dell'organizzazione di destinazione e scegliere Gestisci firewall. d Fare clic sulla scheda Raggruppamento di oggetti.
Dalle impostazioni dei servizi di un gateway edge nel VDC dell'organizzazione	<ul style="list-style-type: none"> a Nella barra di navigazione superiore, in Risorse, selezionare Risorse cloud. b Nel riquadro a sinistra fare clic su Gateway edge. c Selezionare il pulsante di opzione accanto al nome di un gateway edge che viene utilizzato per il virtual data center dell'organizzazione di destinazione e fare clic su Servizi. d Fare clic sulla scheda 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.

Visualizzazione dell'utilizzo delle reti e delle allocazioni IP in un gateway edge

È possibile visualizzare le reti in un gateway edge con informazioni relative all'utilizzo di pool di IP e alle subnet. È inoltre possibile visualizzare l'indirizzo IP allocato a ciascuna rete.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 3 Per visualizzare le reti esterne con le informazioni relative all'utilizzo del pool di IP e alle subnet, fare clic sulla scheda **Reti esterne > Reti e subnet**.
- 4 Per visualizzare le reti esterne con le informazioni relative agli indirizzi IP e alle categorie, fare clic sulla scheda **Reti esterne > Allocazioni IP**.

Modifica delle proprietà dei gateway edge

Abilitazione o disabilitazione del routing distribuito in un gateway edge

Dopo aver abilitato il routing distribuito VMware Cloud Director in un gateway edge, l'amministratore dell'organizzazione può creare molte reti di virtual data center dell'organizzazione instradate con interfacce distribuite connesse a questo gateway edge. Il traffico in tali reti viene ottimizzato per la comunicazione tra macchine virtuali.

Prerequisiti

L'istanza di NSX Manager di supporto è configurata con un cluster di NSX Controller. Vedere *Guida per l'amministratore di NSX*.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge**.
- 3 Selezionare il pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Abilita routing distribuito** o **Disabilita routing distribuito**.
- 4 Per confermare, fare clic su **OK**.

Modifica delle impostazioni di reti esterne e di gateway edge

Per modificare le impostazioni delle reti esterne e del gateway edge, è possibile utilizzare la procedura guidata **Modifica gateway edge**, che contiene le stesse pagine della procedura guidata utilizzata per creare il gateway edge.

È possibile modificare le impostazioni configurate in fase di aggiunta del gateway edge. Vedere [Aggiunta di un gateway edge NSX Data Center for vSphere](#).

Per modificare l'impostazione del routing distribuito, vedere [Abilitazione o disabilitazione del routing distribuito in un gateway edge](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge**.
- 3 Fare clic sul pulsante di opzione accanto al nome del gateway edge che si desidera modificare e fare clic su **Modifica**.
- 4 Per modificare le impostazioni del gateway edge, passare attraverso le pagine della procedura guidata di **modifica del gateway edge** facendo clic su **Avanti** e, nella pagina **Pronto per il completamento**, fare clic su **Fine**.

Modifica delle impostazioni generali di un gateway edge

È possibile modificare il nome e la descrizione di un gateway edge, abilitare o disabilitare la modalità FIPS e lo stato di alta disponibilità e modificare la configurazione della dimensione del gateway edge.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 3 Nell'angolo superiore destro della scheda **Generale**, fare clic su **Modifica**.
- 4 (Facoltativo) Modificare il nome e la descrizione del gateway edge.
- 5 (Facoltativo) Attivare o disattivare tutte le impostazioni generali del gateway edge.

Impostazione generale	Descrizione
Modalità FIPS	Configura il gateway edge per l'utilizzo della modalità NSX FIPS.
High Availability	Abilita il failover automatico in un gateway edge di backup.

- 6 (Facoltativo) Modificare la configurazione del gateway edge per le risorse di sistema.

Configurazione	Descrizione
Compatta	Richiede meno memoria e risorse di elaborazione.
Large	Offre capacità e prestazioni migliori rispetto alla configurazione Compatta. Le configurazioni Large e X-Large offrono funzioni di sicurezza identiche.
X-Large	Utilizzata in ambienti che hanno un bilanciamento del carico con un grande numero di sessioni simultanee.
Quad Large	Utilizzata in ambienti a elevata velocità effettiva. Richiede una velocità di connessione elevata.

- 7 Per confermare le modifiche, fare clic su **Salva**.

Modifica del gateway predefinito di un gateway edge

È possibile modificare la rete utilizzata da un gateway edge come gateway predefinito.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 3 Nella scheda **Reti esterne > Gateway predefinito**, fare clic su **Modifica** nell'angolo superiore destro.

- 4 (Facoltativo) Configurare una rete come gateway predefinito.
 - a Attivare l'opzione **Configura gateway predefinito**.
 - b Selezionare il pulsante di opzione accanto al nome della rete esterna di destinazione e il pulsante di opzione accanto all'indirizzo IP di destinazione.
 - c (Facoltativo) Attivare l'opzione **Utilizza il gateway predefinito per l'inoltro DNS**.
- 5 Per confermare le modifiche, fare clic su **Salva**.

Modifica delle impostazioni IP di un gateway edge

È possibile modificare le impostazioni IP per le reti esterne in un gateway edge.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 3 Nella scheda **Reti esterne > Impostazioni IP**, fare clic su **Modifica**.
- 4 Per ogni rete nel gateway edge, nella cella **Indirizzi IP**, immettere un indirizzo IP o lasciare vuota la cella.

Se non si immette un indirizzo IP per una rete, il sistema assegna un indirizzo IP arbitrario a tale rete.
- 5 Per confermare le modifiche, fare clic su **Salva**.

Modifica dei pool di IP sottoallocati in un gateway edge

È possibile sottoallocare più pool di IP statici dai pool di IP disponibili di una rete esterna in un gateway edge.

Nota L'allocazione degli indirizzi IP a un gateway edge tramite sottoallocazione è un processo in cui il provider assegna la proprietà degli indirizzi IP al gateway. VMware Cloud Director configura automaticamente l'interfaccia del gateway appropriata con gli indirizzi secondari durante il processo di sottoallocazione, che può causare conflitti di indirizzi IP se uno qualsiasi degli indirizzi IP viene utilizzato all'esterno di VMware Cloud Director.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 3 Fare clic sulla scheda **Reti esterne > Pool di IP sottoallocati**.

È possibile visualizzare i pool di IP sottoallocati correnti per ogni rete esterna in questo gateway edge.

- 4 Fare clic sul pulsante di opzione accanto al nome di una rete esterna e fare clic su **Modifica**.

È possibile visualizzare i pool di IP disponibili per questa rete esterna e i pool di IP sottoallocati correnti, se configurati.

- 5 Modificare i pool di IP sottoallocati per questa rete esterna e fare clic su **Salva**.

È possibile aggiungere, modificare e rimuovere indirizzi IP e intervalli di indirizzi IP dagli intervalli dei pool di IP disponibili.

Risultati

Il sistema combina gli intervalli IP che si sovrappongono.

Modifica dei limiti di classificazione in un gateway edge

È possibile configurare i limiti di classificazione in entrata e in uscita per ciascuna rete esterna nel gateway edge.

I limiti di classificazione sono validi solo per le reti esterne supportate da gruppi di porte distribuiti con binding statico.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 3 Nella scheda **Reti esterne > Limiti classificazione**, fare clic su **Modifica** nell'angolo superiore destro.

È possibile visualizzare i limiti di classificazione correnti per ogni rete esterna in questo gateway edge.

- 4 Modificare i limiti di classificazione e fare clic su **Salva**.

Per ogni rete esterna nel gateway edge, è possibile abilitare o disabilitare i limiti di classificazione e modificare le classificazioni in entrata e in uscita.

Ridistribuzione di un gateway edge

È possibile eliminare e distribuire una nuova appliance gateway edge con le configurazioni più recenti.

Se i servizi edge non funzionano come previsto, è possibile ridistribuire l'appliance del gateway edge.

Quando si ridistribuisce un gateway edge, VMware Cloud Director lo elimina e lo ricrea con le configurazioni più recenti.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.

- 2 Nel riquadro a sinistra fare clic su **Gateway edge**.
- 3 Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Ridistribuisce**.
- 4 Per confermare, fare clic su **OK**.

Risultati

La macchina virtuale del gateway edge viene sostituita con una nuova macchina virtuale e tutti i servizi vengono ripristinati.

Eliminazione di un gateway edge

È possibile rimuovere un gateway edge dal virtual data center dell'organizzazione.

Prerequisiti

Eliminare tutte le reti del virtual data center dell'organizzazione che utilizzano il gateway edge di destinazione.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge**.
- 3 Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e quindi su **Elimina**.
- 4 Per confermare, fare clic su **Elimina**.

Statistiche e registri per un gateway edge

È possibile visualizzare le statistiche e i registri per un gateway edge.

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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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 le statistiche di connessione relative ai servizi firewall e di bilanciamento del carico. 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

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

Procedura

1 Aprire i servizi gateway edge.

- Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- Nel riquadro a sinistra fare clic su **Gateway edge**.
- Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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 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, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione 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.

Gestione dei gateway edge NSX-T Data Center



Un gateway edge NSX-T Data Center fornisce una rete VDC dell'organizzazione instradata con connettività a reti esterne e proprietà di gestione IP. Può inoltre fornire servizi quali firewall, Network Address Translation (NAT), VPN IPsec, inoltro DNS e DHCP, abilitato per impostazione predefinita.

Questo capitolo include i seguenti argomenti:

- Reti esterne dedicate
- Aggiunta di un gateway edge NSX-T Data Center
- Aggiunta di un gruppo di firewall a un gateway edge NSX-T
- Aggiunta di una regola del firewall del gateway edge NSX-T
- Aggiunta di una regola SNAT o DNAT a un gateway edge NSX-T
- Configurazione di un servizio di inoltro DNS su un gateway edge NSX-T
- Modifica delle allocazioni IP di un gateway edge NSX-T
- Allocazione IP rapida
- Creazione di profili delle porte dell'applicazione personalizzata
- VPN basata su criteri IPsec per i gateway edge NSX-T Data Center
- Configurazione dei servizi della rete esterna dedicata

Reti esterne dedicate

Per fornire una topologia di rete completamente instradata in un virtual data center, è possibile 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 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.

Se si dedica una rete esterna a un gateway edge, si fornisce ai tenant servizi gateway edge aggiuntivi, come la gestione della comunicazione della route e la configurazione di BGP (Border Gateway Protocol).

Il tenant può decidere quale delle reti tenant 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.

È possibile dedicare una rete esterna a un gateway edge NSX-T Data Center durante la creazione del gateway edge o in un secondo momento, modificando le impostazioni generali del gateway edge.

Aggiunta di un gateway edge NSX-T Data Center

Un gateway edge NSX-T Data Center fornisce una rete VDC dell'organizzazione instradata con connettività a reti esterne e può fornire servizi come bilanciamento del carico, NAT e firewall.

Prerequisiti

Per informazioni sui requisiti di sistema per la distribuzione di un gateway edge NSX-T Data Center, consultare *Guida all'amministrazione di NSX-T Data Center*.

A partire dalla versione 10.1, VMware Cloud Director supporta una configurazione di rete esterna dedicata. Se si dedica una rete esterna a un gateway edge, si fornisce ai tenant servizi gateway edge aggiuntivi, come la gestione della comunicazione della route e la configurazione di BGP (Border Gateway Protocol). Per ulteriori informazioni, vedere [Reti esterne dedicate](#).

VMware Cloud Director 10.1 supporta la configurazione del cluster edge di NSX-T Data Center di base. Per ulteriori informazioni sulla creazione dei cluster edge, vedere *Guida all'installazione di NSX-T Data Center*.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge**.
- 3 Fare clic su **Nuovo**.
- 4 Selezionare il VDC dell'organizzazione supportato da NSX-T Data Center in cui si desidera creare il gateway edge e fare clic su **Avanti**.
- 5 Immettere un nome e, facoltativamente, una descrizione per il nuovo gateway edge.
- 6 Per abilitare BGP e l'annuncio della route per il gateway edge, attivare l'opzione **Rete esterna dedicata** e fare clic su **Avanti**.
- 7 Selezionare una rete esterna a cui collegare il nuovo gateway edge e fare clic su **Avanti**.

Se si attiva l'opzione **Rete esterna dedicata**, gli altri gateway edge non possono accedere a questa rete esterna.

- 8 Selezionare un cluster edge in cui distribuire il gateway edge e fare clic su **Avanti**.

Se si desidera eseguire i servizi del gateway edge in un cluster edge diverso da quello associato alla rete esterna, è possibile configurare il gateway edge in modo che utilizzi un altro cluster edge.

- Utilizzare il cluster edge della rete esterna a cui è connesso il gateway edge.
- Effettuare la selezione in un elenco di cluster edge disponibili per il VDC dell'organizzazione in cui si sta distribuendo il gateway edge.

- 9 (Facoltativo) Modificare gli indirizzi IP o gli intervalli di indirizzi IP allocati al gateway edge e fare clic su **Avanti**.

- 10 Controllare la pagina **Pronto per il completamento** e fare clic su **Fine**.

Aggiunta di un gruppo di firewall a un gateway edge NSX-T

Per creare regole del firewall e aggiungerle a un gateway edge NSX-T, è innanzitutto necessario creare gruppi di firewall. I gruppi di firewall sono gruppi di oggetti a cui si applicano le regole del firewall. La combinazione di più oggetti in gruppi di firewall consente di ridurre il numero totale di regole del firewall da creare.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic sul gateway edge NSX-T, quindi su **Sicurezza**.
- 3 Fare clic sulla scheda **Gruppi**, quindi su **Nuovo**.
- 4 Immettere un nome e, facoltativamente, una descrizione per il gruppo di firewall.
- 5 Immettere un indirizzo IP o un intervallo di indirizzi IP per le macchine virtuali che vengono incluse nel gruppo e fare clic su **Aggiungi**.
- 6 Per salvare il gruppo di firewall, fare clic su **Salva**.

Risultati

Un gruppo di firewall è stato creato e aggiunto al gateway edge NSX-T.

Operazioni successive

[Aggiunta di una regola del firewall del gateway edge NSX-T](#)

Aggiunta di una regola del firewall del gateway edge NSX-T

Per controllare il traffico di rete in entrata e in uscita da e verso un gateway edge NSX-T, è possibile creare regole del firewall.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic sul gateway edge, quindi su **Servizi**.
- 3 Se la schermata **Firewall** non è già visualizzata, fare clic sulla scheda **Firewall**.
- 4 Fare clic su **Modifica regole**.
- 5 Selezionare una regola firewall e fare clic sul pulsante **Aggiungi sopra**.
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 negare 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 proveniente da 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.
Protocollo IP	Selezionare se applicare la regola al traffico IPv4 o IPv6.

Opzione	Descrizione
Direzione	Selezionare la direzione del traffico a cui applicare la regola.
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.

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 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic sul gateway edge e 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.
Stato	Per abilitare la regola al momento della creazione, attivare l'opzione Stato .
Tipo di interfaccia	Dal menu a discesa, selezionare SNAT o NO SNAT.
IP esterno	In base al tipo di regola che si sta creando, scegliere una delle opzioni. <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 intervallo di indirizzi IP per le 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 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.
Registrazione	Per registrare la conversione degli indirizzi da parte di questa regola, attivare l'opzione Registrazione .

- 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.
Stato	Per abilitare la regola al momento della creazione, attivare l'interruttore Stato .
Tipo di interfaccia	Dal menu a discesa, selezionare DNAT o NO DNAT.

Opzione	Descrizione
IP esterno	Immettere l'indirizzo IP pubblico del gateway edge per il quale si sta configurando la regola DNAT. Gli indirizzi IP inseriti devono appartenere all'intervallo IP sottoallocato del gateway edge.
Applicazione	(Facoltativo) Selezionare un profilo di porta dell'applicazione specifico a cui applicare la regola. 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.
IP interno	In base al tipo di regola che si sta creando, scegliere una delle opzioni. <ul style="list-style-type: none"> ■ Se si crea una regola DNAT, immettere l'indirizzo IP o l'intervallo 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.
Porta interna	(Facoltativo) Selezionare la porta o l'intervallo di porte in cui la regola DNAT esegue la conversione per i pacchetti in entrata per le macchine virtuali.
Registrazione	Per registrare la conversione degli indirizzi da parte di questa regola, attivare l'opzione Registrazione .

- 6 Fare clic su **Salva**.
- 7 Per configurare regole aggiuntive, ripetere questi passaggi.

Configurazione di un servizio di inoltrato DNS su un gateway edge NSX-T

Per inoltrare query DNS a server DNS esterni, configurare un server di inoltrato DNS.

Come parte della configurazione del servizio di inoltrato DNS, è anche possibile aggiungere zone di inoltrato condizionale. Una zona di inoltrato 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 inoltrato corrispondente.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic sul gateway edge, quindi su **Servizi**.
- 3 Fare clic su **DNS** e, nella sezione **Server di inoltrato DNS**, fare clic su **Modifica**.
- 4 Per abilitare il servizio del server di inoltrato 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**.

Modifica delle allocazioni IP di un gateway edge NSX-T

È possibile allocare più indirizzi IP di una rete esterna a un gateway edge.

