

vCloud Director- Mandantenportal- Handbuch

28. MÄRZ 2019

VMware Cloud Director 9.7

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2017-2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

vCloud Director-Mandantenportal-Handbuch 10

1 Erste Schritte mit dem vCloud Director-Mandantenportal 11

- Grundlegendes zu VMware vCloud Director 11
- Anmelden beim vCloud Director-Mandantenportal 13
- Rollen und Rechte für das vCloud Director-Mandantenportal 13
- Verwenden des vCloud Director-Mandantenportals 14
- Verwenden der globalen vCloud Director-Suche 15
- Anzeigen von Aufgaben 16
- Beenden einer in Bearbeitung befindlichen Aufgabe 17
- Anzeigen von Ereignissen 18

2 Arbeiten mit virtuellen Maschinen 20

- Architektur von virtuellen Maschinen 21
- Anzeigen und Bearbeiten von virtuellen Maschinen 22
- Erstellen einer neuen eigenständigen virtuellen Maschine 23
- Öffnen der Konsole einer virtuellen Maschine 24
 - Installieren von VMware Remote Console auf einem Client 24
 - Öffnen einer Remote-Konsole für die virtuelle Maschine 25
 - Öffnen einer Webkonsole 26
- Ausführen von Energievorgängen auf virtuellen Maschinen 27
 - Einschalten einer virtuellen Maschine 27
 - Ausschalten einer virtuellen Maschine 28
 - Herunterfahren eines Gastbetriebssystems 28
 - Zurücksetzen einer virtuellen Maschine 29
 - Anhalten einer virtuellen Maschine 29
 - Verwerfen des Status „Angehalten“ einer virtuellen Maschine 30
- Installieren von VMware Tools in einer virtuellen Maschine 30
- Ausführen eines Upgrades der virtuellen Hardwareversion für eine virtuelle Maschine 31
- Bearbeiten der Eigenschaften von virtuellen Maschinen 32
 - Ändern der allgemeinen Eigenschaften einer virtuellen Maschine 32
 - Ändern der Hardwareeigenschaften einer virtuellen Maschine 34
 - Ändern der Eigenschaften für die Gastbetriebssystem-Anpassung einer virtuellen Maschine 37
 - Ändern der erweiterten Eigenschaften einer virtuellen Maschine 41
- Medium einlegen 44
- Medium auswerfen 45
- Kopieren einer virtuellen Maschine in eine andere vApp 45

Verschieben einer virtuellen Maschine in eine andere vApp	46
Affinität und Anti-Affinität virtueller Maschinen	47
Anzeigen von Affinitäts- und Anti-Affinitätsregeln	48
Erstellen einer Affinitätsregel	48
Erstellen einer Anti-Affinitätsregel	49
Bearbeiten einer Affinitäts- oder Anti-Affinitätsregel	50
Löschen einer Affinitäts- oder Anti-Affinitätsregel	51
Überwachen von virtuellen Maschinen	51
Arbeiten mit Snapshots	52
Erstellen eines Snapshots einer virtuellen Maschine	53
Zurücksetzen einer virtuellen Maschine auf einen Snapshot	54
Entfernen eines Snapshots einer virtuellen Maschine	55
Verlängern des Lease einer virtuellen Maschine	55
Löschen einer virtuellen Maschine	56

3 Arbeiten mit vApps 57

Anzeigen von vApps	58
Erstellen einer neuen vApp	58
Erstellen einer vApp von einem OVF-Paket aus	60
Erstellen einer vApp aus einer vApp-Vorlage	62
Öffnen einer vApp	64
Ausführen von Energievorgängen auf vApps	65
Einschalten einer vApp	65
Ausschalten einer vApp	65
Beenden einer vApp	66
Zurücksetzen einer vApp	66
Anhalten einer vApp	67
Verwerfen des Zustands „Angehalten“ einer vApp	67
vApp-Eigenschaften bearbeiten	68
Bearbeiten der allgemeinen Eigenschaften der vApp	68
Bearbeiten der erweiterten vApp-Eigenschaften	69
Freigeben einer vApp	70
Anzeigen eines vApp-Netzwerkdiagramms	71
Arbeiten mit Netzwerken in einer vApp	72
Anzeigen von vApp-Netzwerken	73
Fencing eines vApp-Netzwerks	73
Hinzufügen eines Netzwerks zu einer vApp	74
Konfigurieren von Netzwerkdiensten für ein vApp-Netzwerk	75
Löschen eines vApp-Netzwerks	80
Arbeiten mit Snapshots	81
Erstellen eines Snapshots einer vApp	81

Zurücksetzen einer vApp auf einen Snapshot	82
Entfernen eines Snapshots einer vApp	83
Ändern des Besitzers einer vApp	83
Verschieben einer vApp in ein anderes virtuelles Datacenter	84
Kopieren einer beendeten vApp in ein anderes virtuelles Datacenter	85
Kopieren einer eingeschalteten vApp	85
Hinzufügen einer virtuellen Maschine zu einer vApp	86
Speichern einer vApp als vApp-Vorlage in einem Katalog	87
Herunterladen einer vApp als OVF-Paket	89
Verlängern eines vApp-Lease	89
Löschen einer vApp	90

4 Verwalten von VDC-Organisationsnetzwerken 91

Anzeigen der verfügbaren VDC-Organisationsnetzwerke	93
Hinzufügen eines isolierten VDC-Organisationsnetzwerks	94
Hinzufügen eines VDC-Organisationsnetzwerks mit Routing	95
Hinzufügen eines direkten VDC-Organisationsnetzwerks	98
Bearbeiten der allgemeinen Einstellungen eines VDC-Organisationsnetzwerks	98
Konvertieren eines VDC-Organisationsnetzwerks	99
Konvertieren der Schnittstelle eines VDC-Organisationsnetzwerks mit Routing	100
Anzeigen der für ein VDC-Organisationsnetzwerk verwendeten IP-Adressen	101
Hinzufügen von IP-Adressen zum IP-Pool eines VDC-Organisationsnetzwerks	102
Bearbeiten oder Entfernen von IP-Bereichen, die in einem VDC-Organisationsnetzwerk verwendet werden	102
Bearbeiten der DNS-Einstellungen eines VDC-Organisationsnetzwerks	103
Konfigurieren von DHCP-Einstellungen für ein isoliertes VDC-Organisationsnetzwerk	104
Bearbeiten oder Löschen eines vorhandenen DHCP-Pools für ein Netzwerk	105
Zurücksetzen eines VDC-Organisationsnetzwerks	106
Löschen eines VDC-Organisationsnetzwerks	106

5 Verwalten von VDC-übergreifenden Netzwerken 107

Verwalten von Datacenter-Gruppen	108
Erstellen und Konfigurieren einer Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration	108
Erstellen und Konfigurieren einer Datacenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration	111
Anzeigen einer Datacenter-Gruppe	113
Hinzufügen eines virtuellen Datacenters zu einer Datacenter-Gruppe	114
Entfernen eines virtuellen Datacenters aus einer Datacenter-Gruppe	115
Synchronisieren einer Datacenter-Gruppe	115
Tauschen der Egress-Punkte in einer Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration	116
Ersetzen des Edge-Gateway eines Egress-Punkts	117

Entfernen eines Egress-Punkts	118
Synchronisieren von Routen und Egress-Punkten	118
Verwalten von ausgeweiteten Netzwerken	119
Hinzufügen eines ausgeweiteten Netzwerks	120
Anzeigen oder Bearbeiten eines ausgeweiteten Netzwerks	121
Löschen eines ausgeweiteten Netzwerks	122
Synchronisieren eines ausgeweiteten-Netzwerks	122