Procedura

- 1 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic sul gateway edge, quindi su **Allocazioni IP**.

Nelle griglie di gestione IP, è possibile visualizzare gli indirizzi IP allocati al gateway edge e quelli attualmente utilizzati dal gateway edge.
- 3 Nella sezione **IP allocati**, fare clic su **Gestione IP**.

Nella griglia **Gestione IP**, è possibile visualizzare l'utilizzo dell'IP per ciascuna rete esterna disponibile per l'uso da parte del gateway edge.
- 4 Immettere un intervallo IP e fare clic su **Aggiungi**.
- 5 Fare clic su **Salva**.

Risultati

Gli indirizzi IP vengono allocati al gateway edge.

Operazioni successive

Visualizzare gli indirizzi IP allocati al gateway edge, aggiungere altri indirizzi IP o rimuoverli in base alle esigenze.

Allocazione IP rapida

È possibile allocare gli indirizzi IP da una subnet di rete esterna a un gateway edge senza immettere specifici indirizzi IP o intervalli di indirizzi IP utilizzando l'allocazione IP rapida.

Procedura

1 Aprire i servizi gateway edge.

- a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- b Nel riquadro a sinistra fare clic su **Gateway edge**.
- c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.

2 Fare clic sul gateway edge, quindi su **Allocazioni IP**.

Nelle griglie di gestione IP, è possibile visualizzare gli indirizzi IP allocati al gateway edge e quelli attualmente utilizzati dal gateway edge.

3 Nella sezione **IP allocati**, fare clic su **Allocazione IP rapida**.

4 Nel menu a discesa, selezionare una subnet da cui assegnare gli indirizzi IP.

Se sono disponibili più subnet, selezionando l'opzione **Qualsiasi** verranno allocati gli indirizzi IP da una o più subnet.

5 Immettere il numero di indirizzi IP da allocare al gateway edge e fare clic su **Salva**.

Il numero deve essere inferiore al numero di indirizzi IP disponibili nella subnet selezionata.

Risultati

Gli indirizzi IP vengono allocati al gateway edge.

Operazioni successive

Visualizzare gli indirizzi IP allocati al gateway edge, aggiungere altri indirizzi IP o rimuoverli in base alle esigenze.

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 Aprire i servizi gateway edge.
 - a Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
 - b Nel riquadro a sinistra fare clic su **Gateway edge**.
 - c Fare clic sul pulsante di opzione accanto al nome del gateway edge di destinazione e fare clic su **Servizi**.
- 2 Fare clic sul gateway edge, quindi sulla scheda **Sicurezza**.
- 3 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](#) 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 redistribuzione 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, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 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 Scegliere una chiave precondivisa da immettere.

Nota La chiave precondivisa deve essere identica nell'altra estremità del tunnel VPN IPSec.

- 7 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.

- 8 Immettere almeno un indirizzo di subnet IP locale nella notazione CIDR da utilizzare per il tunnel VPN IPSec.
- 9 Immettere l'indirizzo IP per il sito remoto.
- 10 Immettere almeno un indirizzo di subnet IP remoto nella notazione CIDR da utilizzare per il tunnel VPN IPSec.
- 11 (Facoltativo) Per abilitare la registrazione, attivare l'opzione **Registrazione**.
- 12 Fare clic su **Salva**.
- 13 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, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 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).

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 di aver dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione. Vedere [Reti esterne dedicate](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 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.

Prerequisiti

- Verificare di aver dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione. Vedere [Reti esterne dedicate](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 3 In **Routing** fare clic su **BGP** e in **Configurazione** fare clic su **Modifica**.
- 4 Attivare l'opzione **Stato** per abilitare 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 abilitare la funzionalità di riavvio normale nel gateway edge perché i peering BGP da 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	Disabilita 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 abilitare ECMP.

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 di aver dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione. Vedere [Reti esterne dedicate](#).
- [Configurazione delle impostazioni generali BGP](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 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 redistribuzione 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 di aver dedicato una rete esterna a un gateway edge di NSX-T Data Center nell'organizzazione. Vedere [Reti esterne dedicate](#).
- 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, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel riquadro a sinistra fare clic su **Gateway edge** e quindi sul nome del gateway edge di destinazione.
- 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 disabilita 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.

Operazioni successive

È possibile visualizzare lo stato di ciascun router adiacente BGP, modificare o eliminare i router adiacenti BGP in base alle esigenze.

Gestione di istanze di vCenter Server dedicate

9

Con le istanze di vCenter Server dedicate, è possibile utilizzare VMware Cloud Director come punto di gestione centrale (CPOM) per gli ambienti vSphere.

Quando si aggiunge un'istanza di vCenter Server a VMware Cloud Director, è possibile specificare lo scopo dell'istanza.

vCenter Server dedicato

L'infrastruttura di un'istanza di vCenter Server collegata è incapsulata come Centro dati definito da software (SDDC) ed è completamente dedicata a un singolo tenant. È possibile creare un'istanza di vCenter Server dedicata abilitando l'accesso tenant per tale istanza. Dopo aver abilitato l'accesso tenant, è possibile pubblicare un'istanza di vCenter Server dedicata in un tenant.

vCenter Server condiviso

Il provider può utilizzare pool di risorse diversi dell'istanza di vCenter Server in più VDC del provider e quindi allocare tali pool di risorse a tenant diversi. Un'istanza di vCenter Server condivisa non può essere pubblicata nei tenant.

Nessuno

L'istanza di vCenter Server non ha uno scopo specifico.

VMware Cloud Director può fungere da server proxy HTTP per le istanze di vCenter Server dedicate e le istanze di vCenter Server che non hanno uno scopo impostato.

Con le istanze di vCenter Server dedicate, è possibile utilizzare VMware Cloud Director come punto di gestione centrale per tutti gli ambienti vSphere.

- È possibile dedicare le risorse di un'istanza di vCenter Server a un singolo tenant pubblicando l'istanza di vCenter Server dedicata corrispondente solo nella relativa organizzazione. Il tenant non condivide queste risorse con altri tenant. Il tenant può accedere a questa istanza di vCenter Server dedicata utilizzando un proxy interfaccia utente o API senza che sia necessaria una VPN.
- È possibile utilizzare VMware Cloud Director come directory lightweight per registrare tutte le istanze di vCenter Server.
- È possibile utilizzare VMware Cloud Director come endpoint API per tutte le istanze di vCenter Server.

È possibile abilitare l'accesso tenant e contrassegnare un'istanza di vCenter Server come dedicata durante o dopo il collegamento dell'istanza di vCenter Server di destinazione a VMware Cloud Director. Vedere [Collegamento di un'istanza di vCenter Server da sola o insieme a un'istanza di NSX Manager](#).

Con un'istanza di vCenter Server collegata, è possibile creare un'istanza di vCenter Server condivisa o un'istanza di vCenter Server dedicata. Se è stata creata un'istanza di vCenter Server condivisa, non è possibile utilizzare questa istanza di vCenter Server per creare un'istanza di vCenter Server dedicata e viceversa.

È possibile creare proxy che possono essere utilizzati dai tenant per accedere all'ambiente di vSphere sottostante. Gli utenti possono accedere all'interfaccia utente o all'API dei componenti con proxy utilizzando i loro account VMware Cloud Director.

Le istanze di vCenter Server dedicate in VMware Cloud Director rimuovono il requisito per cui vCenter Server deve essere accessibile pubblicamente. Per controllare l'accesso, è possibile abilitare e disabilitare l'accesso tenant a un SDDC in VMware Cloud Director.

Un proxy è il punto di accesso a un componente di un SDDC, ad esempio un'istanza di vCenter Server, un host ESXi o un'istanza di NSX Manager. Abilitando e disabilitando un proxy, è possibile consentire e interrompere l'accesso tenant tramite tale proxy.

Creazione e gestione delle istanze di vCenter Server dedicate

Per creare e gestire le istanze e i proxy di vCenter Server dedicati, è possibile utilizzare il portale di amministrazione del provider di servizi o VMware Cloud Director OpenAPI. Per VMware Cloud Director OpenAPI, vedere *Guida introduttiva a VMware Cloud Director OpenAPI* all'indirizzo <https://code.vmware.com>.

Importante VMware Cloud Director richiede una connessione di rete diretta a ciascuna istanza di vCenter Server dedicata. Se l'istanza di vCenter Server utilizza un'istanza di Platform Services Controller esterna, VMware Cloud Director richiede una connessione di rete diretta anche a Platform Services Controller.

Per utilizzare VMware OVF Tool in un'istanza di vCenter Server dedicata con proxy, VMware Cloud Director richiede una connessione diretta a ciascun host ESXi.

1 Creare un'istanza di vCenter Server dedicata.

Quando si aggiunge un'istanza di vCenter Server all'ambiente VMware Cloud Director, è possibile creare un'istanza di vCenter Server dedicata abilitando l'accesso tenant nella procedura guidata **Aggiungi vCenter Server**. Quando si collega l'istanza di vCenter Server, è inoltre possibile creare un proxy per tale istanza. Vedere [Aggiunta dell'istanza di vCenter Server](#). È possibile abilitare l'accesso tenant alle istanze di vCenter Server già aggiunte a VMware Cloud Director che non hanno un utilizzo specifico. Vedere [Abilitazione dell'accesso tenant di un'istanza di vCenter Server collegata](#). L'abilitazione dell'accesso tenant rende l'istanza di vCenter Server disponibile per la pubblicazione nei tenant.

2 Aggiungere un proxy.

È possibile creare un proxy quando si collega un'istanza di vCenter Server a VMware Cloud Director o in un secondo momento. Se l'istanza di vCenter Server utilizza un'istanza di Platform Services Controller esterna, VMware Cloud Director crea anche un proxy per l'istanza di Platform Services Controller. Con i proxy principali e secondari, è possibile nascondere determinati proxy ai tenant oppure abilitare e disabilitare gruppi di proxy secondari tramite i loro proxy principali. Per ulteriori informazioni sulla creazione di un proxy dopo l'aggiunta di un'istanza di vCenter Server in VMware Cloud Director, vedere [Aggiunta di un proxy per l'accesso alle risorse vCenter Server sottostanti](#).

È possibile modificare, abilitare, disabilitare ed eliminare i proxy dalla scheda **Proxy** in **Risorse vSphere**.

Nota Quando si aggiunge un proxy a un'istanza di vCenter Server dedicata, è necessario caricare il certificato e l'identificazione personale, in modo che i tenant possano recuperarli se il componente con proxy utilizza certificati autofirmati.

Per visualizzare e gestire i certificati e gli elenchi di revocche dei certificati (CRL), vedere [Gestione dei certificati e dei CRL del proxy](#).

- 3 Recuperare il certificato e l'identificazione personale dei proxy creati e verificare che il certificato e l'identificazione personale siano presenti e corretti. Vedere [Gestione dei certificati e dei CRL del proxy](#).
- 4 Pubblicare l'istanza di vCenter Server dedicata in una o più organizzazioni.
È possibile pubblicare un'istanza di vCenter Server dedicata in un tenant e renderla visibile nel VMware Cloud Director Tenant Portal. Nella maggior parte dei casi, un'istanza di vCenter Server deve essere pubblicata solo in un tenant. Vedere [Pubblicazione di un'istanza di vCenter Server dedicata](#).
- 5 Per consentire ai tenant di accedere alle istanze e ai proxy di vCenter Server dedicati da VMware Cloud Director Tenant Portal, è necessario pubblicare il plug-in dell'**estensione CPOM** nelle loro organizzazioni. Vedere [Pubblica o Annulla la pubblicazione di un plug-in da un'organizzazione](#).

Questo capitolo include i seguenti argomenti:

- [Abilitazione dell'accesso tenant di un'istanza di vCenter Server collegata](#)
- [Pubblicazione di un'istanza di vCenter Server dedicata](#)

Abilitazione dell'accesso tenant di un'istanza di vCenter Server collegata

È possibile abilitare l'accesso tenant alle istanze di vCenter Server già aggiunte a VMware Cloud Director che non hanno un utilizzo specifico. L'abilitazione dell'accesso tenant crea un'istanza di vCenter Server dedicata e la rende disponibile per la pubblicazione nei tenant.

Con un'istanza di vCenter Server collegata, è possibile creare un'istanza di vCenter Server condivisa o un'istanza di vCenter Server dedicata. Se è stata creata un'istanza di vCenter Server condivisa e si desidera utilizzarla come un'istanza di vCenter Server dedicata, è innanzitutto necessario eliminare tutti i virtual data center (VDC) del provider che utilizzano le risorse dell'istanza di vCenter Server. Se si eliminano tutti i VDC del provider collegati all'istanza di vCenter Server condivisa, il relativo stato diventa Nessuno.

Prerequisiti

Verificare che nell'ambiente sia presente almeno un'istanza di vCenter Server collegata che non sia dedicata o condivisa.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.
- 3 Selezionare un'istanza di vCenter Server senza uno scopo specifico nella colonna **Utilizzo**.
- 4 Fare clic su **Abilita accesso tenant**.

Operazioni successive

[Pubblicazione di un'istanza di vCenter Server dedicata.](#)

Pubblicazione di un'istanza di vCenter Server dedicata

È possibile pubblicare un'istanza di vCenter Server dedicata in un tenant e renderla visibile tramite il VMware Cloud Director Tenant Portal. Per impostazione predefinita, un'istanza di vCenter Server deve essere pubblicata solo in un tenant.

Per impostazione predefinita, un SDDC è un'istanza di vCenter Server che viene dedicata a un singolo tenant pubblicando l'istanza di vCenter Server dedicata corrispondente solo nella relativa organizzazione. Il tenant non condivide le risorse dell'istanza di vCenter Server dedicata con altri tenant. La pubblicazione di un'istanza di vCenter Server dedicata in più tenant viola i limiti di tenancy. Tuttavia, a volte un tenant deve poter accedere a più istanze di vCenter Server dedicate. In questi casi, è possibile pubblicare un'istanza di vCenter Server dedicata in più tenant.

Prerequisiti

- Verificare di disporre di almeno un'istanza di vCenter Server con accesso tenant abilitato nell'ambiente VMware Cloud Director. Vedere [Capitolo 9 Gestione di istanze di vCenter Server dedicate](#).

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse vSphere**.
- 2 Nel pannello sinistro, selezionare **Istanze di vCenter Server**.

- 3 Selezionare un'istanza di vCenter Server con accesso tenant abilitato.

Nelle istanze di vCenter Server con accesso tenant abilitato è presente un valore dedicato nella colonna **Utilizzo**.

- 4 Fare clic su **Gestisci tenant**.

- 5 Selezionare il tenant o i tenant in cui si desidera pubblicare l'istanza di vCenter Server.

Se si deselecta un tenant nell'elenco, viene annullata la pubblicazione dell'istanza di vCenter Server.

- 6 Fare clic su **Salva**.

Operazioni successive

Per consentire agli utenti di accedere alle istanze e ai proxy di vCenter Server dedicati da VMware Cloud Director Tenant Portal, è necessario pubblicare il plug-in dell'**estensione CPOM** nelle loro organizzazioni. Vedere [Pubblica o Annulla la pubblicazione di un plug-in da un'organizzazione](#).

Gestione degli amministratori di sistema e dei ruoli

10

Utilizzando portale di amministrazione del provider di servizi di VMware Cloud Director, è possibile aggiungere amministratori di sistema 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.

Nota A partire da VMware Cloud Director 9.5, i provider di servizi possono creare ruoli del provider e gestire utenti e gruppi del provider utilizzando il portale di amministrazione del provider di servizi di VMware Cloud Director o vCloud OpenAPI. Per informazioni sulla gestione di gruppi, utenti e ruoli del provider, vedere *Guida del portale di amministrazione del provider di servizi di VMware Cloud Director*. Per esaminare la documentazione di vCloud OpenAPI, consultare la pagina https://vCloud_Director_IP_address_or_host_name/docs.

Questo capitolo include i seguenti argomenti:

- [Gestione di diritti e ruoli](#)
- [Gestione di utenti e gruppi di Provider](#)

Gestione di diritti e ruoli

Un diritto è l'unità fondamentale per il controllo degli accessi in VMware Cloud Director. Un ruolo associa un nome di ruolo a un set di diritti. Ogni organizzazione può avere ruoli e diritti diversi.

VMware Cloud Director utilizza i ruoli e i rispettivi diritti associati per determinare se un utente o un gruppo è autorizzato a eseguire un'operazione. Molte delle procedure documentate nelle guide di VMware Cloud Director hanno come prerequisito un ruolo. Questi prerequisiti si basano sull'assunto che il ruolo denominato corrisponda al ruolo predefinito non modificato o a un ruolo che include un set di diritti equivalente.

Gli amministratori di sistema possono utilizzare bundle diritti e ruoli tenant globali per gestire i diritti e i ruoli disponibili per ogni organizzazione.

Dopo aver installato VMware Cloud Director, il sistema contiene solo il bundle diritti Sistema, che include tutti i diritti disponibili nel sistema. Il bundle diritti Sistema non viene pubblicato in alcuna organizzazione. Il sistema contiene anche i ruoli tenant globali predefiniti pubblicati in tutte le organizzazioni. Per informazioni sui ruoli predefiniti, vedere [Ruoli predefiniti e relativi diritti](#).

Dopo aver aggiornato VMware Cloud Director dalla versione 9.1 o precedente, oltre al bundle diritti Sistema, il sistema contiene un bundle diritti Legacy per ogni organizzazione esistente. Ogni bundle diritti legacy include i diritti che sono disponibili nell'organizzazione associata al momento dell'aggiornamento e viene pubblicato solo in questa organizzazione.

Nota Per iniziare a utilizzare il modello di bundle diritti per un'organizzazione esistente, è necessario eliminare il bundle diritti legacy corrispondente.

Se è stato effettuato l'aggiornamento di VMware Cloud Director dalla versione 9.1 o precedenti, i modelli di ruolo esistenti vengono pubblicati in tutte le organizzazioni come ruoli tenant globali, mentre i ruoli esistenti che non sono collegati ad alcun modello di ruolo sono disponibili come ruoli specifici del tenant per le rispettive organizzazioni.

Terminologia dei diritti

Diritto

Ogni diritto fornisce l'accesso in visualizzazione o gestione a un determinato tipo di oggetto in VMware Cloud Director. I diritti appartengono a categorie diverse in base agli oggetti a cui si riferiscono, ad esempio vApp, Catalogo, Organizzazione e così via. L'organizzazione Provider contiene tutti i diritti disponibili nel sistema. L'amministratore di sistema definisce quali sono i diritti disponibili per ogni organizzazione. È possibile creare o modificare i diritti inclusi in VMware Cloud Director.

Bundle diritti

Gli amministratori di sistema possono utilizzare i bundle diritti per gestire i diritti disponibili per ogni organizzazione. Un bundle diritti è un insieme di diritti che l'amministratore di sistema può pubblicare in una o più organizzazioni. L'amministratore di sistema può creare e pubblicare bundle diritti corrispondenti a livelli di servizio, funzionalità monetizzabili separatamente o qualsiasi altro raggruppamento di diritti arbitrario. Solo gli amministratori di sistema possono visualizzare e gestire i bundle diritti. È possibile pubblicare più bundle nella stessa organizzazione.

Diritti organizzazione

Si tratta dell'insieme completo dei diritti disponibili per un'organizzazione. I diritti dell'organizzazione possono includere più bundle diritti, ma per gli amministratori e gli utenti dell'organizzazione viene visualizzato solo l'insieme dei diritti che possono utilizzare per creare e modificare ruoli specifici del tenant.

Terminologia dei ruoli

Ruolo

Un ruolo è un insieme di diritti che può essere assegnato a uno o più utenti e gruppi. Quando si crea o importa un utente o un gruppo, è necessario assegnare a esso un ruolo.

Ruoli di Provider

I ruoli di Provider sono l'insieme di ruoli disponibili solo per l'organizzazione Provider. Tali ruoli possono essere assegnati solo agli utenti di Provider. Gli amministratori di sistema possono creare ruoli di Provider personalizzati.

Ruoli tenant

I ruoli tenant sono l'insieme dei ruoli disponibili per un'organizzazione.

Gli amministratori di sistema possono creare e modificare ruoli tenant globali e pubblicarli in una o più organizzazioni. I ruoli tenant globali possono essere assegnati a utenti tenant nelle organizzazioni in cui sono pubblicati. Gli amministratori delle organizzazioni non possono modificare i ruoli tenant globali.

Nota Gli utenti tenant possono utilizzare solo i diritti dei loro ruoli che sono stati pubblicati nelle organizzazioni.

Ruoli specifici del tenant

Gli amministratori delle organizzazioni possono creare e modificare ruoli specifici del tenant, che sono locali per le loro organizzazioni. I ruoli specifici del tenant possono essere assegnati solo a utenti tenant nell'organizzazione a cui appartengono. I ruoli specifici del tenant possono contenere un sottoinsieme dei soli diritti dell'organizzazione.

Per informazioni sulla gestione dei ruoli specifici del tenant, vedere *VMware Cloud Director Tenant Portal Guide*.

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 [Diritti dell'amministratore di sistema](#). 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

Un **Amministratore di sistema** può utilizzare il Service Provider Admin Portal per visualizzare l'elenco di diritti inclusi in un ruolo.

- 1 Nella barra di navigazione superiore, fare clic su **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, fare clic su **Ruoli**.
- 3 Fare clic sul nome del ruolo che si desidera visualizzare.

Un **Amministratore organizzazione** può utilizzare Service Provider Admin Portal o Cloud Director OpenAPI per visualizzare i diritti in un ruolo o creare ruoli locali dell'organizzazione.

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 dell'amministratore di sistema

Il ruolo **Amministratore di sistema** esiste solo nell'organizzazione del provider. Per impostazione predefinita, il ruolo **Amministratore di sistema** dispone di tutti i diritti di VMware Cloud Director.

Il ruolo **Amministratore di sistema** dispone di tutti i diritti di VMware Cloud Director. Il seguente elenco include i diritti disponibili solo per gli **amministratori di sistema**. Il ruolo **Amministratore di sistema** dispone anche dei [Diritti nei ruoli tenant globali predefiniti](#).

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema

Novità di questa versione	Nome diritto
	Elenco di controllo di accesso: gestione
	Elenco di controllo di accesso: visualizzazione
	Servizi aggiuntivi: esecuzione flussi di lavoro
	Servizi aggiuntivi: visualizzazione flussi di lavoro in esecuzione
	Servizi aggiuntivi: visualizzazione flussi di lavoro
	Adotta pool di risorse: visualizzazione
	Entità amministratore alternativa: visualizzazione
	Impostazioni AMQP: gestione
	Impostazioni AMQP: visualizzazione
	API Explorer: visualizzazione
	Catalogo: importazione file multimediali da vSphere
	Catalogo: vista macchina virtuale shadow
	Catalogo: memorizzazione nella cache pubblicazione/sottoscrizione VCSP
	Configurazione cella: visualizzazione
	Server tunnel cloud: gestione
	Server tunnel cloud: visualizzazione
	Impostazioni di sistema libreria di contenuti: gestione
	Impostazioni di sistema libreria di contenuti: visualizzazione
	Entità personalizzata: creazione definizioni entità personalizzate
	Entità personalizzata: eliminazione definizioni entità personalizzate
	Entità personalizzata: modifica definizioni entità personalizzate
	Entità personalizzata: visualizzazione definizioni entità personalizzate
	Archivio dati: eliminazione
	Archivio dati: modifica
	Archivio dati: abilitazione o disabilitazione

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	Archivio dati: apertura in vSphere
	Archivio dati: visualizzazione
	Rete vDC dell'organizzazione diretta: gestione
	Commutatore virtuale distribuito: apertura in vSphere
	Cluster edge: gestione
	Cluster edge: visualizzazione
	Definizione API servizio estensione: gestione
	Definizione API servizio estensione: visualizzazione
	Servizi estensione: visualizzazione
	Estensioni: visualizzazione
	Servizio esterno: gestione
	Servizio esterno: visualizzazione
	Generale: visualizzazione dettagli errori
	Ruolo globale: modifica
	Ruolo globale: visualizzazione
	Host: abilitazione o disabilitazione
	Host: gestione
	Host: apertura in vSphere
	Host: preparazione o annullamento della preparazione
	Host: riparazione
	Host: aggiornamento
	Host: visualizzazione
	Impostazioni Kerberos: gestione
	Impostazioni Kerberos: visualizzazione
	Impostazioni LDAP: gestione
	Impostazioni LDAP: visualizzazione
	Report licenze: visualizzazione
	Risorse localizzazione: gestione

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	Operazioni sistema multisito
	Pool di reti: creazione o eliminazione
	Pool di reti: modifica
	Pool di reti: apertura in vSphere
	Pool di reti: riparazione
	Pool di reti: visualizzazione
	NSX-T: modifica
	NSX-T: visualizzazione
	Estensioni oggetto: gestione
	Estensioni oggetto: visualizzazione
	Rete organizzazione: creazione o eliminazione
	Rete organizzazione: apertura in vSphere
	Criterio di calcolo del vDC dell'organizzazione: vista amministratore
	Criterio di calcolo del vDC dell'organizzazione: gestione
	Firewall distribuito del vDC dell'organizzazione: abilitazione/disabilitazione
	Gateway vDC dell'organizzazione: configurazione routing BGP
	Gateway vDC dell'organizzazione: configurazione VPN L2
	Gateway vDC dell'organizzazione: configurazione routing OSPF
	Gateway vDC dell'organizzazione: configurazione accesso remoto
✓	Gateway vDC dell'organizzazione: configurazione comunicazione route
	Gateway vDC dell'organizzazione: configurazione VPN SSL
	Gateway vDC dell'organizzazione: configurazione registrazione di sistema
	Gateway vDC dell'organizzazione: creazione
	Gateway vDC dell'organizzazione: eliminazione
	Gateway vDC dell'organizzazione: routing distribuito
	Gateway vDC dell'organizzazione: importazione
	Gateway vDC dell'organizzazione: modifica fattore di forma
	Gateway vDC dell'organizzazione: aggiornamento

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	Gateway vDC dell'organizzazione: proprietà aggiornamento
	Gateway vDC dell'organizzazione: aggiornamento
	Gateway vDC dell'organizzazione: visualizzazione routing BGP
	Gateway vDC dell'organizzazione: visualizzazione VPN L2
	Gateway vDC dell'organizzazione: visualizzazione routing OSPF
	Gateway vDC dell'organizzazione: visualizzazione accesso remoto
✓	Gateway vDC dell'organizzazione: visualizzazione comunicazione route
	Gateway vDC dell'organizzazione: visualizzazione VPN SSL
	Rete vDC dell'organizzazione: importazione
	Pool di risorse vDC dell'organizzazione: apertura in vSphere
	Pool di risorse vDC dell'organizzazione: visualizzazione
	Criterio di storage vDC dell'organizzazione: modifica
	Criterio di storage vDC dell'organizzazione: abilitazione o disabilitazione
	Criterio di storage vDC dell'organizzazione: apertura in vSphere
	Criterio di storage vDC dell'organizzazione: rimozione
	vDC dell'organizzazione: creazione
	vDC dell'organizzazione: eliminazione
	vDC dell'organizzazione: abilitazione o disabilitazione
	vDC dell'organizzazione: modifica estesa
	vDC organizzazione: visualizzazione estesa
	Organizzazione: attivazione o disattivazione
	Organizzazione: creazione o eliminazione
	Organizzazione: modifica dei limiti
	Organizzazione: modifica del nome
	Organizzazione: migrazione storage tenant
	Organizzazione: esecuzione di query dell'amministratore
	Organizzazione: utilizzo LDAP del provider come tenant
	Gruppo di porte: apertura in vSphere

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	Preferenza: gestione definizione preferenze
	Rete del provider: creazione o eliminazione
	Rete del provider: modifica
	Rete del provider: apertura in vSphere
	Rete del provider: visualizzazione
	Criterio di calcolo vDC del provider: gestione
	Criterio di calcolo vDC del provider: visualizzazione
	Pool di risorse vDC del provider: migrazione delle macchine virtuali
	Pool di risorse vDC del provider: apertura in vSphere
	Pool di risorse vDC del provider: visualizzazione
	Criterio di storage vDC del provider: modifica
	Criterio di storage vDC del provider: abilitazione o disabilitazione
	Criterio di storage vDC del provider: apertura in vSphere
	Criterio di storage vDC del provider: rimozione
	Criterio di storage vDC del provider: visualizzazione
	VDC del provider: aggiunta pool di risorse
	VDC del provider: creazione o eliminazione
	VDC del provider: eliminazione pool di risorse
	VDC del provider: modifica
	VDC del provider: abilitazione o disabilitazione
	VDC del provider: abilitazione o disabilitazione pool di risorse
	VDC del provider: abilitazione rete VXLAN di vSphere
	VDC del provider: unione
	VDC del provider: visualizzazione
✓	Criterio di quota: gestione
✓	Criterio di quota: visualizzazione
	Ricarica macchina virtuale: gestione
	Azione classe risorsa: gestione

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	Azione classe risorsa: visualizzazione
	Pool di risorse: apertura
	Pool di risorse: apertura in vSphere
	Pool di risorse: visualizzazione
	Diritto: gestione
	Diritto: visualizzazione
	Bundle diritti: modifica
	Bundle diritti: visualizzazione
	SDDC: gestione
	SDDC: gestione del proxy
	SDDC: visualizzazione
	Estensioni selettore: gestione
	Estensioni selettore: visualizzazione
✓	Certificati server: gestione
✓	Certificati server: visualizzazione
	App del servizio: gestione
	App del servizio: visualizzazione
	Autorizzazione del servizio: gestione
	Configurazione del servizio: gestione
	Configurazione del servizio: visualizzazione
	Libreria dei servizi: creazione librerie dei servizi
	Libreria dei servizi: eliminazione servizi dalla libreria dei servizi
	Libreria dei servizi: modifica dei metadati servizi
	Libreria dei servizi: modifica contenuto di un servizio
	Collegamento servizio: gestione
	Collegamento servizio: visualizzazione
	Tipo di risorsa servizio: gestione
	Tipo di risorsa servizio: visualizzazione

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	Risorsa servizio: gestione
	Risorsa servizio: visualizzazione
	Rete vDC dell'organizzazione condivisa: gestione
	Sito: modifica
	Sito: visualizzazione
✓	Impostazioni SSL: visualizzazione
	Elemento bloccato: gestione
	Elemento bloccato: visualizzazione
	Operazioni sistema: esecuzione delle operazioni di sistema
	Organizzazione sistema: gestione
	Organizzazione sistema: visualizzazione
	Impostazioni sistema: gestione
	Impostazioni sistema: visualizzazione
	Attività: ripresa, interruzione o errore
	Attività: aggiornamento
	Attività: visualizzazione attività
	Token: gestione
	Token: gestione di tutto
✓	Archivio attendibilità: gestione
✓	Archivio attendibilità: visualizzazione
	Plug-in interfaccia utente: definizione, caricamento, modifica, eliminazione, associazione o annullamento dell'associazione
	Branding portale interfaccia utente: gestione
	Modello di vApp: forzatura scadenza lease dello storage
	Modello di vApp: importazione
	Modello di vApp: apertura in vSphere
	vApp: autorizzazione di tutte le configurazioni aggiuntive
	vApp: autorizzazione configurazione aggiuntiva unione Ethernet

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	vApp: autorizzazione configurazione aggiuntiva latenza
	vApp: autorizzazione configurazione aggiuntiva corrispondente
	vApp: autorizzazione configurazione aggiuntiva affinità nodi NUMA
	vApp: modifica impostazioni prenotazione CPU e memoria macchine virtuali in tutti i tipi di VDC
	vApp: attivazione/disattivazione modalità di manutenzione
	vApp: forzatura scadenza lease di runtime
	vApp: forzatura scadenza lease di storage
	vApp: opzioni importazione
	vApp: gestione manutenzione
	vApp: apertura in vSphere
	vApp: visualizzazione macchine virtuali shadow
	vApp: verifica conformità macchine virtuali
	vApp: migrazione, forzatura annullamento distribuzione, trasferimento e consolidamento macchine virtuali
	Estensione VCD: registrazione, annullamento registrazione, aggiornamento, associazione o annullamento associazione
	Estensione VCD: visualizzazione
	vCenter: collegamento o scollegamento
	vCenter: abilitazione o disabilitazione
	vCenter: apertura in vSphere
	vCenter: aggiornamento
	vCenter: visualizzazione
	Gruppo di vDC: configurazione
	Gruppo di vDC: visualizzazione
	Modello VDC: gestione ACL
	Modello VDC: visualizzazione estesa
	Modello VDC: gestione
	VMC: registrazione SDDC
	vRealize Orchestrator: pubblicazione e annullamento pubblicazione flussi di lavoro nei tenant

Tabella 10-1. Diritti disponibili solo per gli amministratori di sistema (continua)

Novità di questa versione	Nome diritto
	vRealize Orchestrator: registrazione e annullamento registrazione server vRealize Orchestrator
	vRealize Orchestrator: visualizzazione server vRealize Orchestrator registrati
	Server vSphere: gestione
	Server vSphere: gestione proxy
✓	Server vSphere: gestione configurazione proxy
	Server vSphere: visualizzazione