6 Erweiterte Netzwerkfunktionen für vCloud Director-Mandanten 124

Erste Schritte mit erweiterten vCloud Director-Netzwerken	125
Firewallkonfiguration über das Mandantenportal	126
Edge-Gateway-Firewall	127
Verwalten einer Edge-Gateway-Firewall	127
Distributed Firewall	132
Aktivieren der Distributed Firewall in einem Organisations-VDC mithilfe des Mandantenportals	133
Verwalten der Distributed Firewall-Regeln mithilfe des Mandantenportals	134
Verwalten des DHCP-Protokolls für Edge-Gateways	139
Hinzufügen eines DHCP-IP-Pools	139
Hinzufügen von DHCP-Bindungen	141
Konfigurieren von DHCP-Relay für Edge-Gateways	142
Angabe einer DHCP-Relay-Konfiguration für ein Edge-Gateway	143
Verwalten der Netzwerkadressübersetzung mithilfe des Mandantenportals	144
Hinzufügen einer SNAT- oder DNAT-Regel	145
Konfiguration für erweitertes Routing	148
Angabe von Standard-Routing-Konfigurationen für das Edge-Gateway	149
Hinzufügen einer statischen Route	150
Konfigurieren des OSPF-Protokolls	151
Konfigurieren des BGP-Protokolls	155
Konfigurieren der Route Redistribution	157
Lastausgleich	158
Lastausgleich	159
Sicherer Zugriff mit virtuellen privaten Netzwerken	173
Konfigurieren von SSL VPN-Plus	174
Konfigurieren von IPsec-VPN	189
L2 VPN konfigurieren	196
Entfernen der L2 VPN-Dienstkonfiguration von einem Edge-Gateway	201
SSL-Zertifikatsverwaltung	202
Generieren einer Zertifikatsignieranforderung für ein Edge-Gateway	203
Importieren des von der Zertifizierungsstelle signierten Zertifikats, das der für ein Edge-Gateway generierten CSR entspricht	204
Konfigurieren eines selbstsignierten Dienstzertifikats	205

Hinzufügen eines CA-Zertifikats zum Edge-Gateway für die Überprüfung der Vertrauenswürdigkeit von SSL-Zertifikaten	206
Hinzufügen einer Zertifikatswiderrufsliste zu einem Edge-Gateway	208
Hinzufügen eines Dienstzertifikats zum Edge-Gateway	209
Benutzerdefiniertes Gruppieren von Objekten	210
Erstellen eines IP Sets zur Verwendung in Firewallregeln und bei der DHCP-Relay-Konfiguration	210
Erstellen eines MAC Sets für die Verwendung in Firewallregeln	211
Anzeigen der für Firewallregeln verfügbaren Dienste	212
Anzeigen der für Firewallregeln verfügbaren Dienstgruppen	212
Statistiken und Protokolle für ein Edge-Gateway	213
Anzeigen von Statistiken	213
Protokollierung aktivieren	214
Aktivieren des SSH-Befehlszeilenzugriffs auf ein Edge-Gateway	215
Arbeiten mit Sicherheitstags	216
Erstellen und Zuweisen von Sicherheitstags	216
Ändern der Zuweisung von Sicherheitstags	217
Anzeigen von angewendeten Sicherheitstags	218
Bearbeiten eines Sicherheits-Tags	219
Löschen eines Sicherheitstags	220
Arbeiten mit Sicherheitsgruppen	221
Erstellen einer Sicherheitsgruppe	221
Bearbeiten einer Sicherheitsgruppe	222
Löschen einer Sicherheitsgruppe	224
7 Verwendung unabhängiger Festplatten und Überprüfen von Speicherrichtlinien	226
Erstellen und Verwenden von unabhängigen Festplatten	226
Erstellen einer unabhängigen Festplatte	226
Bearbeiten einer unabhängigen Festplatte	227
Löschen einer unabhängigen Festplatte	227
Überprüfen der Eigenschaften von Speicherrichtlinien	228
8 Überprüfen der Eigenschaften von virtuellen Datencentern	229
Überprüfen der Eigenschaften von virtuellen Datencentern	229
Überprüfen der Metadaten des virtuellen Datencenters	229
9 Arbeiten mit SDDCs und SDDC-Proxys	231
Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen	231
Aktivieren oder Deaktivieren eines SDDC-Proxys	232
Anmelden bei der Benutzeroberfläche einer Proxy-SDDC-Komponente	233

10 Arbeiten mit vApp-Vorlagen 235

- Anzeigen einer vApp-Vorlage 235
- vApp-Vorlage aus einer OVF-Datei erstellen 236
- vApp-Vorlage herunterladen 237
- Löschen einer vApp-Vorlage 238

11 Arbeiten mit Mediendateien 239

- Hochladen von Mediendateien 239
- Löschen einer Mediendatei 240
- Herunterladen einer Mediendatei 240

12 Arbeiten mit Katalogen 242

- Anzeigen von Katalogen 243
- Erstellen eines Katalogs 243
- Freigeben eines Katalogs 244
- Löschen eines Katalogs 245
- Verwalten von Metadaten für einen Katalog 246
- Veröffentlichen eines Katalogs 246
- Abonnieren eines externen Katalogs 247
- Aktualisieren der Speicherort-URL und des Kennworts für einen abonnierten Katalog 248
- Synchronisieren eines abonnierten Katalogs 248

13 Arbeiten mit VDC-Organisationsvorlagen 250

- Anzeigen verfügbarer Vorlagen für virtuelle Datacenter 250
- Erstellen eines virtuellen Datacenters aus einer Vorlage 251

14 Verwalten von Benutzern, Gruppen und Rollen 252

- Verwalten von Benutzern 252
 - Erstellen eines Benutzers 252
 - Benutzer importieren 254
 - Ändern eines Benutzers 255
 - Deaktivieren oder Aktivieren eines Benutzerkontos 256
 - Löschen eines Benutzers 256
 - Entsperren eines gesperrten Benutzerkontos 257
- Verwalten von Gruppen 257
 - Importieren einer Gruppe 257
 - Löschen einer Gruppe 258
 - Bearbeiten einer Gruppe 259
- Rollen und Rechte 259
 - Vordefinierte Rollen und ihre Rechte 260
 - Erstellen einer benutzerdefinierten Mandantenrolle 269

Bearbeiten einer benutzerdefinierten Mandantenrolle 270

Löschen einer Rolle 270

15 Aktivieren der Verwendung eines SAML-Identitätsanbieter für die Organisation 272

16 Verwalten Ihrer Organisation 275

Bearbeiten des Namens und der Beschreibung der Organisation 275

Ändern der E-Mail-Einstellungen 276

Testen der SMTP-Einstellungen 277

Ändern der Domäneneinstellungen für die virtuellen Maschinen in Ihrer Organisation 278

Arbeiten mit mehreren Sites 278

Konfigurieren und Verwalten von Multisite-Bereitstellungen 278

Wissenswertes über Leases 280

Ändern der Richtlinien für vApp- und vApp-Vorlage-Leases innerhalb der Organisation 280

Ändern der Standardkontingente für die virtuellen Maschinen in Ihrer Organisation 281

Ändern des Kennworts und der Richtlinien für Benutzerkonten in Ihrer Organisation 282

17 Arbeiten mit der Dienstbibliothek 283

Auffinden eines Diensts 283

Ausführen eines Diensts 284

18 Arbeiten mit benutzerdefinierten Entitätsdefinitionen 285

Auffinden einer benutzerdefinierten Entität 285

Bearbeiten einer benutzerdefinierten Entitätsdefinition 286

Hinzufügen einer benutzerdefinierten Entitätsdefinition 287

Benutzerdefinierte Entitätsinstanzen 288

Verknüpfen einer Aktion mit einer benutzerdefinierten Entität 288

Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entitätsdefinition 289

Veröffentlichen einer benutzerdefinierten Entität 290

Löschen einer benutzerdefinierten Entität 291

vCloud Director-Mandantenportal-Handbuch

Das *VMware vCloud Director-Mandantenportal-Handbuch* enthält Informationen zur Verwendung des VMware vCloud Director-Mandantenportals. In dieser Version verwenden Sie das Mandantenportal zum Verwalten von Organisationen, Erstellen und Konfigurieren virtueller Maschinen, vApps und Netzwerke innerhalb von vApps. Außerdem haben Sie die Möglichkeit, erweiterte Netzwerkfunktionen zu konfigurieren, die von VMware NSX[®] for vSphere[®] innerhalb einer vCloud Director-Umgebung bereitgestellt werden. Mit dem vCloud Director-Mandantenportal können Sie auch Kataloge, vApp- und VDC-Vorlagen sowie VDC-übergreifende Netzwerke erstellen und verwalten.

Zielgruppe

Dieses Handbuch richtet sich an alle Anwender, die die Funktionen des vCloud Director-Mandantenportals verwenden möchten. Die Informationen wurden in erster Linie für **Organisationsadministratoren** verfasst, die im Mandantenportal ihre Organisation sowie virtuelle Maschinen, vApps, Netzwerke usw. verwalten.

Verwandte Dokumentation

Weitere Informationen zu den Funktionen, die einem Organisationsadministrator bei Verwendung der vCloud Director-Webkonsole anstelle des vCloud Director-Mandantenportals zur Verfügung stehen, finden Sie im *vCloud Director-Benutzerhandbuch*.