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: aggiunta della vApp da Cloud personale	✓	✓	✓		
	Catalogo: cambio del proprietario	✓				
	Catalogo: pubblicazione e sottoscrizione di CLSP	✓	✓			
	Catalogo: creazione/eliminazione catalogo	✓	✓			
	Catalogo: modifica proprietà	✓	✓			
	Catalogo: pubblicazione	✓	✓			
	Catalogo: condivisione	✓	✓			
	Catalogo: visualizzazione ACL	✓	✓			
	Catalogo: visualizzazione cataloghi privati e condivisi	✓	✓	✓		
	Catalogo: visualizzazione cataloghi pubblicati	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Entità personalizzata: visualizzazione di tutte le istanze di entità personalizzata nell'organizzazione	✓				
	Entità personalizzata: visualizzazione istanza di entità personalizzata	✓				
	Disco: cambio del proprietario	✓	✓			
	Disco: creazione	✓	✓	✓		
	Disco: eliminazione	✓	✓	✓		
	Disco: modifica proprietà	✓	✓	✓		
✓	Disco: visualizzazione stato crittografia	✓		✓		
	Disco: visualizzazione proprietà	✓	✓	✓	✓	
	Generale: controllo amministratore	✓				
	Generale: vista amministratore	✓				
	Generale: invio notifica	✓				
	Gruppo/Utente: visualizzazione	✓				
	Operazioni cloud ibrido: acquisizione ticket di controllo	✓				
	Operazioni cloud ibrido: acquisizione ticket del tunnel dal cloud	✓				
	Operazioni cloud ibrido: acquisizione ticket del tunnel verso il cloud	✓				
	Operazioni cloud ibrido: creazione tunnel dal cloud	✓				
	Operazioni cloud ibrido: creazione tunnel verso il cloud	✓				
	Operazioni cloud ibrido: eliminazione tunnel dal cloud	✓				
	Operazioni cloud ibrido: eliminazione tunnel verso il cloud	✓				
	Operazioni cloud ibrido: aggiornamento tag endpoint del tunnel dal cloud	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Operazioni cloud ibrido: visualizzazione tunnel dal cloud	✓				
	Operazioni cloud ibrido: visualizzazione tunnel verso il cloud	✓				
	Rete organizzazione: modifica proprietà	✓				
	Rete organizzazione: visualizzazione	✓				
	Criterio di calcolo vDC dell'organizzazione: visualizzazione	✓	✓	✓	✓	
	Firewall distribuito vDC dell'organizzazione: configurazione regole	✓				
	Firewall distribuito vDC dell'organizzazione: visualizzazione regole	✓				
	Gateway vDC dell'organizzazione: configurazione DHCP	✓				
	Gateway vDC dell'organizzazione: configurazione DNS	✓				
	Gateway vDC dell'organizzazione: configurazione routing ECMP	✓				
	Gateway vDC dell'organizzazione: configurazione firewall	✓				
	Gateway vDC dell'organizzazione: configurazione VPN IPsec	✓				
	Gateway vDC dell'organizzazione: configurazione bilanciamento del carico	✓				
	Gateway vDC dell'organizzazione: configurazione NAT	✓				
	Gateway vDC dell'organizzazione: configurazione routing statico	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Gateway vDC dell'organizzazione: configurazione syslog	✓				
	Gateway vDC dell'organizzazione: conversione in Advanced Networking	✓				
	Gateway vDC dell'organizzazione: visualizzazione	✓				
	Gateway vDC dell'organizzazione: visualizzazione DHCP	✓				
	Gateway vDC dell'organizzazione: visualizzazione DNS	✓				
	Gateway vDC dell'organizzazione: visualizzazione firewall	✓				
	Gateway vDC dell'organizzazione: visualizzazione VPN IPsec	✓				
	Gateway vDC dell'organizzazione: visualizzazione bilanciamento del carico	✓				
	Gateway vDC dell'organizzazione: visualizzazione NAT	✓				
	Gateway vDC dell'organizzazione: visualizzazione routing statico	✓				
	Rete vDC dell'organizzazione: modifica proprietà	✓				
	Rete vDC dell'organizzazione: visualizzazione proprietà	✓		✓		
✓	Criterio di storage vDC dell'organizzazione: visualizzazione funzionalità	✓				
	Profilo di storage vDC dell'organizzazione: impostazione valore predefinito	✓				
	vDC dell'organizzazione: modifica	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	vDC dell'organizzazione: modifica ACL	✓				
	vDC dell'organizzazione: gestione firewall	✓				
	vDC dell'organizzazione: visualizzazione	✓	✓			
	vDC dell'organizzazione: visualizzazione ACL	✓				
	vDC dell'organizzazione: visualizzazione metriche	✓				
	vDC dell'organizzazione: modifica affinità macchina virtuale-macchina virtuale	✓	✓	✓		
	Organizzazione: modifica impostazioni associazione	✓				
	Organizzazione: modifica impostazioni federazione	✓				
	Organizzazione: modifica impostazioni LDAP	✓				
	Organizzazione: modifica criterio lease	✓				
	Organizzazione: modifica impostazioni OAuth	✓				
	Organizzazione: modifica criterio password	✓				
	Organizzazione: modifica proprietà	✓				
	Organizzazione: modifica criterio quote	✓				
	Organizzazione: modifica impostazioni SMTP	✓				
	Organizzazione: importazione utente/gruppo da IdP durante la modifica dell'ACL del VDC	✓				
	Organizzazione: visualizzazione	✓	✓	✓		
	Organizzazione: visualizzazione metriche	✓				
	Ruolo: creazione, modifica, eliminazione o copia	✓				

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	Libreria dei servizi: visualizzazione librerie dei servizi	✓				
	Plug-in interfaccia utente: visualizzazione	✓	✓	✓	✓	
	Modello di vApp/multimedia: copia	✓	✓	✓		
	Modello di vApp/multimedia: creazione/caricamento	✓	✓			
	Modello di vApp/multimedia: modifica	✓	✓	✓		
	Modello di vApp/multimedia: visualizzazione	✓	✓	✓	✓	
	Modello di vApp: cambio del proprietario	✓	✓			
	Modello di vApp: checkout	✓	✓	✓	✓	
	Modello di vApp: download	✓	✓			
	vApp: cambio proprietario	✓				
	vApp: copia	✓	✓	✓	✓	
	vApp: creazione/riconfigurazione	✓	✓	✓		
	vApp: eliminazione	✓	✓	✓	✓	
	vApp: download	✓	✓	✓		
	vApp: modifica proprietà	✓	✓	✓	✓	
	vApp: modifica criterio di calcolo macchina virtuale	✓	✓	✓		
	vApp: modifica CPU macchina virtuale	✓	✓	✓		
	vApp: modifica disco rigido macchina virtuale	✓	✓	✓		
	vApp: modifica memoria macchina virtuale	✓	✓	✓		
	vApp: modifica rete macchina virtuale	✓	✓	✓	✓	
	vApp: modifica proprietà macchina virtuale	✓	✓	✓	✓	
	vApp: gestione impostazioni password macchina virtuale	✓	✓	✓	✓	✓

Novità di questa versione	Nome diritto	Amministratore organizzazione	Autore catalogo	Autore vApp	Utente vApp	Solo accesso console
	vApp: operazioni attivazione	✓	✓	✓	✓	
	vApp: condivisione	✓	✓	✓	✓	
	vApp: operazioni di creazione snapshot	✓	✓	✓	✓	
	vApp: caricamento	✓	✓	✓		
	vApp: utilizzo console	✓	✓	✓	✓	✓
	vApp: visualizzazione ACL	✓	✓	✓	✓	
✓	vApp: visualizzazione macchina virtuale e stato crittografia dischi macchina virtuale	✓		✓		
	vApp: visualizzazione metriche macchina virtuale	✓		✓	✓	
	vApp: opzioni di avvio macchina virtuale	✓	✓	✓		
	vApp: metadati macchina virtuale in vCenter	✓	✓	✓		
	Modello VDC: creazione di istanze	✓				
	Modello VDC: visualizzazione	✓				

Gestione dei bundle diritti

Un amministratore di sistema può creare bundle diritti e pubblicarli in una o più organizzazioni nel cloud. È possibile modificare ed eliminare i bundle diritti esistenti. È possibile annullare la pubblicazione di bundle diritti dalle organizzazioni nel cloud.

Creazione di un bundle diritti

È possibile raggruppare un set di diritti come bundle e pubblicarlo in una o più organizzazioni nel sistema.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Bundle diritti**.
- 3 Fare clic su **Aggiungi**.
- 4 Immettere un nome e, facoltativamente, una descrizione per il nuovo bundle diritti.

5 Selezionare i diritti che si desidera associare a questo bundle.

I diritti sono raggruppati in categorie e sottocategorie in base all'accesso in visualizzazione o in gestione all'oggetto a cui si riferiscono.

È possibile selezionare i diritti singolarmente, in base all'accesso in visualizzazione o in gestione per sottocategoria o globalmente.

Categoria	Descrizione
Controllo accessi	Include i diritti per la visualizzazione e la gestione di organizzazioni, diritti, ruoli e utenti.
Amministrazione	Include i diritti per la visualizzazione e la gestione delle impostazioni generali e multisito.
Calcola	Include i diritti per la visualizzazione e la gestione di VDC di provider e organizzazione, vApp, modelli di VDC di organizzazione e monitoraggio delle macchine virtuali.
Estensioni	Include i diritti per la visualizzazione e la gestione di estensioni e plug-in di VMware Cloud Director.
Infrastruttura	Include i diritti per la visualizzazione e la gestione delle risorse di vSphere.
Librerie	Include i diritti per la visualizzazione e la gestione dei cataloghi e degli elementi di catalogo.
Rete	Include i diritti per la visualizzazione e la gestione delle risorse di rete.

6 Fare clic su **Salva**.

Operazioni successive

Il bundle diritti appena creato può essere pubblicato in una o più organizzazioni nel sistema. Vedere [Pubblicazione o annullamento della pubblicazione di un bundle diritti](#).

Clonazione di un bundle di diritti

È possibile utilizzare un bundle di diritti esistente come modello per la creazione di un nuovo bundle.

Prerequisiti

Verificare di disporre dei diritti necessari per aggiungere nuovi ruoli in VMware Cloud Director.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Bundle diritti**.
- 3 Selezionare il bundle di diritti che si desidera clonare e fare clic su **Clona**.
- 4 Nella finestra **Bundle diritti clone**, immettere un nome e una descrizione per il bundle clonato.

- 5 (Facoltativo) Per modificare i diritti clonati, attivare l'opzione **Modifica diritti selezionati** e selezionare o deselezionare i diritti che si desidera modificare per il ruolo clonato.
- 6 Fare clic su **Salva**.

Pubblicazione o annullamento della pubblicazione di un bundle diritti

È possibile pubblicare un bundle diritti in una o più organizzazioni nel sistema. Dopo aver pubblicato un bundle diritti in un'organizzazione, i diritti inclusi nel bundle diventano parte dell'insieme di diritti dell'organizzazione.

I diritti dell'organizzazione possono includere più bundle diritti, ma per gli amministratori e gli utenti dell'organizzazione viene visualizzato solo l'insieme dei diritti che possono utilizzare per creare e modificare ruoli.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Bundle diritti**.
- 3 Selezionare il pulsante di opzione accanto al bundle di destinazione e fare clic su **Pubblica**.
- 4 Per pubblicare il bundle:
 - a Selezionare **Pubblica nei tenant**.
 - b Selezionare le organizzazioni in cui si desidera pubblicare il ruolo.
 - Se si desidera pubblicare il bundle in tutte le organizzazioni esistenti e create di recente nel sistema, selezionare **Pubblica in tutti i tenant**.
 - Se si desidera pubblicare il bundle in determinate organizzazioni nel sistema, selezionare le organizzazioni singolarmente.
- 5 Per annullare la pubblicazione del bundle:
 - Se si desidera annullare la pubblicazione del bundle in tutte le organizzazioni nel sistema, deselezionare **Pubblica nei tenant**.
 - Se si desidera annullare la pubblicazione del bundle in determinate organizzazioni nel sistema, deselezionare **Pubblica nei tenant** e deselezionare le organizzazioni singolarmente.
- 6 Fare clic su **Salva**.

Risultati

I diritti inclusi nel bundle pubblicato sono disponibili nelle organizzazioni selezionate e possono essere utilizzati nei ruoli di tali organizzazioni.

I diritti inclusi nel ruolo di cui è stata annullata la pubblicazione vengono rimossi dalle organizzazioni selezionate e non possono essere utilizzati nei ruoli di tali organizzazioni.

Visualizzazione e modifica di un bundle diritti

È possibile visualizzare i diritti inclusi in un bundle diritti. È possibile modificare il nome, la descrizione e i diritti di un bundle.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Bundle diritti**.
- 3 Fare clic sul nome del bundle di destinazione.

È possibile visualizzare i diritti associati al bundle estendendo le categorie dei diritti.

- 4 Modificare il bundle e fare clic su **Mantieni**.

Risultati

Se si modificano i diritti del bundle, il nuovo set di diritti viene applicato a tutte le organizzazioni in cui questo bundle diritti è pubblicato.

Eliminazione di un bundle di diritti

È possibile rimuovere un bundle di diritti che non si utilizza più nelle organizzazioni.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Bundle diritti**.
- 3 Selezionare il pulsante di opzione accanto al bundle di destinazione e fare clic su **Elimina**.
- 4 Per confermare, fare clic su **OK**.

Gestione dei ruoli tenant globali

Un amministratore di sistema può creare ruoli tenant globali e pubblicarli in una o più organizzazioni nel cloud. È possibile modificare ed eliminare i ruoli tenant globali esistenti. È possibile annullare la pubblicazione di ruoli tenant globali da singole organizzazioni nel cloud.

Dopo l'installazione e la configurazione di VMware Cloud Director iniziali, il sistema contiene un insieme di tenant globali predefiniti pubblicati in tutte le organizzazioni. Vedere [Ruoli predefiniti e relativi diritti](#).

Creazione di un ruolo tenant globale

È possibile creare un ruolo tenant globale da pubblicare in una o più organizzazioni nel sistema.

Dopo l'installazione e la configurazione iniziali di VMware Cloud Director, il sistema contiene i ruoli tenant globali predefiniti che vengono pubblicati in tutte le organizzazioni. Per informazioni sui ruoli predefiniti, vedere [Ruoli predefiniti e relativi diritti](#).

È possibile aggiungere ruoli globali personalizzati al sistema.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Ruoli globali**.
- 3 Fare clic su **Aggiungi**.
- 4 Immettere un nome e, facoltativamente, una descrizione per il nuovo ruolo.
- 5 Selezionare i diritti che si desidera associare al ruolo.

I diritti sono raggruppati in categorie e sottocategorie in base all'accesso in visualizzazione o in gestione all'oggetto a cui si riferiscono.

È possibile selezionare i diritti singolarmente, in base all'accesso in visualizzazione o in gestione per sottocategoria o globalmente.

Categoria	Descrizione
Controllo accessi	Include i diritti per la visualizzazione e la gestione di organizzazioni, diritti, ruoli e utenti.
Amministrazione	Include i diritti per la visualizzazione e la gestione delle impostazioni generali e multisito.
Calcola	Include i diritti per la visualizzazione e la gestione di VDC di provider e organizzazione, vApp, modelli di VDC di organizzazione e monitoraggio delle macchine virtuali.
Estensioni	Include i diritti per la visualizzazione e la gestione di estensioni e plug-in di VMware Cloud Director.
Infrastruttura	Include i diritti per la visualizzazione e la gestione delle risorse di vSphere.
Librerie	Include i diritti per la visualizzazione e la gestione dei cataloghi e degli elementi di catalogo.
Rete	Include i diritti per la visualizzazione e la gestione delle risorse di rete.

- 6 Fare clic su **Mantieni**.

Risultati

Al momento della creazione, il nuovo diritto tenant globale è disponibile solo per l'organizzazione Provider di VMware Cloud Director.

Operazioni successive

È possibile pubblicare il ruolo appena creato in una o più organizzazioni nel sistema. Vedere [Pubblicazione o annullamento della pubblicazione di un ruolo tenant globale](#).

Clonazione di un ruolo tenant globale

È possibile utilizzare un ruolo tenant globale esistente come modello per la creazione di un nuovo ruolo.

Prerequisiti

Verificare di disporre dei diritti necessari per aggiungere nuovi ruoli in VMware Cloud Director.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Ruoli globali**.
- 3 Selezionare il ruolo che si desidera clonare e fare clic su **Clona**.
- 4 Nella finestra **Ruolo globale clone**, immettere un nome e una descrizione per il ruolo clonato.
- 5 (Facoltativo) Per modificare i diritti clonati, attivare l'opzione **Modifica diritti selezionati** e selezionare o deselezionare i diritti che si desidera modificare per il ruolo clonato.
- 6 Fare clic su **Salva**.

Pubblicazione o annullamento della pubblicazione di un ruolo tenant globale

È possibile pubblicare un ruolo tenant globale in una o più organizzazioni nel sistema. Dopo aver pubblicato un ruolo in un'organizzazione, questo ruolo diventa parte del set di ruoli tenant dell'organizzazione.

Prerequisiti

Se si desidera annullare la pubblicazione di un ruolo tenant globale da un'organizzazione, verificare che il ruolo non sia stato assegnato ad alcun utente dell'organizzazione.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Ruoli globali**.
- 3 Selezionare il pulsante di opzione accanto al ruolo di destinazione e fare clic su **Pubblica**.
- 4 Per pubblicare il ruolo:
 - a Selezionare **Pubblica nei tenant**.
 - b Selezionare le organizzazioni in cui si desidera pubblicare il ruolo.
 - Se si desidera pubblicare il ruolo in tutte le organizzazioni esistenti e create di recente nel sistema, selezionare **Pubblica in tutti i tenant**.
 - Se si desidera pubblicare il ruolo in determinate organizzazioni nel sistema, selezionare le organizzazioni singolarmente.
- 5 Per annullare la pubblicazione del ruolo:
 - Se si desidera annullare la pubblicazione del ruolo in tutte le organizzazioni nel sistema, deselezionare **Pubblica nei tenant**.