VMware Technical Publications – Glossar

VMware Technical Publications stellt Ihnen ein Glossar mit Begriffen zur Verfügung, mit denen Sie möglicherweise nicht vertraut sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter <http://www.vmware.com/support/pubs>.

Erste Schritte mit dem vCloud Director-Mandantenportal

1

Wenn Sie sich beim Mandantenportal anmelden, können Sie eine Reihe von Aufgaben ausführen, wie z. B. virtuelle Maschinen und vApps erstellen, erweiterte Netzwerkkonfigurationen einrichten und vRealize Orchestrator-Workflows ausführen.

Dieses Kapitel enthält die folgenden Themen:

- Grundlegendes zu VMware vCloud Director
- Anmelden beim vCloud Director-Mandantenportal
- Rollen und Rechte für das vCloud Director-Mandantenportal
- Verwenden des vCloud Director-Mandantenportals
- Verwenden der globalen vCloud Director-Suche
- Anzeigen von Aufgaben
- Beenden einer in Bearbeitung befindlichen Aufgabe
- Anzeigen von Ereignissen

Grundlegendes zu VMware vCloud Director

VMware vCloud Director bietet rollenbasierten Zugriff auf ein webbasiertes Mandantenportal, das Mitgliedern einer Organisation gestattet, mit den Ressourcen der Organisation zu interagieren, um vApps und virtuelle Maschinen zu erstellen und mit ihnen zu arbeiten.

Bevor Sie auf Ihre Organisation zugreifen können, muss ein vCloud Director-**Systemadministrator** die Organisation erstellen, ihr Ressourcen zuweisen und die URL für den Zugriff auf das Mandantenportal bereitstellen. Jede Organisation hat einen oder mehrere **Organisationsadministratoren**, die das Einrichten der Organisation durch Hinzufügen von Mitgliedern und Festlegen von Richtlinien und Einstellungen abschließen. Nach dem Einrichten einer Organisation können Benutzer, die keine Administratoren sind, sich bei ihr anmelden, um virtuelle Maschinen und vApps zu erstellen, zu verwenden und zu verwalten.

Organisationen

Eine Organisation ist eine Verwaltungseinheit für eine Sammlung von Benutzern, Gruppen und Rechenressourcen. Benutzer authentifizieren sich auf der Ebene von Organisationen mit den Anmeldeinformationen, die vom **Organisationsadministrator** beim Erstellen oder Importieren des Benutzers angelegt wurden. **Systemadministratoren** erstellen Organisationen und stellen sie bereit, während **Organisationsadministratoren** Benutzer, Gruppen und Kataloge der Organisation verwalten.

Benutzer und Gruppen

Organisationen können über eine beliebige Anzahl an Benutzern und Gruppen verfügen. Benutzer können lokal vom Organisationsadministrator erstellt oder aus einem Verzeichnisdienst importiert werden. Gruppen müssen jedoch aus dem Verzeichnisdienst importiert werden. Die Berechtigungen innerhalb einer Organisation werden durch Zuweisung von Rechten und Rollen zu Benutzern und Gruppen gesteuert.

Virtuelle Datencenter

Ein Organisations-VDC stellt Ressourcen für eine Organisation bereit. Virtuelle Datencenter stellen eine Umgebung bereit, in der virtuelle Systeme gespeichert, bereitgestellt und betrieben werden können. Sie stellen außerdem Speicher für virtuelle CD- und DVD-Medien bereit. Eine Organisation kann mehrere virtuelle Datencenter aufweisen.

VDC-Organisationsnetzwerke

Ein VDC-Organisationsnetzwerk ist ein Bestandteil eines vCloud Director-Organisations-VDCs. Es steht allen vApps in der Organisation zur Verfügung. VDC-Organisationsnetzwerke ermöglichen es vApps, Daten innerhalb einer Organisation miteinander auszutauschen. Ein VDC-Organisationsnetzwerk kann mit einem externen Netzwerk verbunden sein oder isoliert und intern auf die Organisation beschränkt werden. Nur **Systemadministratoren** können VDC-Organisationsnetzwerke erstellen. **Organisationsadministratoren** hingegen können VDC-Organisationsnetzwerke verwalten, einschließlich der von ihnen bereitgestellten Netzwerkdienste.

vApp-Netzwerke

vApp-Netzwerke sind Bestandteile von vApps und ermöglichen es virtuellen Maschinen in der vApp, Daten miteinander auszutauschen. Sie können ein vApp-Netzwerk mit einem VDC-Organisationsnetzwerk verbinden, damit die vApp Daten mit den anderen vApps in der Organisation und sogar außerhalb der Organisation austauschen kann, sofern das VDC-Organisationsnetzwerk mit einem externen Netzwerk verbunden ist.

Kataloge

Organisationen verwenden Kataloge, um vApp-Vorlagen und Mediendateien zu speichern. Die Mitglieder einer Organisation mit Zugriff auf einen Katalog können die vApp-Vorlagen und Mediendateien des Katalogs zum Erstellen eigener vApps verwenden.

Organisationsadministratoren können Objekte aus öffentlichen Katalogen in ihren Organisationskatalog kopieren.

SDDCs und SDDC-Proxys

Ein Software-Defined Data Center (SDDC) kapselt eine gesamte vCenter Server-Umgebung. Ein SDDC kann einen oder mehrere SDDC-Proxys enthalten, die Zugriff auf verschiedene Komponenten aus der zugrunde liegenden Umgebung bieten. Der **Systemadministrator** kann ein oder mehrere SDDCs in Ihrer Organisation veröffentlichen. Sie können die enthaltenen SDDC-Proxys verwenden, um auf die Benutzeroberfläche oder die API der Proxy-Komponenten zuzugreifen.

Anmelden beim vCloud Director-Mandantenportal

Sie können auf das vCloud Director-Mandantenportal mithilfe einer für Ihre Organisation spezifischen URL zugreifen.

Wenden Sie sich an den **Organisationsadministrator**, wenn Sie die Organisations-URL des Mandantenportals nicht kennen. Weitere Informationen zu unterstützten Browsern und Konfigurationen finden Sie unter *vCloud Director-Versionshinweise*.

Verfahren

- 1 Navigieren Sie in einem Webbrowser zur URL des Mandantenportals Ihrer Organisation.
Beispiel: *https://vcloud.example.com/tenant/myOrg*.
- 2 Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie auf **Anmelden**.

Rollen und Rechte für das vCloud Director-Mandantenportal

vCloud Director enthält einen vorkonfigurierten Satz an Benutzerrollen und deren Rechte. Die Rollen für den Zugriff auf das vCloud Director-Mandantenportal sind die Rollen, die standardmäßig in jeder Organisation erstellt werden, oder andere Rollen, die vom Organisationsadministrator erstellt werden.

Benutzer, denen die folgenden Organisationsrollen zugewiesen sind, können auf das Mandantenportal zugreifen. Die angezeigten Objekte und die durchführbaren Aktionen hängen von den Rechten ab, die mit einer bestimmten Rolle verbunden sind.

- **Organisationsadministrator**
- **Katalogautor**
- **vApp-Autor**

- **vApp-Benutzer**
- **Nur Konsolenzugriff**

Weitere Informationen zu den vordefinierten Rollen und den jeweiligen Rechten erhalten Sie unter [Vordefinierte Rollen und ihre Rechte](#).

Verwenden des vCloud Director-Mandantenportals

Wenn Sie über mehrere virtuelle Datacenter verfügen, werden Sie zum Dashboard-Bildschirm **Virtuelle Datacenter** geleitet, sobald Sie sich beim vCloud Director-Mandantenportal anmelden. Wenn Sie über nur ein virtuelles Datacenter verfügen, werden Sie bei der Anmeldung beim Mandantenportal von vCloud Director direkt an das Datacenter weitergeleitet.

Der Dashboard-Bildschirm **Virtuelle Datacenter** ist Teil der Multisite-Funktion von vCloud Director, die es Mandanten ermöglicht, ihre geografisch verteilte Cloud-Umgebung als eine einzelne Einheit anzuzeigen. Weitere Multisite-Informationen finden Sie unter [Arbeiten mit mehreren Sites](#).

Das Dashboard ist eine einheitliche Ansicht der vCloud Director-VDCs und -Sites nicht nur in einer einzelnen Organisation. In einer Umgebung mit mehreren Zellen und mehreren Organisationen können Sie auch die virtuellen Datacenter für alle anderen zugehörigen Organisationen einsehen.

Hinweis Abhängig von ihren Rechten können Mandantenbenutzer alle Mitgliedssites einer Organisation oder nur eine Teilmenge der Sites anzeigen.

Die Informationen zur Organisation werden ganz oben im Übersichtsmenüband angezeigt.



Wenn Sie sich als **Organisationsadministrator** anmelden, können Sie Folgendes sehen:

- Die Anzahl der Sites, Organisationen und virtuellen Datacenter
- Die Gesamtzahl der ausgeführten vApps und virtuellen Maschinen
- Verwendete Hardwareressourcen, wie z. B. CPU, Arbeitsspeicher und Speicher

Die virtuellen Datacenter werden in einer Kartenansicht angezeigt. Jede Karte enthält Informationen zu der Organisation, zu der das Datacenter gehört, zur Anzahl der vApps, zur Gesamtzahl der virtuellen Maschinen und zur Anzahl der virtuellen Maschinen, die aktuell ausgeführt werden. Auf der Karte werden auch die verfügbaren Prozessor-, Arbeitsspeicher- und Speicherressourcen für das Datacenter sowie Echtzeitmetriken über die aktuellen Zuteilungen und Reservierungen von Ressourcen angezeigt.

Im Hauptmenü () können Sie zu den verschiedenen Menüelementen navigieren.

Menüelement	Beschreibung
Datencenter	Leitet Sie zum Bildschirm Virtuelle Datencenter , in dem die virtuellen Datencenter innerhalb der Organisation angezeigt werden.
Datencenter-Gruppen	Führt zum Bildschirm für die Datencenter-Gruppen zum Verwalten von VDC-übergreifenden Netzwerken. Standardmäßig kann nur der Systemadministrator dieses Menüelement anzeigen.
Bibliotheken	Leitet Sie zu einer konsolidierten Ansicht für vApp-Vorlagen, Kataloge, Medien und andere Arten von Dateien. Sie verwenden diese Vorlagen und Dateien, um virtuelle Maschinen oder vApps bereitzustellen.
Administration	Leitet Sie zum Multisite-Verwaltungsbildschirm, in dem Organisationsadministratoren eine Vertrauensstellung mit einer anderen Organisation herstellen können.
Aufgaben	Leitet Sie zum Fenster Aufgaben , in dem die von vCloud Director gemeldeten Aufgaben angezeigt werden.
Ereignisse	Leitet Sie zum Fenster Ereignisse , in dem die von vCloud Director gemeldeten Ereignisse angezeigt werden.
Betriebe	Leitet Sie zum Bildschirm Dienstbibliothek . Die Dienstbibliothek enthält Gruppen von vCloud Director-Komponenten, für die Sie vRealize Orchestrator-Workflows ausführen können.

Sie können Ihr vCloud Director-Mandantenportal mithilfe der *Branding* vCloud OpenAPIs anpassen. Informationen über die Verwendung der vCloud OpenAPI finden Sie im Dokument *Erste Schritte mit vCloud OpenAPI* unter <https://code.vmware.com>.

Verwenden der globalen vCloud Director-Suche

Mithilfe der globalen vCloud Director-Suche können Sie eine Suche nach einem Namen oder einem Teil eines Namens in den Namen der Objekte in Ihrer Umgebung durchführen. Sie können auch nach einer virtuellen Maschine anhand ihrer IP-Adresse suchen, wenn die IP-Adresse der virtuellen Maschine statisch ist.



Die Liste der voreingestellten Objekte lautet:

- Datencenter
- vApp-Vorlagen
- vApps
- Virtuelle Maschinen
- vApp-Netzwerke
- Kataloge

Wenn eine virtuelle Maschine eine über DHCP zugewiesene IP-Adresse verwendet, gibt die Suche deren IP-Adresse nicht zurück. Wenn Sie nach einer virtuellen Maschine suchen möchten, die über eine per DHCP zugewiesene IP-Adresse verfügt, müssen Sie nach Name suchen.

Standardmäßig können Sie nur innerhalb der Objekte in Ihrer lokalen Site suchen. Wenn Sie über eine Multisite-Umgebung verfügen, können Sie mehrere Sites durchsuchen.

Verfahren

- 1 Klicken Sie in der oberen rechten Ecke des vCloud Director-Mandantenportals auf das Symbol **Suchen** ().
- 2 (Optional) Fixieren Sie den Suchbereich, indem Sie auf das Stecknadelsymbol () klicken.
- 3 Geben Sie im Textfeld **Suche** ein Symbol, einen Teil eines Namens oder eine IP-Adresse ein, anhand dessen bzw. anhand derer nach übereinstimmenden Objektnamen oder statischen IP-Adressen von virtuellen Maschinen gesucht werden soll.
- 4 Wenn Sie eine Multisite-Umgebung nutzen, wählen Sie die Sites aus, in denen Sie die Suche durchführen möchten.
- 5 Drücken Sie die **Eingabetaste**.

Ergebnisse

Die fünf am besten passenden Ergebnisse pro Objekttyp werden angezeigt. Die Ergebnisse werden alphabetisch sortiert.

Nächste Schritte

- Um ggf. weitere Ergebnisse anzuzeigen, klicken Sie unter jedem Objekttyp auf **Weitere laden**.
- Um weitere Informationen zu einem bestimmten Objekt aus den Suchergebnissen anzuzeigen, zeigen Sie auf das Objekt.
- Um ein bestimmtes Objekt zu verwalten, z. B. um die Einstellungen eines Objekts anzuzeigen oder zu ändern, klicken Sie auf das Objekt. Die Details zum Objekt werden auf der linken Seite angezeigt.


Anzeigen von Aufgaben

Über das Mandantenportal können Sie die Liste der letzten Aufgaben sowie deren Details und Status anzeigen. Darüber hinaus können Sie auch die Liste aller Aufgaben anzeigen.


Der Fensterbereich **Letzte Aufgaben** wird standardmäßig am unteren Rand des Mandantenportals angezeigt. Er enthält eine Liste der Aufgaben, die vor kurzem ausgeführt wurden. Wenn Sie einen Vorgang starten (z. B. Erstellen einer virtuellen Maschine), wird die Aufgabe in diesem Bereich angezeigt. Falls Sie den Fensterbereich **Letzte Aufgaben** minimieren, wird weiterhin die Anzahl der laufenden oder fehlgeschlagenen letzten Aufgaben angezeigt. Sie können den Fensterbereich **Letzte Aufgaben** stets wieder öffnen, indem Sie auf die Doppelpfeile klicken.

Die Aufgabenansicht enthält alle Aufgaben und zeigt an, wenn Aufgaben ausgeführt wurden und ob sie erfolgreich abgeschlossen wurden. Bei dieser Ansicht handelt es sich um den ersten Schritt zur Behebung von Problemen in Ihrer Umgebung. In der Aufgabenansicht werden Vorgänge mit langer Ausführungsdauer angezeigt, z. B. die Erstellung von virtuellen Maschinen oder vApps.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Aufgaben** aus oder klicken Sie im Fensterbereich **Letzte Aufgaben** auf **Weitere Aufgaben**.

Die Liste aller Aufgaben wird angezeigt, zusammen mit dem Zeitpunkt, zu dem die Aufgabe ausgeführt wurde, und dem Status der Aufgabe.

- 2 Klicken Sie auf das Editor-Symbol () , um die Details zu ändern, die Sie zu den Aufgaben anzeigen möchten.

- 3 (Optional) Um die Details der Aufgabe anzuzeigen, klicken Sie auf den Namen der Aufgabe.

Zu den Aufgabendetails zählen beispielsweise Informationen wie der Grund für den Fehler, wenn die Aufgabe fehlgeschlagen ist.

Detail	Beschreibung
Vorgang	Der Name des durchgeführten Vorgangs
Auftrag-ID	Die ID der Aufgabe
Typ	Das Objekt, für das die Aufgabe durchgeführt wurde. Wenn Sie eine virtuelle Maschine erstellt haben, ist der Typ z. B. <code>vm</code> .
Organisation	Der Name der Organisation
Status	Der Status der Aufgabe, z. B. „Erfolgreich“, „Wird ausgeführt“ oder „Fehlgeschlagen“
Initiator	Der Benutzer, der den Vorgang gestartet hat
Startzeit	Datum und Uhrzeit, wann der Vorgang gestartet wurde
Fertigstellungszeit	Datum und Uhrzeit, wann der Vorgang erfolgreich abgeschlossen wurde oder fehlgeschlagen ist
Dienst-Namespace	Der Dienstname, z. B. <code>com.vmware.vcloud</code>
Details	Der Grund für das Fehlschlagen der Aufgabe. Wenn Sie beispielsweise versuchen, einen Snapshot einer virtuellen Maschine zu erstellen, und der Vorgang fehlschlägt, da nicht ausreichend Speicher vorhanden ist, werden Aufgabendetails ähnlich den folgenden angezeigt: Der angeforderte Vorgang überschreitet das Speicherkontingent von VDC: für die Speicherrichtlinie „*“ verbleiben 8.693 MB, angefordert wurden 41.472 MB.