- Se si desidera annullare la pubblicazione del ruolo in determinate organizzazioni nel sistema, deselezionare **Pubblica nei tenant** e deselezionare le organizzazioni singolarmente.

6 Fare clic su **Salva**.

Risultati

Il ruolo pubblicato è disponibile nelle organizzazioni selezionate e può essere assegnato agli utenti in queste organizzazioni. Gli amministratori delle organizzazioni non possono modificare i ruoli tenant globali pubblicati nelle proprie organizzazioni.

Il ruolo di cui è stata annullata la pubblicazione viene rimosso dalle organizzazioni selezionate e non può essere assegnato agli utenti di queste organizzazioni.

Visualizzazione e modifica di un ruolo tenant globale

È possibile visualizzare i diritti inclusi in un ruolo tenant globale. È possibile modificare il nome, la descrizione e i diritti di un ruolo tenant globale.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Ruoli globali**.
- 3 Fare clic sul nome del ruolo di destinazione.

È possibile visualizzare i diritti associati al ruolo espandendo le categorie dei diritti.

- 4 Per modificare il nome, la descrizione o i diritti del ruolo, fare clic su **Modifica**.
- 5 Modificare il ruolo e fare clic su **Mantieni**.

Risultati

In caso di modifica dei diritti del ruolo, il nuovo insieme di diritti viene applicato agli utenti in tutte le organizzazioni in cui il ruolo è assegnato.

Eliminazione di un ruolo tenant globale

È possibile rimuovere un ruolo tenant globale che non si utilizza più nelle organizzazioni.

Prerequisiti

Il ruolo tenant globale che si desidera eliminare non deve essere assegnato a nessun utente delle organizzazioni.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi tenant**, selezionare **Ruoli globali**.
- 3 Selezionare il pulsante di opzione accanto al ruolo di destinazione e fare clic su **Elimina**.

4 Per confermare, fare clic su **OK**.

Gestione dei ruoli di Provider

È possibile creare e gestire i ruoli nell'organizzazione Provider di VMware Cloud Director.

Per informazioni sulla gestione dei ruoli tenant, vedere *VMware Cloud Director Tenant Portal Guide*.

Creazione di un ruolo di Provider

È possibile creare un ruolo all'interno dell'organizzazione Provider di VMware Cloud Director.

Dopo l'installazione e la configurazione iniziali di VMware Cloud Director, il sistema contiene i ruoli predefiniti che sono locali per l'organizzazione Provider e globali per tutte le organizzazioni. Per informazioni sui ruoli predefiniti, vedere [Ruoli predefiniti e relativi diritti](#).

È possibile aggiungere ruoli di Provider personalizzati all'organizzazione Provider.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Ruoli**.
- 3 Fare clic su **Nuovo**.
- 4 Immettere un nome e, facoltativamente, una descrizione per il nuovo ruolo.
- 5 Selezionare i diritti che si desidera associare al ruolo.

I diritti sono raggruppati in categorie e sottocategorie in base all'accesso in visualizzazione o in gestione all'oggetto a cui si riferiscono.

È possibile selezionare i diritti singolarmente, in base all'accesso in visualizzazione o in gestione per sottocategoria o globalmente.

Categoria	Descrizione
Controllo accessi	Include i diritti per la visualizzazione e la gestione di organizzazioni, diritti, ruoli e utenti.
Amministrazione	Include i diritti per la visualizzazione e la gestione delle impostazioni generali e multisito.
Calcola	Include i diritti per la visualizzazione e la gestione di VDC di provider e organizzazione, vApp, modelli di VDC di organizzazione e monitoraggio delle macchine virtuali.
Estensioni	Include i diritti per la visualizzazione e la gestione di estensioni e plug-in di VMware Cloud Director.
Infrastruttura	Include i diritti per la visualizzazione e la gestione delle risorse di vSphere.

Categoria	Descrizione
Librerie	Include i diritti per la visualizzazione e la gestione dei cataloghi e degli elementi di catalogo.
Rete	Include i diritti per la visualizzazione e la gestione delle risorse di rete.

6 Fare clic su **Salva**.

Risultati

Il ruolo appena creato è disponibile per l'assegnazione agli utenti dell'organizzazione Provider.

Clonazione di un ruolo del provider

È possibile utilizzare un ruolo del provider esistente come modello per la creazione di un nuovo ruolo.

Prerequisiti

Verificare di disporre dei diritti necessari per aggiungere nuovi ruoli in VMware Cloud Director.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Ruoli**.
- 3 Selezionare il ruolo che si desidera clonare e fare clic su **Clona**.
- 4 Nella finestra **Ruolo clone**, immettere un nome e una descrizione per il ruolo clonato.
- 5 (Facoltativo) Per modificare i diritti clonati, attivare l'opzione **Modifica diritti selezionati** e selezionare o deselezionare i diritti che si desidera modificare per il ruolo clonato.
- 6 Fare clic su **Salva**.

Visualizzazione o modifica di un ruolo di Provider

È possibile visualizzare i diritti inclusi in un ruolo locale per l'organizzazione Provider di VMware Cloud Director. È possibile modificare il nome, la descrizione e i diritti di un ruolo.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Ruoli**.
- 3 Fare clic sul nome del ruolo di destinazione.
È possibile visualizzare i diritti associati al ruolo espandendo le categorie dei diritti.
- 4 Per modificare il nome, la descrizione o i diritti del ruolo, fare clic su **Modifica**.
- 5 Modificare il ruolo e fare clic su **Salva**.

Risultati

In caso di modifica dei diritti del ruolo, il nuovo insieme di diritti viene applicato agli utenti a cui il ruolo è assegnato.

Importazione di un ruolo del provider

È possibile rimuovere un ruolo che non viene più utilizzato nell'organizzazione del provider di VMware Cloud Director.

Prerequisiti

Il ruolo che si desidera eliminare non deve essere assegnato a nessun utente.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Ruoli**.
- 3 Selezionare il pulsante di opzione accanto al ruolo di destinazione e fare clic su **Elimina**.
- 4 Per confermare, fare clic su **OK**.

Gestione di utenti e gruppi di Provider

È possibile aggiungere e importare utenti e gruppi nell'organizzazione Provider di VMware Cloud Director.

Per informazioni sulla gestione di utenti e gruppi dell'organizzazione, vedere *VMware Cloud Director Tenant Portal Guide*.

Gestione degli utenti di Provider

È possibile gestire gli utenti nell'organizzazione Provider utilizzando Service Provider Admin Portal.

Per informazioni sulla gestione degli utenti tenant nelle organizzazioni, vedere *VMware Cloud Director Tenant Portal Guide*.

Creazione di un utente del provider

È possibile creare un utente all'interno dell'organizzazione del provider di VMware Cloud Director.

Durante l'installazione e la configurazione di VMware Cloud Director, viene creato un account di **amministratore di sistema**. Dopo la configurazione iniziale, è possibile creare altri amministratori e utenti dell'organizzazione del provider.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Utenti**.

- 3 Fare clic su **Nuovo**.
- 4 Immettere un nome utente e una password per il nuovo utente.
La password deve contenere almeno sei caratteri.
- 5 Specificare se si desidera abilitare l'utente al momento della creazione.
- 6 Dal menu a discesa **Ruoli disponibili** selezionare un ruolo per l'utente.
L'elenco di ruoli disponibili comprende i ruoli globali e i ruoli locali dell'organizzazione di sistema.
- 7 (Facoltativo) Immettere le informazioni di contatto per l'utente.
È possibile immettere il nome completo, l'indirizzo e-mail, il numero di telefono e l'ID utilizzato per la messaggistica istantanea.
- 8 (Facoltativo) Impostare le quote per l'utente.
 - a È possibile impostare un limite per le macchine virtuali di proprietà dell'utente oppure selezionare **Illimitate**.
 - b È possibile impostare un limite per le macchine virtuali di proprietà dell'utente in esecuzione oppure selezionare **Illimitate**.

Importazione di utenti del provider

È possibile importare utenti nell'organizzazione del provider di VMware Cloud Director da un provider di identità LDAP o SAML configurato in precedenza.

Prerequisiti

[Configurazione di una connessione LDAP di sistema](#) o [Configurazione del sistema per l'utilizzo di un provider di identità SAML](#).

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Utenti**.
- 3 Fare clic su **Importa utenti**.
- 4 Dal menu a discesa **Origine** selezionare il tipo di provider di identità.
Può essere **LDAP** o **SAML**.
Se è stato configurato un solo provider di identità, questa opzione è hardcoded.

5 Specificare gli utenti.

Opzione	Descrizione
LDAP	<ol style="list-style-type: none"> Digitare il nome completo o parziale di un gruppo, quindi fare clic su Cerca. Dai risultati di ricerca selezionare gli utenti che si desidera importare. Dal menu a discesa Assegna ruolo selezionare un ruolo per gli utenti importati.
SAML	<ol style="list-style-type: none"> Immettere i nomi degli utenti che si desidera importare nel formato identificatore nome supportato dal provider di identità SAML. Utilizzare una nuova riga per ciascun nome utente. Dal menu a discesa Assegna ruolo selezionare un ruolo per gli utenti importati.

6 Fare clic su **Salva**.

Risultati

Gli utenti importati sono visualizzati nell'elenco degli utenti.

Modifica di un utente del provider

È possibile modificare password, ruolo, informazioni di contatto e quote di un utente nell'organizzazione del provider. Non è possibile modificare il nome utente.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Utenti**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'utente di destinazione e fare clic su **Modifica**.
- 4 Modificare i dettagli dell'utente e fare clic su **Salva**.

Disabilitazione o abilitazione di un utente del provider

Dopo essere stato disabilitato, un utente non può eseguire il login a VMware Cloud Director.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Utenti**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'utente di destinazione e scegliere **Disabilita** o su **Abilita**.
- 4 Se si intende disabilitare un utente, fare clic su **OK** per confermare.

Eliminazione di un utente del provider

È possibile rimuovere un utente dall'organizzazione del provider di VMware Cloud Director eliminando il relativo account.

Prerequisiti

Disabilitare l'utente che si desidera eliminare. Vedere [Disabilitazione o abilitazione di un utente del provider](#).

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Utenti**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'utente di destinazione e fare clic su **Elimina**.
- 4 Per confermare, fare clic su **OK**.

Sblocco di un utente di Provider

Se nelle impostazioni di sistema dei criteri delle password è stato abilitato il blocco degli account, è possibile che gli account degli utenti vengano bloccati dopo un determinato numero di tentativi di accesso non validi. Anche se il blocco è impostato con un intervallo di blocco account, è possibile sbloccare un account utente senza attendere la scadenza del blocco.

Per informazioni sulla configurazione dei criteri di blocco degli account, vedere [Configurazione dei criteri della password](#).

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Utenti**.
- 3 Fare clic sul pulsante di opzione accanto al nome dell'utente di destinazione e fare clic su **Sblocca**.

Gestione di gruppi di Provider

È possibile importare, modificare ed eliminare gruppi dall'organizzazione Provider utilizzando Service Provider Admin Portal.

Per informazioni sulla gestione dei gruppi nelle organizzazioni, vedere *VMware Cloud Director Tenant Portal Guide*.

Importazione di un gruppo di provider

È possibile importare gruppi nell'organizzazione del provider VMware Cloud Director da un provider di identità LDAP o SAML configurato in precedenza.

Prerequisiti

[Configurazione di una connessione LDAP di sistema](#) o [Configurazione del sistema per l'utilizzo di un provider di identità SAML](#).

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Gruppi**.
- 3 Fare clic su **Importa gruppi**.
- 4 Dal menu a discesa **Origine** selezionare il tipo di provider di identità.

Può essere **LDAP** o **SAML**.

Se è stato configurato un solo provider di identità, questa opzione è hardcoded.

- 5 Specificare gli utenti.

Opzione	Descrizione
LDAP	<ol style="list-style-type: none"> a Digitare il nome completo o parte del nome di un gruppo, quindi fare clic su Cerca. b Nei risultati di ricerca selezionare i gruppi che si desidera importare. c Dal menu a discesa Assegna ruolo selezionare un ruolo per gli utenti nei gruppi importati.
SAML	<ol style="list-style-type: none"> a Immettere i nomi dei gruppi che si desidera importare nel formato identificatore nome supportato dal provider di identità SAML. Utilizzare una nuova riga per ciascun nome di gruppo. b Dal menu a discesa Assegna ruolo selezionare un ruolo per gli utenti nei gruppi importati.

- 6 Fare clic su **Salva**.

Modifica di un gruppo del provider

È possibile modificare la descrizione e il ruolo dei membri di un gruppo precedentemente importato nell'organizzazione del provider di VMware Cloud Director.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Gruppi**.
- 3 Fare clic sul pulsante di opzione accanto al nome del gruppo di destinazione e fare clic su **Modifica**.
- 4 Modificare i dettagli del gruppo e fare clic su **Salva**.

Eliminazione di un gruppo del provider

È possibile rimuovere un gruppo dall'organizzazione del provider di VMware Cloud Director

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Controllo accessi provider**, selezionare **Gruppi**.
- 3 Fare clic sul pulsante di opzione accanto al nome del gruppo di destinazione e fare clic su **Elimina**.
- 4 Per confermare, fare clic su **OK**.

Gestione delle impostazioni di sistema

11

Un amministratore di sistema di VMware Cloud Director può controllare le impostazioni a livello di sistema correlate alle preferenze generali del sistema, alle licenze, alla notifica tramite e-mail e a LDAP.

Questo capitolo include i seguenti argomenti:

- [Modifica delle impostazioni generali del sistema](#)
- [Impostazioni generali del sistema](#)
- [Configurazione delle impostazioni e-mail di sistema](#)
- [Modifica della licenza di VMware Cloud Director](#)
- [Configurazione delle impostazioni di sincronizzazione del catalogo](#)
- [Configurazione e monitoraggio delle attività bloccanti e delle notifiche](#)
- [Configurazione di indirizzi pubblici](#)
- [Gestione dei provider di identità](#)
- [Gestione dei plug-in](#)
- [Personalizzazione dei portali di VMware Cloud Director](#)
- [Configurazione dei criteri della password](#)
- [Configurazione dei servizi di vSphere](#)

Modifica delle impostazioni generali del sistema

VMware Cloud Director include le impostazioni di sistema generali relative ai registri delle attività, ai servizi di rete, ai timeout delle sessioni, ai certificati, ai limiti dell'organizzazione, ai limiti delle operazioni e così via. Le impostazioni predefinite sono valide per diversi ambienti, ma è possibile modificarle in base alle esigenze.

Per un elenco delle proprietà che è possibile modificare, vedere [Impostazioni generali del sistema](#).

Nota Per informazioni su come modificare data, ora o fuso orario dell'appliance VMware Cloud Director, vedere <https://kb.vmware.com/kb/59674>.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Impostazioni**, fare clic su **Generale**.
- 3 Fare clic su **Modifica** per la sezione che si desidera modificare, quindi modificare le proprietà e fare clic su **Salva**.

Impostazioni generali del sistema

In VMware Cloud Director sono disponibili impostazioni generali del sistema che è possibile modificare in base alle proprie esigenze.

Tabella 11-1. Impostazioni generali del sistema

Nome	Categoria	Descrizione
Activity log history to keep	Registro attività	Numero di giorni in cui conservare la cronologia registro prima che venga eliminata. Immettere 0 per non eliminare mai i registri.
Activity log history shown	Registro attività	Numero di giorni in cui visualizzare la cronologia registro. Per visualizzare tutte le attività, immettere 0 .
Display debug information	Registro attività	Abilitare questa impostazione per visualizzare le informazioni di debug nel registro dei task di VMware Cloud Director.
IP address release timeout	Rete	Numero di secondi per mantenere in sospenso gli indirizzi IP rilasciati prima di renderli di nuovo disponibili per l'allocazione. L'impostazione predefinita è pari a 2 ore (7200 secondi) e consente la scadenza degli elementi meno recenti dalle tabelle ARP del client.
Allow Overlapping External Networks	Rete	Per aggiungere reti esterne in esecuzione sullo stesso segmento di rete, selezionare la casella di controllo. Abilitare questa impostazione solo se si utilizzano metodi non basati su VLAN per isolare le reti esterne.
Allow FIPS mode	Rete	Consente l'abilitazione della modalità FIPS negli edge gateway. Richiede NSX 6.3 o versione successiva. Vedere la sezione relativa alla modalità FIPS nella documentazione di <i>VMware NSX for vSphere</i> .
Default syslog server settings for networks	Rete	Immettere gli indirizzi IP per un massimo di due server Syslog da utilizzare nelle reti. Questa impostazione non è applicabile ai server Syslog utilizzati dalle celle Cloud.
Provider Locale	Localizzazione	Selezionare le impostazioni internazionali per l'attività del provider, inclusi le voci del registro, gli avvisi e-mail e così via.
Idle session timeout	Timeout	Quantità di tempo in cui l'applicazione VMware Cloud Director rimane attiva senza intervento dell'utente.