Beenden einer in Bearbeitung befindlichen Aufgabe


Falls Sie versehentlich einen Vorgang starten, bevor Sie alle erforderlichen Einstellungen angewendet oder überprüft haben, können Sie die laufende Aufgabe beenden.

Der Bereich **Letzte Aufgaben** wird standardmäßig am unteren Rand des Portals angezeigt. Wenn Sie einen Vorgang starten (z. B. Erstellen einer virtuellen Maschine), wird die Aufgabe in diesem Bereich angezeigt.

Voraussetzungen

Der Bereich **Letzte Aufgaben** muss geöffnet sein.

Verfahren

- 1 Starten Sie einen Vorgang mit langer Ausführungszeit.
Vorgänge mit langer Ausführungszeit sind beispielsweise das Erstellen einer virtuellen Maschine oder einer vApp oder für virtuelle Maschinen und vApps durchgeführte Energievorgänge.
- 2 Klicken Sie im Bereich **Letzte Aufgaben** auf das Symbol **Abbrechen** () .
- 3 Bestätigen Sie im Dialogfeld **Aufgabe abbrechen**, dass Sie die Aufgabe abbrechen möchten, indem Sie auf **OK** klicken.

Ergebnisse



Der Vorgang wird beendet.

Anzeigen von Ereignissen

Über das Portal können Sie die Liste aller Ereignisse, die zugehörigen Details und den Status anzeigen.

Die Ereignisansicht bietet eine Möglichkeit, den Status der Ereignisse in Ihrem Portal anzuzeigen. In der Ansicht wird angezeigt, wann die Ereignisse aufgetreten sind und ob die Ausführung erfolgreich war. Die Ereignisansicht enthält einmalige Vorkommen, wie beispielsweise Benutzeranmeldungen und Objekterstellungs- oder -löschvorgänge.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Ereignisse** aus.
Die Liste aller Ereignisse wird angezeigt, sowie die Zeit, zu der das Ereignis aufgetreten ist, und der Status des Ereignisses.
- 2 Klicken Sie auf das Editor-Symbol () , um die Details zu ändern, die Sie zu den Ereignissen anzeigen möchten.
- 3 (Optional) Klicken Sie auf ein Ereignis, um die Ereignisdetails anzuzeigen.

Detail	Beschreibung
Ereignis	Der Name des Ereignisses Wenn Sie beispielsweise eine vApp ändern, um virtuelle Maschinen darin einzuschließen, ist das Ereignis, das den gesamten Vorgang startet, <i>Aufgabe „vApp ändern“ starten</i> .
Ereignis-ID	Die ID der Aufgabe
Typ	Das Objekt, für das die Aufgabe durchgeführt wurde. Wenn Sie eine virtuelle Maschine erstellt haben, ist der Typ z. B. <i>vm</i> .
Ziel	Das Zielobjekt des Ereignisses Wenn Sie beispielsweise eine vApp ändern, um virtuelle Maschinen darin einzuschließen, ist das Ziel des Ereignisses <i>Aufgabe „vApp ändern“ startenvdcUpdateVapp</i> .

Detail	Beschreibung
Status	Der Status des Ereignisses, z. B. „Erfolgreich“ oder „Fehlgeschlagen“
Dienst-Namespace	Der Dienstname, z. B. <i>com.vmware.vcloud</i>
Organisation	Der Name der Organisation
Besitzer	Der Benutzer, der das Ereignis ausgelöst hat
Zeitpunkt des Auftretens	Datum und Uhrzeit, wann das Ereignis aufgetreten ist

Arbeiten mit virtuellen Maschinen

2

Eine virtuelle Maschine ist ein Softwarecomputer, auf dem ein Betriebssystem und Anwendungen wie auf einem physischen Computer ausgeführt werden. Diese virtuelle Maschine besteht aus mehreren Spezifikations- und Konfigurationsdateien und wird von den physischen Ressourcen eines Hosts gesichert. Jede virtuelle Maschine verfügt über virtuelle Geräte, die dieselbe Funktionalität wie physische Hardware bereitstellen, aber portierbarer, sicherer und leichter zu verwalten sind.

Zusätzlich zu den verschiedenen Vorgängen, die Sie auf einem physischen Computer ausführen können, unterstützen vCloud Director-VMs auch Vorgänge an der virtuellen Infrastruktur, wie z. B. das Erstellen eines Snapshots des VM-Zustands und das Verschieben einer virtuellen Maschine von einem Host auf einen anderen.

Ab vCloud Director 9.5 unterstützen virtuelle Maschinen IPv6-Konnektivität. Sie können IPv6-Adressen virtuellen Maschinen zuweisen, die mit IPv6-Netzwerken verbunden sind.

Wichtig Alle Schritte für das Arbeiten mit virtuellen Maschinen werden in der Kartenansicht dokumentiert, wobei davon ausgegangen wird, dass Sie über mehrere Datacenter verfügen. Es ist auch möglich, die gleichen Verfahren über die Rasteransicht durchzuführen. Die Schritte können jedoch geringfügig variieren.

Dieses Kapitel enthält die folgenden Themen:

- [Architektur von virtuellen Maschinen](#)
- [Anzeigen und Bearbeiten von virtuellen Maschinen](#)
- [Erstellen einer neuen eigenständigen virtuellen Maschine](#)
- [Öffnen der Konsole einer virtuellen Maschine](#)
- [Ausführen von Energievorgängen auf virtuellen Maschinen](#)
- [Installieren von VMware Tools in einer virtuellen Maschine](#)
- [Ausführen eines Upgrades der virtuellen Hardwareversion für eine virtuelle Maschine](#)
- [Bearbeiten der Eigenschaften von virtuellen Maschinen](#)
- [Medium einlegen](#)
- [Medium auswerfen](#)

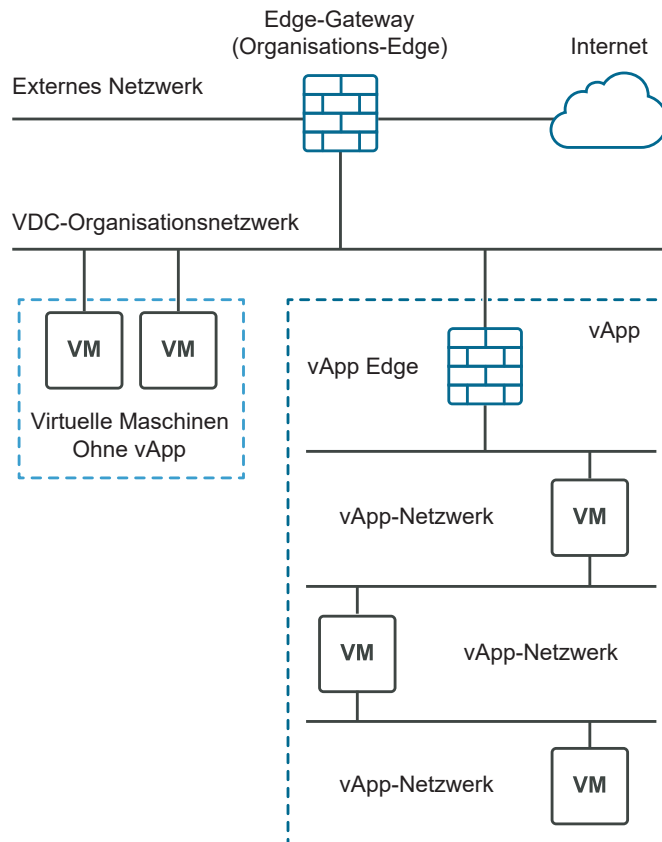
- [Kopieren einer virtuellen Maschine in eine andere vApp](#)
- [Verschieben einer virtuellen Maschine in eine andere vApp](#)
- [Affinität und Anti-Affinität virtueller Maschinen](#)
- [Überwachen von virtuellen Maschinen](#)
- [Arbeiten mit Snapshots](#)
- [Verlängern des Lease einer virtuellen Maschine](#)
- [Löschen einer virtuellen Maschine](#)

Architektur von virtuellen Maschinen

Eine virtuelle Maschine kann als eigenständige Maschine oder innerhalb einer vApp existieren.

Eine virtuelle Maschine ist ein Softwarecomputer, auf dem ein Betriebssystem und Anwendungen wie auf einem physischen Computer ausgeführt werden. Diese virtuelle Maschine besteht aus mehreren Spezifikations- und Konfigurationsdateien und wird von den physischen Ressourcen eines Hosts gesichert. Jede virtuelle Maschine verfügt über virtuelle Geräte, die dieselbe Funktionalität wie physische Hardware bereitstellen, aber portierbarer, sicherer und leichter zu verwalten sind. Virtuelle Maschinen können eigenständig sein oder innerhalb einer vApp existieren. Eine vApp ist ein Verbundobjekt, das aus einer oder mehreren virtuellen Maschinen und einem oder mehreren Netzwerken besteht.




Die folgende Abbildung zeigt die verschiedenen Optionen beim Erstellen einer virtuellen Maschine. Sie können innerhalb einer vApp eine eigenständige virtuelle Maschine erstellen. Die eigenständige virtuelle Maschine ist direkt mit dem Organisations-VDC verbunden. Sie können auch eine virtuelle Maschine innerhalb einer vApp erstellen. Hierdurch können Sie mehrere virtuelle Maschinen und deren zugehörige Netzwerke zusammen gruppieren. Mithilfe von vApps können Sie komplexe Anwendungen erstellen und sie zur künftigen Verwendung in einem Katalog speichern.

Abbildung 2-1. Virtuelle Maschinen sind eigenständig oder befinden sich innerhalb einer vApp


Anzeigen und Bearbeiten von virtuellen Maschinen

Sie können virtuelle Maschinen anzeigen, die eigenständig oder Teil einer vApp sind. Sie können virtuelle Maschinen in einer Rasteransicht oder in einer Kartenansicht anzeigen.


Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Um die virtuellen Maschinen in einer Rasteransicht anzuzeigen, klicken Sie auf . Um sie in einer Kartenansicht anzuzeigen, klicken Sie auf .

Die Liste der virtuellen Maschinen wird in einer Rasteransicht oder als eine Liste mit Karten angezeigt.

- 4 (Optional) Konfigurieren Sie die Rasteransicht so, dass sie die gewünschten Details zu jeder virtuellen Maschine enthält.
 - a Klicken Sie in der Rasteransicht auf das **Raster-Editor**-Symbol ().
 - b Wählen Sie die Details der virtuellen Maschine aus, die in der Rasteransicht enthalten sein sollen, indem Sie die Kontrollkästchen neben den gewünschten Details aktivieren.

Zu den Details zählen u. a. Informationen zur Hardwareversion, zu VMware Tools, zum Arbeitsspeicher usw.
 - c Klicken Sie zum Speichern der Änderungen auf **OK**.


Die ausgewählten Details werden als Spalten für jede virtuelle Maschine angezeigt.
- 5 (Optional) Klicken Sie in der Rasteransicht auf der linken Seite einer virtuellen Maschine auf , um die Aktionen anzuzeigen, die Sie für die ausgewählte virtuelle Maschine durchführen können.

Beispielsweise können Sie eine virtuelle Maschine herunterfahren.
- 6 Um auf die Schnittstelle für das Gastbetriebssystem der virtuellen Maschine zuzugreifen, klicken Sie in der oberen rechten Ecke der Kartenansicht auf das Desktopsymbol:

Erstellen einer neuen eigenständigen virtuellen Maschine

Sie können eine neue eigenständige virtuelle Maschine erstellen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Klicken Sie auf **Neue VM**.
- 4 Geben Sie den Namen und den Computernamen für die virtuelle Maschine an.

Wichtig Der Computername darf nur alphanumerische Zeichen und Bindestriche enthalten. Ein Computername darf nicht nur aus Ziffern bestehen und darf keine Leerzeichen enthalten.

- 5 (Optional) Geben Sie eine aussagekräftige Beschreibung ein.
- 6 Wählen Sie aus, ob die virtuelle Maschine gleich nach der Erstellung eingeschaltet werden soll.

7 Wählen Sie aus, wie die virtuelle Maschine bereitgestellt werden soll.

Option	Aktion
Neu	<p>Sie stellen eine neue virtuelle Maschine mit anpassbaren Einstellungen bereit.</p> <ul style="list-style-type: none"> a Wählen Sie eine Betriebssystemfamilie und ein Betriebssystem aus. b (Optional) Wählen Sie ein Boot-Image aus. c Wählen Sie die Computing-Richtlinie aus. d Wählen Sie die Größe der virtuellen Maschine aus den vordefinierten Größensystemoptionen aus oder klicken Sie auf Benutzerdefinierte Größenänderungsoptionen, um die Anzahl der virtuellen CPUs, Kerne pro Socket und Arbeitsspeichereinstellungen manuell einzugeben. <p>Die vordefinierten Größen der virtuellen Maschinen sind: Klein, Mittel und Groß.</p> <ul style="list-style-type: none"> e Geben Sie die Speichereinstellungen für die virtuelle Maschine an, z. B. Speicherrichtlinie und Größe in GB. f Geben Sie die Netzwerkeinstellungen für die virtuelle Maschine an, z. B. Netzwerk, IP-Modus, IP-Adresse und primäre Netzwerkkarte.
Aus Vorlage	<p>Sie stellen eine virtuelle Maschine anhand einer Vorlage bereit, die Sie aus dem Vorlagenkatalog auswählen.</p> <ul style="list-style-type: none"> a Wählen Sie eine VM-Vorlage aus der Liste der verfügbaren Vorlagen aus. b (Optional) Geben Sie an, dass eine benutzerdefinierte Speicherrichtlinie verwendet werden soll, und wählen Sie die zu verwendende Speicherrichtlinie im Dropdown-Menü Zu verwendende benutzerdefinierte Speicherrichtlinie aus. c Lesen und akzeptieren Sie ggf. die Endbenutzerlizenzvereinbarung.

8 Klicken Sie auf **OK**, um die Einstellungen für die virtuelle Maschine zu speichern und den Erstellungsvorgang zu starten.

Die Karte für die virtuelle Maschine wird im Katalog angezeigt. Bis die virtuelle Maschine erstellt wird, wird der Status „Beschäftigt“ für sie angezeigt.

Öffnen der Konsole einer virtuellen Maschine

Über die Konsole der virtuellen Maschine können Sie Informationen zu einer virtuellen Maschine anzeigen, mit dem Gastbetriebssystem arbeiten und Vorgänge durchführen, die Auswirkungen auf das Gastbetriebssystem haben.

Voraussetzungen

Die virtuelle Maschine ist eingeschaltet.

Installieren von VMware Remote Console auf einem Client

VMware Remote Console bietet eine eingebettete Benutzer-Gast-Interaktion auf allen virtuellen Maschinen, die von vCloud Director bereitgestellt und verwaltet werden. Dieser Abschnitt bietet detaillierte Informationen zu den Aufgaben, die für die Installation von VMware Remote Console unter Windows, Apple OS X und Linux erforderlich sind.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Benutzer** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Laden Sie das Installationsprogramm herunter.
 - Navigieren Sie zur VMware Remote Console-Downloadseite und wählen Sie den Link für Ihre Plattform aus.

www.vmware.com/go/download-vmrc
 - Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** im vCloud Director-Mandantenportal auf die Karte des virtuellen Datencenters, das Sie durchsuchen möchten. Wählen Sie eine virtuelle Maschine aus und wählen Sie im Menü **Aktionen** die Option **VMRC herunterladen** aus.
- 2 Führen Sie Ihre Plattforminstallation aus.
 - Windows

 Doppelklicken Sie auf das `.msi`-Installationsprogramm und folgen Sie den Eingabeaufforderungen.
 - Linux

 Führen Sie das `.bundle`-Installationsprogramm mit Root-Berechtigungen aus und folgen Sie den Eingabeaufforderungen.
 - Mac

 Doppelklicken Sie auf die `.dmg`-Datei, um sie zu öffnen, und doppelklicken Sie dann auf das darin enthaltene VMware Remote Console-Symbol, um den Kopiervorgang in den Ordner „Programme“ durchzuführen.

Ergebnisse

Nach der Installation wird VMware Remote Console beim Klicken auf Uniform Resource Identifiers (URIs) geöffnet, die mit dem Schema `vmrc://` beginnen. VMware Workstation, Player und Fusion verarbeiten ebenfalls das `vmrc://`-URI-Schema.