Tabella 11-1. Impostazioni generali del sistema (continua)

Nome	Categoria	Descrizione
Maximum session timeout	Timeout	Quantità massima di tempo in cui l'applicazione VMware Cloud Director rimane attiva.
Host refresh frequency	Timeout	Frequenza con cui VMware Cloud Director verifica l'accessibilità dei relativi host ESXi.
Host hung timeout	Timeout	Selezionare la quantità di tempo di attesa prima che un host venga contrassegnato come bloccato.
Transfer session timeout	Timeout	Quantità di tempo di attesa prima che si verifichi un errore di un task di caricamento sospeso o annullato, ad esempio il caricamento di un file multimediale o del modello di vApp. Questo timeout non influenza i task di caricamento in corso.
Enable upload quarantine with a timeout of __ seconds	Timeout	Selezionare la casella di controllo e immettere un valore numerico di timeout che rappresenti la quantità di tempo per la quarantena dei file caricati.
Verify vCenter and vSphere SSO certificates	Certificati	VMware Cloud Director verifica sempre i certificati. Quando l'opzione è abilitata, verifica i nomi host nei certificati di vCenter Server.
Verify NSX Manager certificates	Certificati	VMware Cloud Director verifica sempre i certificati. Quando l'opzione è abilitata, VMware Cloud Director verifica i nomi host nei certificati di NSX Manager.
Edit Organization Limits	Limiti VDC organizzazione	Immettere il numero massimo di virtual data center per organizzazione o selezionare Illimitato .
Number of resource intensive operations running per user	Limiti operativi	Immettere il numero massimo di operazioni simultanee che utilizzano molte risorse per utente oppure selezionare Illimitato .
Number of resource intensive operations to be queued per user (in addition to running)	Limiti operativi	Immettere il numero massimo di operazioni inserite in coda che utilizzano molte risorse per utente oppure selezionare Illimitato .
Number of resource intensive operations running per organization	Limiti operativi	Immettere il numero massimo di operazioni simultanee che utilizzano molte risorse per organizzazione oppure selezionare Illimitato .
Number of resource intensive operations to be queued per organization	Limiti operativi	Immettere il numero massimo di operazioni inserite in coda che utilizzano molte risorse per organizzazione oppure selezionare Illimitato .
Provide default vApp names	Altro	Selezionare la casella di controllo per configurare VMware Cloud Director in modo che fornisca i nomi predefiniti per le nuove vApp.

Tabella 11-1. Impostazioni generali del sistema (continua)

Nome	Categoria	Descrizione
Make Allocation pool Org VDCs elastic	Altro	Selezionare la casella di controllo per abilitare il pool di allocazione elastico, per rendere elastici tutti i virtual data center dell'organizzazione del pool di allocazione. Prima di deselezionare questa opzione, assicurarsi che tutte le macchine virtuali per ciascun virtual data center dell'organizzazione siano state migrate a un cluster singolo.
VM discovery enabled	Altro	Per impostazione predefinita, ogni VDC dell'organizzazione rileva automaticamente le macchine virtuali vCenter create in qualsiasi pool di risorse sottostante al VDC. Deselezionare l'opzione per disattivare questa impostazione per tutti i VDC nel sistema.

Configurazione delle impostazioni e-mail di sistema

È possibile modificare le impostazioni e-mail di sistema, tra cui la configurazione delle impostazioni del server SMTP e delle impostazioni di notifica di VMware Cloud Director.

VMware Cloud Director richiede l'utilizzo di un server SMTP per l'invio di messaggi e-mail di notifica e di avviso agli utenti del sistema.

VMware Cloud Director invia e-mail di avviso di sistema quando è necessario segnalare informazioni importanti. Ad esempio, VMware Cloud Director invia un avviso quando lo spazio di un archivio dati sta per esaurirsi. È possibile configurare VMware Cloud Director in modo da inviare avvisi e-mail a tutti gli amministratori di sistema oppure a un elenco specifico di indirizzi e-mail.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel riquadro a sinistra, in **Impostazioni**, selezionare **E-mail** e fare clic su **Modifica**.
- 3 Immettere il nome host DNS o l'indirizzo IP del server di posta SMTP.
- 4 Immettere il numero di porta del server SMTP.
- 5 (Facoltativo) Se il server SMTP richiede un nome utente, attivare l'opzione **Richiede autenticazione** e immettere il nome utente e la password dell'account SMTP.
- 6 Selezionare la scheda **Impostazioni di notifica**.
- 7 Immettere un indirizzo e-mail da visualizzare come mittente dei messaggi e-mail di VMware Cloud Director.

VMware Cloud Director utilizza l'indirizzo e-mail del mittente per inviare avvisi di scadenza del lease di runtime e dello storage.

- 8 (Facoltativo) Immettere il testo per il prefisso dell'oggetto.

9 Selezionare i destinatari delle notifiche.

Per impostazione predefinita, solo gli amministratori dell'organizzazione ricevono le notifiche SMTP.

10 Fare clic su **Salva**.

11 (Facoltativo) Testare le impostazioni SMTP.

- a Fare clic su **Test**.
- b Se è stata abilitata l'opzione **Richiede l'autenticazione**, immettere la password del server SMTP.
- c Immettere un indirizzo e-mail di destinazione e fare clic su **Test**.

Modifica della licenza di VMware Cloud Director

Per eseguire VMware Cloud Director, è necessario disporre di una licenza valida, specificata come numero di serie. È possibile modificare le informazioni della licenza immesse durante la configurazione iniziale di VMware Cloud Director.

Il numero di serie di VMware Cloud Director non corrisponde al codice di licenza di vCenter Server. È possibile ottenere un numero di serie di VMware Cloud Director dal portale delle licenze VMware.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel riquadro a sinistra, selezionare **Licenza** e fare clic su **Modifica**.
- 3 Immettere un nuovo numero di serie e fare clic su **Salva**.

Configurazione delle impostazioni di sincronizzazione del catalogo

È possibile modificare le impostazioni di sincronizzazione del catalogo per tutte le organizzazioni e i cataloghi, inclusa la frequenza di aggiornamento delle sottoscrizioni del catalogo.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel riquadro a sinistra, in **Impostazioni**, selezionare **Catalogo**.
- 3 Fare clic su **Modifica**.
- 4 Abilitare la sincronizzazione del catalogo.
- 5 Impostare gli orari di avvio e arresto della sincronizzazione.

6 Impostare l'intervallo di sincronizzazione.

L'intervallo di sincronizzazione è la frequenza di aggiornamento delle sottoscrizioni del catalogo.

7 Fare clic su **Salva**.

Operazioni successive

Per ulteriori informazioni sulla configurazione della limitazione della sincronizzazione del catalogo, vedere *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*

Configurazione e monitoraggio delle attività bloccanti e delle notifiche

È possibile utilizzare le attività bloccanti e le notifiche per configurare VMware Cloud Director per l'invio di messaggi AMQP attivati da determinati eventi.

Alcuni di questi messaggi sono semplici notifiche che indicano che si è appena verificato un evento. Altri messaggi pubblicano informazioni in un endpoint AMQP designato per indicare che un'azione richiesta è stata bloccata ed è in attesa di azione da parte di un'applicazione client associata a tale endpoint. Tali messaggi sono noti come attività bloccanti.

Un **amministratore di sistema** può configurare un set di attività bloccanti a livello di sistema soggette a un'azione programmatica da parte di un client AMQP.

Configurazione di un broker AMQP

Se si desidera che VMware Cloud Director invii messaggi AMQP attivati da determinati eventi, è necessario configurare un broker AMQP. È possibile utilizzare i messaggi AMQP per automatizzare la gestione di una richiesta dell'utente sottostante.

Procedura

1 Nella barra di navigazione superiore, selezionare **Amministrazione**.

2 In **Impostazioni**, selezionare **Estendibilità**.

Viene aperta la scheda **Broker AMQP**.

3 Fare clic sul pulsante **Modifica** della sezione **Broker AMQP**.

4 Immettere il nome host DNS o l'indirizzo IP dell'host AMQP.

Nome di dominio completo dell'host del server RabbitMQ, ad esempio *amqp.example.com*.

5 Immettere la porta AMQP.

La porta predefinita in cui il broker si mette in ascolto dei messaggi è 5672.

6 Immettere l'istanza di Exchange.

7 Immettere il vHost.

La porta predefinita è /.

8 Immettere il prefisso.**9** (Facoltativo) Per utilizzare SSL, attivare l'interruttore **Usa SSL** e selezionare una delle opzioni del certificato.

Per impostazione predefinita, il servizio AMQP di VMware Cloud Director invia messaggi non crittografati. È possibile configurare il servizio AMQP per crittografare questi messaggi utilizzando SSL. È inoltre possibile configurare il servizio per verificare il certificato del broker utilizzando l'archivio attendibilità JCEKS predefinito dell'ambiente di runtime Java nella cella di VMware Cloud Director, in genere in `$VCLOUD_HOME/jre/lib/security/cacerts`.

Opzione	Descrizione
Accetta tutti i certificati	Il record CN del campo relativo al proprietario del certificato deve corrispondere al nome host del broker AMQP. Per utilizzare certificati che non corrispondono al nome host del broker, attivare l'interruttore Accetta tutti i certificati .
Certificato SSL	Caricare il certificato SSL.
Archivio chiavi SSL (JCEKS)	Caricare l'archivio chiavi SSL e immettere la password dell'archivio chiavi.

10 Immettere un nome utente e una password per la connessione all'host AMQP.**11** Fare clic su **Salva**.**12** (Facoltativo) Per testare le impostazioni, fare clic sul pulsante **Test** sotto la sezione **Broker AMQP** e specificare la password.**13** (Facoltativo) Per pubblicare gli eventi di controllo nel broker AMQP, fare clic sul pulsante **Modifica** sotto la sezione **Notifiche AMQP non bloccanti** e attivare l'interruttore **Abilita notifiche**.

Configurazione delle impostazioni relative alle attività bloccanti

È possibile configurare determinate operazioni come attività bloccanti. Queste operazioni vengono sospese finché un **amministratore di sistema** non esegue determinate azioni o fino alla scadenza di un timer preconfigurato. È possibile specificare le impostazioni di timeout e le azioni predefinite per le attività bloccanti. Le impostazioni si applicano a tutte le organizzazioni dell'installazione.

Procedura

1 Nella barra di navigazione superiore, selezionare **Amministrazione**.**2** In **Impostazioni**, selezionare **Estendibilità**.**3** Fare clic sulla scheda **Attività bloccanti**.

- 4 Per modificare il timeout dell'estensione predefinito e l'azione di timeout predefinita, fare clic sul pulsante **Modifica** nella sezione **Generale**.
 - a Modificare il valore in **Timeout attività bloccante predefinito**.
 - b Modificare il valore in **Azione timeout predefinita**.

Azione timeout predefinita è l'azione dopo la scadenza del valore indicato in **Timeout attività bloccante predefinito**.
 - c Fare clic su **Salva**.
- 5 Per modificare l'elenco di operazioni, considerate come attività bloccanti, fare clic sul pulsante **Modifica** nella sezione **Operazioni**.
 - a Selezionare o deselezionare le operazioni nell'elenco di attività bloccanti.
 - b Fare clic su **Salva**.

Monitoraggio delle attività bloccanti

È possibile monitorare le attività attualmente bloccate oppure annullare, non completare o riprendere manualmente le attività prima che scada il timer preconfigurato.

Prerequisiti

[Configurazione delle impostazioni relative alle attività bloccanti](#)

Procedura

- 1 Nella barra di navigazione superiore, in **Monitora**, selezionare **Attività bloccanti**.

La scheda include un elenco delle attività attualmente bloccate.
- 2 Selezionare l'attività che si desidera modificare manualmente.
- 3 Decidere se annullare, non completare o riprendere l'attività e fare clic sul pulsante corrispondente.
- 4 Immettere un messaggio e fare clic su **Salva**.

Il messaggio viene visualizzato nei dettagli dell'attività.

Configurazione di indirizzi pubblici

Per soddisfare i requisiti del bilanciamento del carico o del proxy, è possibile modificare gli indirizzi Web degli endpoint predefiniti per il portale Web di VMware Cloud Director, l'API di VMware Cloud Director e il proxy della console.

Gli indirizzi pubblici rappresentano indirizzi Web esposti ai client di VMware Cloud Director. Le impostazioni predefinite per questi indirizzi vengono specificate durante l'installazione. Se necessario, è possibile aggiornare gli indirizzi.

Se VMware Cloud Director contiene solo una cella, il programma di installazione crea endpoint pubblici che in genere forniscono un accesso sufficiente per i client API e Web. Le installazioni e le distribuzioni che includono più celle inseriscono in genere un bilanciamento del carico tra le celle e i client. I client effettuano l'accesso al sistema all'indirizzo del bilanciamento del carico. Il bilanciamento del carico distribuisce le richieste del client attraverso le celle disponibili. Altre configurazioni di rete che includono un proxy o inseriscono le celle in una DMZ richiedono anche endpoint personalizzati. I dettagli dell'URL dell'endpoint sono specifici della propria configurazione di rete.

Gli endpoint per il VMware Cloud Director Tenant Portal e la console Web di VMware Cloud Director richiedono certificati SSL, preferibilmente firmati. Quando si installa o si distribuisce VMware Cloud Director, è necessario specificare il percorso di questi certificati. Se si personalizza uno di questi endpoint dopo l'installazione o la distribuzione, potrebbe essere necessario installare nuovi certificati corrispondenti ai dettagli dell'endpoint come `hostname` e `subject alternative name`.

Per l'appliance di VMware Cloud Director, è necessario configurare l'indirizzo del proxy della console pubblica di VMware Cloud Director, perché l'appliance utilizza un singolo indirizzo IP con la porta personalizzata 8443 per il servizio proxy della console. Vedere [Passaggio 6](#).

Prerequisiti

Verificare di aver effettuato l'accesso come **amministratore di sistema**. Solo un **amministratore di sistema** può personalizzare gli endpoint pubblici.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Impostazioni**, fare clic su **Indirizzi pubblici**.
- 3 Per personalizzare gli endpoint pubblici, fare clic su **Modifica**.
- 4 Per personalizzare gli URL di VMware Cloud Director, modificare gli endpoint del **Portale Web**.
 - a Immettere un URL pubblico di VMware Cloud Director personalizzato per le connessioni HTTP (non sicure).
 - b Immettere un URL pubblico di VMware Cloud Director personalizzato per le connessioni HTTPS (sicure) e fare clic su **Carica** per caricare i certificati che stabiliscono la catena di attendibilità per l'endpoint.

La catena di certificati deve corrispondere al certificato utilizzato dall'endpoint del servizio, che è il certificato caricato in ogni archivio chiavi di cella di VMware Cloud Director con alias `consoleproxy`. La terminazione SSL delle connessioni del proxy della console in un bilanciamento del carico non è supportata. La catena di certificati deve includere un certificato di endpoint, certificati intermedi e un certificato root nel formato `PEM` senza una chiave privata.

5 (Facoltativo) Per personalizzare l'API REST di Cloud Director e gli URL di OpenAPI, disattivare l'opzione **Usa impostazioni portale Web**.

- a Immettere un URL di base HTTP personalizzato.

Ad esempio, se si imposta l'URL di base HTTP su **http://vcloud.example.com**, è possibile accedere all'API di VMware Cloud Director all'indirizzo `http://vcloud.example.com/api` ed è possibile accedere a VMware Cloud Director OpenAPI all'indirizzo `http://vcloud.example.com/cloudapi`.

- b Immettere un URL di base dell'API REST HTTPS personalizzato e fare clic su **Carica** per caricare i certificati che stabiliscono la catena di attendibilità per l'endpoint.

Ad esempio, se si imposta l'URL di base dell'API REST HTTPS su **https://vcloud.example.com**, è possibile accedere all'API di VMware Cloud Director all'indirizzo `https://vcloud.example.com/api` ed è possibile accedere a VMware Cloud Director OpenAPI all'indirizzo `https://vcloud.example.com/cloudapi`.

La catena di certificati deve corrispondere al certificato utilizzato dall'endpoint del servizio, che è il certificato caricato in ogni archivio chiavi di cella di VMware Cloud Director con alias `http` o il certificato VIP del bilanciamento del carico se viene utilizzata una terminazione SSL. La catena di certificati deve includere un certificato di endpoint, certificati intermedi e un certificato root nel formato `PEM` senza una chiave privata.

6 Immettere un indirizzo proxy della console pubblica di VMware Cloud Director personalizzato.

- Personalizzare l'indirizzo del proxy della console pubblica dell'appliance di VMware Cloud Director.

Questo indirizzo è il nome di dominio completo (FQDN) del NIC `eth0` dell'appliance di VMware Cloud Director, specificato in base al nome di dominio completo o all'indirizzo IP, con porta personalizzata `8443` per il servizio proxy della console.

- Personalizzare VMware Cloud Director nell'indirizzo del proxy della console pubblica di Linux.

Questo indirizzo è il nome di dominio completo del server VMware Cloud Director o del bilanciamento del carico con il numero di porta. La porta predefinita è `443`.

Ad esempio, per l'istanza di un'appliance VMware Cloud Director con nome di dominio completo `vcloud.example.com`, immettere **`vcloud.example.com:8443`**.

VMware Cloud Director utilizza l'indirizzo del proxy della console quando viene aperta una finestra di console remota in una macchina virtuale.