Öffnen einer Remote-Konsole für die virtuelle Maschine


Sie können eine Konsole für die virtuelle Maschine mithilfe von VMware Remote Console über das vCloud Director-Mandantenportal öffnen.

Voraussetzungen

- Stellen Sie sicher, dass die VMware Remote Console auf Ihrem lokalen System installiert ist.
- Stellen Sie sicher, dass die ausgewählte virtuelle Maschine eingeschaltet ist.

- Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Benutzer** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine die Option **VM-Remote-Konsole starten** aus.

Hinweis Wenn die VMware Remote Console nicht installiert ist, werden Sie in einem Popup-Fenster aufgefordert, entweder VMware Remote Console zu installieren oder die Webkonsole zu verwenden.

Ergebnisse

Die Konsole für die virtuelle Maschine wird als eine externe virtuelle Remote-Konsole geöffnet.

Hinweis Wenn Sie eine Verbindung zu einer virtuellen vCloud Director-Maschine mithilfe von VMware Remote Console herstellen, sind Sie ausschließlich auf Konsoleninteraktionen beschränkt (durch Senden von `Ctrl+Alt+Del`). Sie können keine Geräte- oder Ein-/Ausschaltvorgänge durchführen und keine Einstellungen verwalten.


Öffnen einer Webkonsole

Sie können auch dann eine Verbindung zur Konsole für eine virtuelle Maschine herstellen, wenn VMware Remote Console nicht auf Ihrem lokalen System installiert ist.

Voraussetzungen

- Stellen Sie sicher, dass die virtuelle Maschine eingeschaltet ist.
- Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Benutzer** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine die Option **Webkonsole starten** aus.

Ergebnisse

Die Konsole der virtuellen Maschine wird in einer neuen Browser-Registerkarte über VMware HTML Console SDK geöffnet.

Nächste Schritte

Klicken Sie im Konsolenfenster auf eine beliebige Stelle, um mit der Verwendung der Maus, der Tastatur und anderer Eingabegeräte in der Konsole zu beginnen.

Hinweis Informationen zu unterstützten internationalen Tastaturen finden Sie in der VMware HTML Console SDK-Dokumentation unter <https://www.vmware.com/support/developer/html-console/>.

Ausführen von Energievorgängen auf virtuellen Maschinen

Sie können Energievorgänge für virtuelle Maschinen durchführen, z. B. Ein- oder Ausschalten einer virtuellen Maschine, Anhalten oder Zurücksetzen einer virtuellen Maschine oder Herunterfahren des Gastbetriebssystems einer virtuellen Maschine.

Einschalten einer virtuellen Maschine


Das Einschalten einer virtuellen Maschine ist das virtuelle Äquivalent des Einschaltens eines physischen Computers.

Sie können keine virtuelle Maschine einschalten, für die die Gastanpassung aktiviert ist, sofern auf der virtuellen Maschine keine aktuelle Version von VMware Tools installiert ist.

Voraussetzungen

Die virtuelle Maschine ist ausgeschaltet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, die Sie starten möchten, die Option **Einschalten** aus.

Ergebnisse

Der Status einer eingeschalteten virtuellen Maschine wird grün angezeigt.


Ausschalten einer virtuellen Maschine

Das Ausschalten einer virtuellen Maschine ist das virtuelle Äquivalent des Ausschaltens eines physischen Computers.

Voraussetzungen

Die virtuelle Maschine ist eingeschaltet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, die Sie ausschalten möchten, die Option **Ausschalten** aus.

Ergebnisse

Der Status einer ausgeschalteten virtuellen Maschine wird rot angezeigt.


Herunterfahren eines Gastbetriebssystems

Das Herunterfahren des Gastbetriebssystems für eine virtuelle Maschine entspricht dem Ausschalten eines physischen Computers.

Voraussetzungen

Die virtuelle Maschine und das Gastbetriebssystem müssen eingeschaltet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine die Option **Gastbetriebssystem herunterfahren** aus.

Ergebnisse

Das Gastbetriebssystem wird heruntergefahren.


Zurücksetzen einer virtuellen Maschine

Durch Zurücksetzen einer virtuellen Maschine wird der Zustand (z. B. Arbeitsspeicher und Cache) gelöscht, aber die virtuelle Maschine wird weiterhin ausgeführt. Das Zurücksetzen einer virtuellen Maschine entspricht dem Drücken der Rücksetztaste auf einem physischen Computer. Hierbei wird ein Kaltstart des Betriebssystems ohne Änderung des Betriebszustands der virtuellen Maschine initiiert.

Voraussetzungen

Die virtuelle Maschine ist eingeschaltet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, die Sie zurücksetzen möchten, die Option **Zurücksetzen** aus.

Ergebnisse

Der Zustand für die virtuelle Maschine wird gelöscht.

Anhalten einer virtuellen Maschine


Beim Anhalten einer virtuellen Maschine wird deren aktueller Zustand durch Schreiben des Arbeitsspeichers auf die Festplatte beibehalten.

Die Funktion zum Anhalten und Fortsetzen ist nützlich, wenn Sie den aktuellen Zustand Ihrer virtuellen Maschine speichern und im Anschluss Ihre Arbeit im selben Zustand fortsetzen möchten.

Voraussetzungen

Die virtuelle Maschine ist eingeschaltet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, die Sie anhalten möchten, die Option **Anhalten** aus.

Ergebnisse

Die virtuelle Maschine wird angehalten, aber der Zustand wird beibehalten.


Verwerfen des Status „Angehalten“ einer virtuellen Maschine

Wenn eine virtuelle Maschine den Zustand „Angehalten“ aufweist und die virtuelle Maschine nicht mehr verwendet werden muss, können Sie den Zustand „Angehalten“ verwerfen. Durch Verwerfen des Status „Angehalten“ wird der Speicher entfernt, und die Maschine wird ausgeschaltet.

Voraussetzungen

Eine angehaltene virtuelle Maschine.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine die Option **Zustand „Angehalten“ verwerfen** aus.

Ergebnisse

Der Zustand wird verworfen, und die virtuelle Maschine wird ausgeschaltet.

Installieren von VMware Tools in einer virtuellen Maschine

vCloud Director passt das Gastbetriebssystem mit VMware Tools an.

VMware Tools verbessert das Management und die Leistung der virtuellen Maschine, indem generische Betriebssystemtreiber durch für virtuelle Hardware optimierte VMware-Treiber ersetzt werden. Sie installieren VMware Tools im Gastbetriebssystem. Das Gastbetriebssystem funktioniert zwar auch ohne die VMware Tools, eine Vielzahl wichtiger und praktischer Funktionen steht jedoch nicht zur Verfügung.

Voraussetzungen

- Die virtuelle Maschine muss eingeschaltet sein.
- Wenn die neu erstellte virtuelle Maschine nicht über ein Gastbetriebssystem verfügt, müssen Sie dieses installieren, bevor Sie VMware Tools installieren können.
- Die Gastanpassung muss vor der Installation von VMware Tools deaktiviert werden.
- Wenn Sie eine ältere VMware Tools-Version als 7299 in einer virtuellen Maschine in der vApp verwenden, müssen Sie sie aktualisieren.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, in der Sie VMware Tools installieren möchten, die Option **VMware Tools installieren** aus.

VMware Tools wird auf dem Ziel-Gastbetriebssystem installiert. Wenn während der Installation ein Fehler auftritt, wird eine Fehlermeldung angezeigt. Sie können den Fortschritt des Installationsvorgangs auch im Fenster **Aufgaben** anzeigen.
- 4 Um die Webkonsole der virtuellen Maschine zu öffnen, wählen Sie im Menü **Aktionen** die Option **Webkonsole starten** aus.
- 5 Folgen Sie den Anweisungen im [VMware-Knowledgebase-Artikel 1014294](#), um VMware Tools für Ihr jeweiliges Betriebssystem zu konfigurieren.

Ergebnisse

VMware Tools ist auf dem Gastbetriebssystem installiert und konfiguriert.

Ausführen eines Upgrades der virtuellen Hardwareversion für eine virtuelle Maschine

Sie können einen Upgrade der virtuellen Hardwareversion für eine virtuelle Maschine ausführen. Höhere virtuelle Hardwareversionen unterstützen mehr Funktionen.