7 Fare clic su **Salva**.

Gestione dei provider di identità

È possibile integrare il cloud con un provider di identità esterno e importare utenti e gruppi nelle organizzazioni. È possibile configurare una connessione al server LDAP a livello del sistema o dell'organizzazione. È possibile configurare un'integrazione SAML a livello dell'organizzazione.

Gestione di connessioni LDAP

Un amministratore di sistema può configurare l'organizzazione di sistema di VMware Cloud Director e qualsiasi altra organizzazione nel sistema in modo che utilizzino un server LDAP come origine di utenti e gruppi. Le organizzazioni possono utilizzare la connessione LDAP di sistema o una connessione LDAP privata.

A partire dalla versione 10.1, VMware Cloud Director sta passando a in un'area di storage centralizzata con supporto del tenant per la gestione dei certificati. In questo modo, VMware Cloud Director centralizza tutti i certificati in un'unica posizione per consentire agli **amministratori di sistema** e agli **amministratori dell'organizzazione** di visualizzare, controllare e gestire tutti i certificati utilizzati dai vari componenti nel sistema. È possibile utilizzare l'API di VMware Cloud Director per aggiungere, aggiornare o rimuovere certificati dalla nuova area di storage con supporto del tenant. Vedere *Riferimento dello schema dell'API di VMware Cloud Director*.

Quando si aggiunge o si modifica un nuovo endpoint di un server LDAP, l'interfaccia utente di VMware Cloud Director esegue il probe dell'endpoint per tutti i certificati che presenta. VMware Cloud Director aggiunge a un'area di storage di certificati centralizzata qualsiasi certificato che si decide di considerare attendibile.

Configurazione di una connessione LDAP di sistema

Per offrire a VMware Cloud Director e alle relative organizzazioni l'accesso condiviso a utenti e gruppi, è possibile configurare una connessione LDAP a livello di sistema.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Provider di identità**, fare clic su **LDAP**.

Vengono visualizzate le impostazioni di LDAP correnti.

Operazioni successive

[Configurazione, prova e sincronizzazione di una connessione LDAP](#).

Configurazione di una connessione LDAP dell'organizzazione

È possibile configurare un'organizzazione in modo che utilizzi la connessione LDAP del sistema come origine condivisa di utenti e gruppi. È possibile configurare un'organizzazione in modo che utilizzi una connessione LDAP distinta come origine privata di utenti e gruppi.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro selezionare **Organizzazioni**.
- 3 Fare clic sul nome dell'organizzazione di destinazione.

Si verrà reindirizzati al portale tenant di VMware Cloud Director dell'organizzazione.

- 4 Nella barra di navigazione superiore, selezionare **Amministrazione**.

- 5 Nel pannello sinistro, in **Provider di identità**, fare clic su **LDAP**.

Vengono visualizzate le impostazioni di LDAP correnti.

- 6 Nella scheda **Opzioni LDAP**, fare clic su **Modifica**.

- 7 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 VCD	L'organizzazione utilizza la connessione LDAP del sistema VMware Cloud Director che è stata configurata in precedenza. Vedere Configurazione di una connessione LDAP di sistema .
Servizio LDAP personalizzato	L'organizzazione utilizza un server LDAP privato come origine di utenti e gruppi dell'organizzazione. Fare clic sulla scheda LDAP personalizzato e 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>.

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 sull'icona di caricamento () 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>

- 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.
- 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.
- Fare clic su **Salva**.
- 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.

Configurazione del sistema per l'utilizzo di un provider di identità SAML

Se si desidera importare utenti e gruppi da un provider di identità SAML nell'organizzazione di sistema, è necessario configurare l'organizzazione di sistema con tale provider di identità SAML. Gli utenti importati possono accedere all'organizzazione di sistema con le credenziali stabilite nel provider di identità SAML.

Per configurare VMware Cloud Director con un provider di identità SAML, stabilire una relazione di attendibilità reciproca mediante lo scambio dei metadati del provider di identità e del provider di servizi SAML.

Quando un utente importato tenta di accedere, il sistema estrae i seguenti attributi dal token SAML, se disponibile, e li utilizza per interpretare le informazioni sull'utente corrispondenti.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"` (questo attributo è configurabile)

Le informazioni sul gruppo vengono utilizzate se l'utente non viene importato direttamente ma si suppone che acceda in virtù dell'appartenenza ai gruppi importati. Un utente può appartenere a più gruppi e pertanto può disporre di più ruoli durante una sessione.

Se un utente o un gruppo importato viene assegnato al 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 utilizzando l'API e solo l'attributo Ruoli è configurabile. Se viene utilizzato il ruolo Rimanda a provider di identità e non è possibile estrarre alcuna informazione sul ruolo, l'utente può accedere ma non dispone di alcun diritto per eseguire le attività.


Prerequisiti

- Verificare di disporre dell'accesso a un provider di identità compatibile con SAML 2.0.
- Ottenere un file XML con i seguenti metadati dal provider di identità SAML.
 - Posizione del servizio single sign-on
 - Posizione del servizio single logout
 - Posizione del certificato del servizio X.509

Per informazioni sulla configurazione e l'acquisizione di metadati da un provider SAML, consultare la documentazione del provider SAML.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in Provider di identità, fare clic su **SAML** e quindi su **Modifica**.
Vengono visualizzate le impostazioni di SAML correnti.
- 3 Nella scheda **Provider di servizi**, scaricare i metadati del provider di servizi SAML di VMware Cloud Director.
 - a Immettere un ID entità per l'organizzazione di sistema.
L'ID entità identifica in modo univoco l'organizzazione di sistema per il provider di identità.
 - b Esaminare la data di scadenza del certificato e, se prossima, rigenerare il certificato facendo clic su **Rigenera**.
Il certificato è incluso nei metadati SAML e viene utilizzato per la crittografia e per la firma. Potrebbe essere necessario eseguire una di queste operazioni o entrambe, in base a come viene stabilita la relazione di attendibilità tra l'organizzazione e il provider di identità SAML.
 - c Fare clic sul collegamento **Metadati**.
Il collegamento è simile a `https://VCD_host_name/cloud/org/System/saml/metadata/alias/vcd`.
Il browser scarica i metadati del provider di servizi SAML, un file XML che è necessario fornire al provider di identità.

- 4 Nella scheda **Provider di identità**, caricare i metadati SAML ricevuti in precedenza dal provider di identità.
 - a Selezionare **Utilizza provider identità SAML**.
 - b Fare clic sull'icona **Sfoglia** () e caricare il file o copiare e incollare il suo contenuto nella casella di testo **XML metadati**.
- 5 Fare clic su **Salva**.

Risultati

Gestione dei plug-in

I plug-in di VMware Cloud Director estendono le funzioni di Service Provider Admin Portal e VMware Cloud Director Tenant Portal. È possibile caricare, disabilitare ed eliminare plug-in dal Service Provider Admin Portal. È possibile pubblicare un plug-in per il provider di servizi e le singole organizzazioni.

Alcuni plug-in sono installati come parte di VMware Cloud Director.

Estensione CPOM

Offre la possibilità di visualizzare e gestire proxy e istanze di vCenter Server dedicate utilizzando VMware Cloud Director Tenant Portal.

Personalizza portale

Fornisce la funzionalità per la personalizzazione di VMware Cloud Director Service Provider Admin Portal e VMware Cloud Director Tenant Portal.

Disponibilità vCloud

Il plug-in VMware vCloud[®] Availability[™] offre la possibilità di accedere a vCloud Availability Portal direttamente dall'interfaccia utente di VMware Cloud Director. Per ulteriori informazioni, vedere la [documentazione di vCloud Availability](#).

Caricamento di un plug-in

È possibile caricare plug-in aggiuntivi in VMware Cloud Director Service Provider Admin Portal in modo che possano essere utilizzati dal provider di servizi e dalle organizzazioni nel cloud.

Prerequisiti

Scaricare il file di installazione del plug-in.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Altro > Personalizza portale**.
- 2 Fare clic su **Carica**.

- 3 Fare clic su **Seleziona file del plug-in**, selezionare il file di installazione di destinazione e fare clic su **Apri**.
- 4 Fare clic su **Avanti**.
- 5 Selezionare l'ambito per il plug-in.

Opzione	Descrizione
Provider di servizi	La funzionalità del plug-in diventa disponibile nel VMware Cloud Director Service Provider Admin Portal.
Tenant	La funzionalità del plug-in diventa disponibile nel VMware Cloud Director Service Provider Admin Portal delle organizzazioni selezionate.

- 6 Se è stato selezionato l'ambito Tenant per il plug-in, selezionare le organizzazioni in cui si desidera pubblicare il plug-in.
- 7 Controllare la pagina **Verifica e completa** e fare clic su **Fine**.

Abilitazione o disabilitazione di un plug-in

Per impedire a tutte le organizzazioni di utilizzare un plug-in, è possibile disabilitare questo plug-in.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Altro > Personalizza portale**.
- 2 Selezionare la casella di controllo accanto ai nomi dei plug-in di destinazione e fare clic su **Abilita o Disabilita**.

Eliminazione di un plug-in

È possibile rimuovere uno o più plug-in dal VMware Cloud Director Service Provider Admin Portal.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Altro > Personalizza portale**.
- 2 Selezionare le caselle di controllo accanto ai nomi dei plug-in che si desidera rimuovere e fare clic su **Elimina**.
- 3 Per confermare, fare clic su **Salva**.

Pubblica o Annulla la pubblicazione di un plug-in da un'organizzazione

È possibile modificare il set di organizzazioni che possono utilizzare la funzione fornita da un plug-in.

È possibile modificare il set di organizzazioni per più plug-in.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Altro > Personalizza portale**.
- 2 Selezionare le caselle di controllo accanto ai nomi dei plug-in di destinazione e fare clic su **Pubblica**.
- 3 Selezionare l'ambito per questo plug-in.

Opzione	Descrizione
Provider di servizi	La funzione del plug-in diventa disponibile nella VMware Cloud Director Service Provider Admin Portal.
Tenant	La funzione del plug-in diventa disponibile nella VMware Cloud Director Service Provider Admin Portal delle organizzazioni selezionate.

- 4 Se si dispone dell'ambito del plug-in per i tenant, selezionare le organizzazioni in cui si desidera pubblicare questo plug-in.
- 5 Fare clic su **Salva**.

Personalizzazione dei portali di VMware Cloud Director

Per associare gli standard di branding aziendali e creare un'esperienza cloud completamente personalizzata, è possibile impostare il logo e il tema per VMware Cloud Director Service Provider Admin Portal e per il VMware Cloud Director Tenant Portal di ciascuna organizzazione. Inoltre, è possibile modificare e aggiungere collegamenti personalizzati nei due menu in alto a destra nei portali di VMware Cloud Director.

Nota Per personalizzare gli attributi e i collegamenti di branding, è necessario utilizzare i metodi `branding` di vCloud OpenAPI. Vedere *Guida introduttiva a VMware Cloud Director OpenAPI* all'indirizzo <https://code.vmware.com>.

Branding del portale

Come parte dell'installazione, VMware Cloud Director contiene due temi, predefinito e scuro. È possibile creare, gestire e applicare temi personalizzati. È inoltre possibile modificare il nome del portale, il logo e l'icona del browser. Il titolo del browser adotta inoltre il nome del portale impostato.

È possibile impostare gli attributi di branding a livello di sistema, in modo da personalizzare VMware Cloud Director Service Provider Admin Portal. Il VMware Cloud Director Tenant Portal per ogni organizzazione adotta gli attributi di branding del sistema a meno che non vengano configurati attributi di branding per il tenant specifico.

Per un determinato tenant, è possibile sovrascrivere in modo selettivo qualsiasi combinazione del nome del portale, del colore di sfondo, del logo, dell'icona, del tema e dei collegamenti personalizzati. Qualsiasi valore non impostato utilizza il valore predefinito del sistema corrispondente.

Nota Per impostazione predefinita, il branding del tenant individuale non viene visualizzato all'esterno di una sessione di accesso. Il branding del tenant individuale non viene visualizzato nelle pagine di accesso e disconnessione, in modo che i tenant non possano scoprire l'esistenza di altri tenant. È possibile abilitare il branding al di fuori delle sessioni di accesso utilizzando lo strumento di gestione delle celle:

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

Per informazioni sull'uso dello strumento di gestione delle celle, vedere la *Guida all'installazione, alla configurazione e all'aggiornamento di VMware Cloud Director*.

Collegamenti personalizzati

I collegamenti personalizzati sono un componente del branding del portale. Sono disponibili due tipi di collegamenti personalizzati:

- Le voci di menu di `override` sostituiscono i collegamenti esistenti per le voci di menu **Guida**, **Informazioni** e **Scarica VMRC**. Per impostazione predefinita, **Scarica VMRC** reindirizza gli utenti a <https://my.vmware.com> per scaricare VMRC. Per eseguire questa operazione, gli utenti devono disporre di account registrati per il download. Sovrascrivendo questo collegamento, è possibile trasferire il programma di installazione di VMRC nel proprio server.
- Le voci di menu `link` sono nuovi collegamenti aggiunti alla voce di menu **Esci** nell'angolo superiore destro del portale. I nuovi collegamenti personalizzati vengono visualizzati nell'ordine indicato nella chiamata API.

È possibile organizzare questi collegamenti personalizzati utilizzando le voci di menu `section` e `separator`. Una voce di menu `section` aggiunge un'intestazione al menu, mentre una voce di menu `separator` aggiunge una riga al menu.

I collegamenti personalizzati supportano variabili personalizzate che è possibile utilizzare per passare informazioni di identificazione ad altre applicazioni sotto forma di parametri di query.

VMware Cloud Director supporta le seguenti variabili personalizzate nel valore `url` per un collegamento personalizzato:

Tabella 11-2. Variabili personalizzate per i collegamenti personalizzati

Variabile	Descrizione
<code>\${TENANT_NAME}</code>	Nome organizzazione
<code>\${TENANT_ID}</code>	ID organizzazione
<code>\${SESSION_TOKEN}</code>	Token x-vcloud-authorization

Ad esempio,

```
url: https://host:port/tenant/${TENANT_NAME}/vdc
```

nel VMware Cloud Director Tenant Portal per myorg dell'organizzazione viene convertito in:

```
url: https://host:port/tenant/myorg/vdc
```

Configurazione dei criteri della password

Per impedire a un utente di accedere a VMware Cloud Director dopo un certo numero di tentativi non riusciti, è possibile abilitare il blocco dell'account.

Modifiche all'applicazione dei criteri di blocco degli account di sistema per tutte le nuove organizzazioni. Le organizzazioni create prima delle modifiche ai criteri di blocco degli account devono essere modificate a livello aziendale.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Impostazioni**, fare clic su **Criterio password**.
- 3 Fare clic su **Modifica**.
- 4 Per abilitare il blocco dell'account, attivare l'interruttore **Blocco account**.
- 5 Selezionare il numero di login non validi da accettare prima di bloccare un account.
- 6 Selezionare l'intervallo del blocco.
- 7 Per abilitare il blocco dell'account dell'**amministratore di sistema**, attivare l'interruttore **L'account dell'amministratore di sistema può essere bloccato**.
- 8 Fare clic su **Salva**.

Configurazione dei servizi di vSphere

È possibile configurare e abilitare VMware Cloud Director per l'utilizzo di vCenter Single Sign-On in modo che il provider di identità di vSphere esegua l'autenticazione degli amministratori di sistema.

vCenter Lookup Service contiene informazioni sulla topologia dell'infrastruttura di vSphere, consentendo ai componenti di vSphere di connettersi reciprocamente in modo sicuro.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Amministrazione**.
- 2 Nel riquadro a sinistra, in **Impostazioni**, selezionare **Servizi vSphere**.
- 3 Configurare i servizi di vSphere.
 - Per registrare VMware Cloud Director in vCenter Lookup Service, fare clic su **Registra**.

- Per annullare la registrazione di VMware Cloud Director in vCenter Lookup Service, fare clic su **Annulla registrazione**.
- 4 Immettere l'URL di vCenter Lookup Service, ad esempio `https://hostname:443/lookupservice/sdk`.
 - 5 Immettere il nome utente e la password di un utente di vCenter Single Sign-On con privilegi amministrativi, ad esempio l'utente `administrator@your_domain_name`.

Risultati

Se VMware Cloud Director è stato registrato in vCenter Lookup Service, gli **amministratori di sistema** devono accedere a VMware Cloud Director con le loro credenziali vCenter Single Sign-On.

Monitoraggio di VMware Cloud Director

12

Gli amministratori di sistema possono monitorare le operazioni completate e in corso, nonché visualizzare le informazioni sull'utilizzo delle risorse a livello del virtual data center provider, del virtual data center dell'organizzazione e dell'archivio dati.

A partire dalla versione 9.1, VMware Cloud Director non supporta VMware vCenter Chargeback Manager. Vedere [Tabelle di interoperabilità dei prodotti VMware](#).

Questo capitolo include i seguenti argomenti:

- [VMware Cloud Director e report sui costi](#)
- [Visualizzazione delle informazioni di utilizzo per un virtual data center del provider](#)

VMware Cloud Director e report sui costi

È possibile utilizzare VMware vRealize Operations Tenant App per VMware Cloud Director per configurare un sistema di report dei costi per VMware Cloud Director.

VMware vRealize Operations Tenant App offre funzionalità di misurazione che consentono ai provider di servizi di fornire alla propria base clienti servizi di chargeback.

VMware vRealize Operations Tenant App è anche un'applicazione lato tenant che fornisce agli amministratori tenant la visibilità del proprio ambiente e dei relativi dati di fatturazione.

Per informazioni sulla compatibilità tra VMware Cloud Director e VMware vRealize Operations Tenant App, vedere le *Matrici di compatibilità dei prodotti VMware* in http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

È possibile scaricare VMware vRealize Operations Tenant App in <https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director>.

Per informazioni su come utilizzare VMware vRealize Operations Tenant App, vedere *Utilizzo dell'app del tenant di vRealize Operations per VMware Cloud Director come provider di servizi e Utilizzo dell'app del tenant di vRealize Operations per VMware Cloud Director come tenant*.

Visualizzazione delle informazioni di utilizzo per un virtual data center del provider

I virtual data center del provider forniscono risorse di elaborazione, memoria e storage ai rispettivi virtual data center dell'organizzazione. È possibile monitorare l'utilizzo delle risorse del virtual data center del provider, in modo da poter decidere se aggiungere altre risorse.

Procedura

- 1 Nella barra di navigazione superiore, in **Risorse**, selezionare **Risorse cloud**.
- 2 Nel pannello sinistro, selezionare **VDC del provider** e quindi fare clic sul nome del virtual data center del provider di destinazione.
- 3 Fare clic sulla scheda **Configura > Metriche**.
- 4 Per informazioni dettagliate su ciascun parametro, fare clic sull'icona delle informazioni corrispondente.

La visualizzazione Librerie di contenuti in VMware Cloud Director Service Provider Admin Portal fornisce un'interfaccia per l'integrazione con vRealize Orchestrator. I flussi di lavoro di vRealize Orchestrator sono disponibili in forma di catalogo di servizi che gli amministratori dei provider di servizi possono pubblicare nei tenant o in altri provider di servizi, estendendo in tal modo il set di funzionalità e caratteristiche di gestione offerti.

Questo capitolo include i seguenti argomenti:

- [Integrazione di vRealize Orchestrator con VMware Cloud Director](#)
- [Creazione di una categoria di servizi](#)
- [Modifica di una categoria di servizi](#)
- [Importazione di un servizio](#)
- [Ricerca di un servizio](#)
- [Esecuzione di un servizio](#)
- [Modifica di una categoria di servizio](#)
- [Annullamento della registrazione di un servizio](#)
- [Pubblicazione di un servizio](#)

Integrazione di vRealize Orchestrator con VMware Cloud Director

È possibile integrare vRealize Orchestrator con VMware Cloud Director attraverso VMware Cloud Director Service Provider Admin Portal.

L'integrazione di vRealize Orchestrator con VMware Cloud Director estende le funzionalità di base di VMware Cloud Director, consentendo agli amministratori dei provider di servizi di sviluppare complessi task di automazione tramite l'orchestrazione dei flussi di lavoro e l'utilizzo di plug-in di terze parti.

Tramite VMware Cloud Director Service Provider Admin Portal, gli amministratori dei provider di servizi possono visualizzare, importare ed eseguire i flussi di lavoro da istanze server di vRealize Orchestrator registrate.

In VMware Cloud Director Service Provider Admin Portal, i flussi di lavoro di vRealize Orchestrator possono essere pubblicati in provider di servizi o tenant, consentendo il controllo degli accessi rapido e l'esecuzione dei servizi personalizzati e integrati.

vRealize Orchestrator dispone di una libreria di flussi di lavoro completa che contiene task predefiniti progettati per risolvere problematiche specifiche ed eseguire task amministrativi comuni. Plug-in di terze parti sono disponibili anche in [VMware Solution Exchange](#).

Registrazione di un'istanza di vRealize Orchestrator con VMware Cloud Director

Per utilizzare al meglio l'orchestrazione dei flussi di lavoro e l'automazione dei task attraverso vRealize Orchestrator in VMware Cloud Director, registrare un'istanza di vRealize Orchestrator in VMware Cloud Director Service Provider Admin Portal.


Prerequisiti

- Distribuire e configurare un'istanza server di vRealize Orchestrator. Per ulteriori informazioni, vedere *Installazione e configurazione di VMware vRealize Orchestrator* nella documentazione di vRealize Orchestrator.
- Configurare vRealize Orchestrator per utilizzare vSphere come provider di autenticazione.
- Verificare che VMware Cloud Director sia registrato con il servizio di ricerca dello stesso Platform Services Controller del vCenter Single Sign-On utilizzato da vRealize Orchestrator per l'autenticazione.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**
 - a Dal riquadro sinistro, selezionare **Gestione servizi**.
Viene visualizzato l'elenco dei server vRealize Orchestrator registrati.
- 2 Per registrare un nuovo server vRealize Orchestrator, fare clic su **Aggiungi**.
Viene visualizzata la finestra di dialogo **Registra vRealize Orchestrator**.
- 3 Immettere i valori seguenti.

Opzione	Descrizione
Nome	Nome dell'istanza vRealize Orchestrator registrata.
Descrizione	Descrizione dell'istanza server di vRealize Orchestrator registrata.
Nome host	Nome di dominio completo e porta del server vRealize Orchestrator. Il valore predefinito della porta HTTPS è 443. Nota VMware Cloud Director si connette all'interfaccia dell'API di vRealize Orchestrator.
Nome utente	Un account utente membro del gruppo di amministratori di vRealize Orchestrator.

Opzione	Descrizione
Password	La password dell'account amministratore di vRealize Orchestrator.
Trust Anchor	Il certificato SSL del server vRealize Orchestrator in formato PEM.
	Fare clic sull'icona di caricamento () per individuare e selezionare il file .PEM.

- 4 Fare clic su **OK** per completare la registrazione.

Il server vRealize Orchestrator è registrato con VMware Cloud Director.

Creazione di una categoria di servizi

È possibile organizzare i servizi in categorie di servizi.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**

- a Dal riquadro sinistro, selezionare **Gestione servizi**.
- b Passare alla scheda **Categorie servizi**.

Viene visualizzato un elenco delle categorie di server esistenti.

- 2 Per creare una nuova categoria di servizi, fare clic sul pulsante ().

Viene visualizzata la finestra di dialogo **Nuova categoria servizio**.

- 3 Immettere i valori seguenti.

Opzione	Descrizione
Nome	Nome della categoria di servizi.
Icona	Consente di importare l'icona da visualizzare in corrispondenza della categoria di servizi.
Descrizione	Breve descrizione della categoria di servizi.

Modifica di una categoria di servizi


È possibile modificare le categorie di servizi esistenti.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**

- a Dal riquadro sinistro, selezionare **Gestione servizi**.
- b Passare alla scheda **Categorie servizi**.

Viene visualizzato un elenco delle categorie di server esistenti.

- 2 Utilizzare la barra di elenco () a sinistra di una categoria di servizi selezionata e fare clic su **Modifica**.

3 Modificare i valori seguenti.

Opzione	Descrizione
Nome	Nome della categoria di servizi.
Icona	Consente di importare l'icona da visualizzare in corrispondenza della categoria di servizi.
Descrizione	Breve descrizione della categoria di servizi.

Importazione di un servizio

È possibile importare servizi dalla libreria dei flussi di lavoro di un'istanza di vRealize Orchestrator registrata con VMware Cloud Director.

Prerequisiti

- Registrare un'istanza di vRealize Orchestrator. Vedere [Registrazione di un'istanza di vRealize Orchestrator con VMware Cloud Director](#).
- Creare una categoria di servizi. Vedere [Creazione di una categoria di servizi](#).

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.

a Dal riquadro sinistro, selezionare **Libreria dei servizi**.

I servizi disponibili vengono elencati in una visualizzazione a schede di 12 elementi per pagina, ordinati alfabeticamente per nome. Ogni scheda indica che l'elemento è un flusso di lavoro di vRealize Orchestrator e mostra il nome del servizio e un tag che corrisponde alla categoria dei servizi in cui è stato importato il flusso di lavoro.

- 2 Per importare un nuovo servizio, fare clic sul pulsante **Importa**.
- 3 Seguire i passaggi della procedura guidata **Importa**.

Opzione	Descrizione
Importa nella libreria di destinazione	Selezionare la categoria di servizi in cui importare il servizio.
Seleziona origine	Selezionare l'istanza di vRealize Orchestrator da cui importare flussi di lavoro.
Seleziona flussi di lavoro	Espandere la visualizzazione della struttura gerarchica per selezionare uno o più flussi di lavoro da importare.
Verifica	Riesaminare i dettagli e fare clic su Fine per completare l'importazione.

I flussi di lavoro importati vengono mostrati nella visualizzazione della scheda **Libreria dei servizi**.

Ricerca di un servizio

È possibile cercare un servizio in base al suo nome o categoria di servizi a cui appartiene.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.

- a Dal riquadro sinistro, selezionare **Libreria dei servizi**.

I servizi disponibili vengono elencati in una visualizzazione a schede di 12 elementi per pagina, ordinati alfabeticamente per nome. Ogni scheda indica che l'elemento è un flusso di lavoro di vRealize Orchestrator e mostra il nome del servizio e un tag che corrisponde alla categoria dei servizi in cui è stato importato il flusso di lavoro.

- 2 Nella casella di testo di **ricerca** nella parte superiore della pagina, immettere una parola o un carattere del nome del servizio o della categoria di servizi da trovare.

- 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 flussi di lavoro di vRealize Orchestrator come servizi importati.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.

- a Dal riquadro sinistro, selezionare **Libreria dei servizi**.

I servizi disponibili vengono elencati in una visualizzazione a schede di 12 elementi per pagina, ordinati alfabeticamente per nome. Ogni scheda indica che l'elemento è un flusso di lavoro di vRealize Orchestrator e mostra il nome del servizio e un tag che corrisponde alla categoria dei servizi in cui è stato importato il flusso di lavoro.

- 2 Per eseguire un servizio, nella scheda del servizio selezionato, fare clic su **Esegui**.

Viene visualizzata la procedura guidata **Esegui un servizio**.

- 3 Compilare i parametri di input richiesti del servizio e fare clic su **Fine**.

Risultati

È possibile monitorare lo stato dell'esecuzione nella visualizzazione **Task recenti**. Per ulteriori informazioni, vedere [Visualizzazione dei task](#).

Nota Quando si avvia un flusso di lavoro di vRealize Orchestrator come servizio di VMware Cloud Director, VMware Cloud Director aggiunge alcuni parametri personalizzati al contesto di esecuzione del flusso di lavoro.

Proprietà personalizzata	Descrizione
_vcd_orgName	Nome dell'organizzazione a cui appartiene l'utente che esegue il servizio.
_vcd_orgId	ID dell'organizzazione a cui appartiene l'utente che esegue il servizio.
_vcd_userName	Nome dell'utente che esegue il servizio.
_vcd_isAdmin	Ha valore <code>True</code> se l'utente che esegue il servizio è un amministratore .
_vdc_isAdmin	Obsoleto. Ha valore <code>True</code> se l'utente che esegue il servizio è un amministratore .
_vdc_userName	Obsoleto. Nome dell'utente che esegue il servizio.
_vcd_sessionToken	Token di autenticazione ricevuto dopo l'autenticazione riuscita in VMware Cloud Director
_vcd_apiEndpoint	Endpoint dell'API REST di VMware Cloud Director

Modifica di una categoria di servizio

È possibile modificare la categoria a cui appartiene un servizio.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.
 - a Dal riquadro sinistro, selezionare **Libreria dei servizi**.
 I servizi disponibili vengono elencati in una visualizzazione a schede di 12 elementi per pagina, ordinati alfabeticamente per nome. Ogni scheda indica che l'elemento è un flusso di lavoro di vRealize Orchestrator e mostra il nome del servizio e un tag che corrisponde alla categoria dei servizi in cui è stato importato il flusso di lavoro.
- 2 Nella scheda del servizio selezionato, selezionare **Gestisci > Cambia categoria**.
 Viene aperta la finestra di dialogo **Cambia categoria**.
- 3 Selezionare la categoria in cui inserire il servizio e fare clic su **Salva**.

Annullamento della registrazione di un servizio

È possibile rimuovere l'accesso a un servizio sia per i provider dei servizi che per i tenant annullando la registrazione del servizio.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.

- a Dal riquadro sinistro, selezionare **Libreria dei servizi**.

I servizi disponibili vengono elencati in una visualizzazione a schede di 12 elementi per pagina, ordinati alfabeticamente per nome. Ogni scheda indica che l'elemento è un flusso di lavoro di vRealize Orchestrator e mostra il nome del servizio e un tag che corrisponde alla categoria dei servizi in cui è stato importato il flusso di lavoro.

- 2 Nella scheda del servizio selezionato, selezionare **Gestisci > Annulla registrazione flusso di lavoro**.

Viene visualizzata la finestra di dialogo **Annulla registrazione flusso di lavoro**.

- 3 Per rimuovere il servizio dalla libreria dei servizi, fare clic su **Elimina**.

Pubblicazione di un servizio

È possibile controllare l'accesso di provider di servizi e tenant ai servizi tramite la pubblicazione di un servizio.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.

- a Dal riquadro sinistro, selezionare **Libreria dei servizi**.

I servizi disponibili vengono elencati in una visualizzazione a schede di 12 elementi per pagina, ordinati alfabeticamente per nome. Ogni scheda indica che l'elemento è un flusso di lavoro di vRealize Orchestrator e mostra il nome del servizio e un tag che corrisponde alla categoria dei servizi in cui è stato importato il flusso di lavoro.

- 2 Nella scheda del servizio selezionato, selezionare **Gestisci > Pubblica flusso di lavoro**.

Viene visualizzata la finestra di dialogo **Pubblica flusso di lavoro**.

- 3 Per pubblicare nei provider di servizi, selezionare **Pubblica in provider di servizi** e fare clic su **Salva**.

- 4 Per pubblicare in un'organizzazione tenant specifica, selezionare il pulsante **Pubblica in tenant**.

- a Viene visualizzato un elenco con le organizzazioni tenant disponibili. Selezionare l'organizzazione di tenant in cui pubblicare il flusso di lavoro e fare clic su **Salva**.

- 5 Per pubblicare in tutte le organizzazioni di tenant, selezionare **Pubblica in tutti i tenant** e fare clic su **Salva**.

Gestione delle entità personalizzate

14

Le definizioni delle entità personalizzate in VMware Cloud Director sono tipi di oggetto associati ai tipi di oggetto vRealize Orchestrator. Quando un provider di servizi pubblica definizioni di un'entità personalizzata in un altro provider di servizi o in uno o più tenant, gli utenti VMware Cloud Director possono possedere, gestire e modificare questi tipi di in base alle proprie esigenze. Mediante l'esecuzione di servizi, gli utenti dei provider di servizi e gli utenti delle organizzazioni possono creare istanze di entità personalizzate e applicare azioni sulle istanze degli oggetti.

Questo capitolo include i seguenti argomenti:

- [Ricerca di un'entità personalizzata](#)
- [Modifica di una definizione entità personalizzata](#)
- [Aggiunta di una definizione entità personalizzata](#)
- [Istanze entità personalizzata](#)
- [Associazione di un'azione a un'entità personalizzata](#)
- [Annullamento dell'associazione di un'azione da un'entità personalizzata](#)
- [Pubblicazione di un'entità personalizzata](#)
- [Eliminazione di un'entità personalizzata](#)

Ricerca di un'entità personalizzata

È possibile cercare un'entità personalizzata in base al nome.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.
 - a Dal riquadro sinistro, 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 modificare il tipo di entità o il tipo di oggetto vRealize Orchestrator, al quale è associata l'entità. Queste sono le proprietà predefinite dell'entità personalizzata. Se si desidera modificare una delle proprietà predefinite, è necessario eliminare la definizione dell'entità personalizzata e ricrearla.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.
 - a Dal riquadro sinistro, 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**.


Si apre 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.


Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.
 - a Dal riquadro sinistro, 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 Fare clic sull'icona di  per aggiungere una nuova entità personalizzata.

Si apre una nuova finestra di dialogo.

3 Seguire i passaggi della procedura guidata **Definizione entità personalizzata**.

Passaggio	
Nome e descrizione	Immettere un nome e, facoltativamente, una descrizione 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.
Tipo	Fare clic sull'icona dell'elenco di visualizzazione () per sfogliare i tipi di oggetto 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.

Procedura

- Nella barra di navigazione superiore, selezionare **Librerie**.
 - Dal riquadro sinistro, 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.
- Nella scheda dell'entità personalizzata selezionata, fare clic su **Istanze**.
Vengono mostrate le istanze disponibili in una visualizzazione a griglia.
- 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 si avvia l'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.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.
 - a Dal riquadro sinistro, 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**.
 Si apre 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 da un'entità personalizzata

È possibile rimuovere un flusso di lavoro di vRealize Orchestrator dall'elenco delle azioni associate.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.
 - a Dal riquadro sinistro, 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**.

Si apre 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.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.

a Dal riquadro sinistro, 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**.

Si apre 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.

Procedura

- 1 Nella barra di navigazione superiore, selezionare **Librerie**.

a Dal riquadro sinistro, 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.