Eine Herabstufung der Hardwareversion für die virtuellen Maschinen in einer vApp ist nicht möglich.

vCloud Director unterstützt Hardwareversionen abhängig von den zugrunde liegenden vSphere-Ressourcen. Die unterstützte Hardwareversion hängt von der neuesten unterstützten virtuellen Hardwareversion im zugrunde liegenden Provider-VDC ab. Ein **-Organisationsadministrator** oder ein **Systemadministrator** kann die Hardwareversion auf eine frühere als die neueste unterstützte Version der zugrunde liegenden Hardware festlegen. Das vCloud Director-Mandantenportal legt dynamisch die Liste der auswählbaren Versionen virtueller Hardware fest, basierend auf der unterstützenden Hardware des Organisations-VDCs oder des Provider-VDCs.


Informationen zu den verfügbaren Hardwarefunktionen mit Einstellungen zur Kompatibilität der virtuellen Maschinen finden Sie im *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Informationen zu den VMware-Produkten und ihren Versionen virtueller Hardware finden Sie unter <https://kb.vmware.com/s/article/1003746>.

Voraussetzungen

- Beenden Sie die virtuelle Maschine oder die vApp, die die virtuelle Maschine enthält.
- Überprüfen Sie, ob die neueste Version von VMware Tools auf der virtuellen Maschine installiert ist.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, die Sie aktualisieren möchten, die Option **Upgrade für virtuelle Hardwareversion ausführen** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Die virtuelle Maschine wird auf die neueste Version aktualisiert.

Bearbeiten der Eigenschaften von virtuellen Maschinen

Sie können die Eigenschaften einer virtuellen Maschine bearbeiten, einschließlich des Namens und der Beschreibung der virtuellen Maschine, Hardware- und Netzwerkeinstellungen, Gastbetriebssystemeinstellungen und so weiter.


Ändern der allgemeinen Eigenschaften einer virtuellen Maschine

Sie können den Namen, die Beschreibung und andere allgemeine Eigenschaften einer virtuellen Maschine prüfen und ändern.

Voraussetzungen

Zum Ändern von Eigenschaften, wie z. B. des Betriebssystems, muss die Maschine ausgeschaltet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Klicken Sie in der Karte der zu bearbeitenden virtuellen Maschine auf **Details**.

- 4 Die Liste der Eigenschaften, die angezeigt oder bearbeitet werden können, wird unter **Allgemein** standardmäßig angezeigt.

Option	Aktion
Name der virtuellen Maschine	Bearbeiten Sie den Namen der virtuellen Maschine. Sie können diese Eigenschaft bearbeiten, während die virtuelle Maschine eingeschaltet ist.
Computer-Name	Bearbeiten Sie die im Gastbetriebssystem festgelegten Computer- und Hostnamen, die die virtuelle Maschine in einem Netzwerk angeben. Dieses Feld ist aufgrund einer Windows-Beschränkung für Computernamen auf 15 Zeichen beschränkt. Sie können diese Eigenschaft bearbeiten, während die virtuelle Maschine eingeschaltet ist.
Beschreibung	Bearbeiten Sie die optionale Beschreibung der virtuellen Maschine. Sie können diese Eigenschaft bearbeiten, während die virtuelle Maschine eingeschaltet ist.
Betriebssystem-Familie	Wählen Sie im Dropdown-Menü eine Betriebssystem-Familie aus. Sie können diese Eigenschaft bearbeiten, während die virtuelle Maschine ausgeschaltet ist. Sie können diese Eigenschaft nicht bearbeiten, wenn bereits ein Betriebssystem auf der virtuellen Maschine vorhanden ist.
Betriebssystem	Wählen Sie im Dropdown-Menü ein Betriebssystem aus. Sie können diese Eigenschaft bearbeiten, während die virtuelle Maschine ausgeschaltet ist. Sie können diese Eigenschaft nicht bearbeiten, wenn bereits ein Betriebssystem auf der virtuellen Maschine vorhanden ist.
Startverzögerung	Geben Sie die Zeit für die Verzögerung des Startvorgangs in Millisekunden an. Die Zeit zwischen dem Einschalten der virtuellen Maschine und dem Zeitpunkt, zu dem das BIOS verlassen wird und die Software des Gastbetriebssystems gestartet wird, kann kurz sein. Sie können die Startverzögerung ändern, um hierfür mehr Zeit einzuräumen.
Speicherrichtlinie	Wählen Sie im Dropdown-Menü eine Speicherrichtlinie zur Verwendung durch die virtuelle Maschine aus. Sie können diese Eigenschaft bearbeiten, während die virtuelle Maschine eingeschaltet ist.
Virtuelles Datencenter	Zeigen Sie den Namen des virtuellen Datencenters an, zu dem diese virtuelle Maschine gehört.
VMware Tools	Prüfen Sie, ob VMware Tools auf der virtuellen Maschine installiert ist.
Version der virtuellen Hardware	Überprüfen Sie die Version der virtuellen Hardware der virtuellen Maschine.
Upgrade auf:	Um ein Upgrade durchzuführen, wählen Sie im Dropdown-Menü eine Version aus.

Option	Aktion
Zeit synchronisieren	Aktivieren Sie dieses Kontrollkästchen, um die Zeitsynchronisierung zwischen dem Gastbetriebssystem der virtuellen Maschine und dem virtuellen Datencenter, in dem die VM ausgeführt wird, zu aktivieren.
BIOS-Setup aufrufen	Wählen Sie, ob beim nächsten Starten der virtuellen Maschine die Eingabe auf dem BIOS-Setup-Bildschirm erzwungen werden soll. Sie können diese Eigenschaft bearbeiten, während die virtuelle Maschine ausgeschaltet ist.

- 5 Klicken Sie auf **Speichern**, sobald Sie die gewünschten Änderungen vorgenommen haben.


Ändern der Hardwareeigenschaften einer virtuellen Maschine

Sie können die Hardwareeigenschaften einer virtuellen Maschine überprüfen und ändern.

Voraussetzungen

Die virtuelle Maschine muss ausgeschaltet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Klicken Sie in der Karte der zu bearbeitenden virtuellen Maschine auf **Details**.
- 4 Klicken Sie auf **Hardware**, um die Liste der Hardwareeigenschaften zu erweitern, die Sie anzeigen und bearbeiten können.

Option	Beschreibung
Anzahl der virtuellen CPUs	Bearbeiten Sie die Anzahl der CPUs. Die maximale Anzahl von virtuellen CPUs, die Sie einer virtuellen Maschine zuweisen können, hängt von der Anzahl der logischen CPUs auf dem Host und dem Typ des Gastbetriebssystems ab, das auf der virtuellen Maschine installiert ist.
Kerne pro Socket	Bearbeiten Sie die Kerne pro Socket. Sie können konfigurieren, wie die virtuellen CPUs in Bezug auf die Kerne und die Kerne pro Socket zugewiesen werden. Legen Sie die gewünschte Anzahl der CPU-Kerne in der virtuellen Maschine fest und wählen Sie anschließend die gewünschte Anzahl der Kerne in jedem Socket aus, je nachdem, ob Sie eine Single-Core-CPU, Dual-Core-CPU, Tri-Core-CPU usw. haben möchten.
Offenlegen der hardwaregestützten CPU-Virtualisierung für ein Gastbetriebssystem	Sie können für das Gastbetriebssystem die komplette CPU-Virtualisierung offenlegen, sodass Anwendungen, die Hardwarevirtualisierung benötigen, auf virtuellen Maschinen ohne binäre Übersetzung oder Paravirtualisierung ausgeführt werden können.

Option	Beschreibung
Gesamter Arbeitsspeicher	<p>Bearbeiten Sie die Einstellungen für die Arbeitsspeicherressourcen für eine virtuelle Maschine. Die Größe des Arbeitsspeichers der virtuellen Maschine muss ein Vielfaches von 4 MB sein.</p> <p>Diese Einstellung bestimmt, wie viel Arbeitsspeicher des ESXi-Hosts der virtuellen Maschine zugeteilt wird. Die Arbeitsspeichergröße der virtuellen Hardware legt fest, wie viel Arbeitsspeicher für die in der virtuellen Maschine ausgeführten Anwendungen verfügbar ist. Eine virtuelle Maschine kann Arbeitsspeicherressourcen nur in dem Umfang nutzen, der für die virtuelle Hardware konfiguriert wurde.</p>
Arbeitsspeicher-Hot-Add	Wenn Sie Arbeitsspeicher-Hot-Add aktivieren, können Sie einer virtuellen Maschine Arbeitsspeicherressourcen hinzufügen, während die Maschine eingeschaltet ist. Dieses Merkmal wird nur von bestimmten Gastbetriebssystemen und VM-Hardwareversionen höher als 7 unterstützt.
Hot-Add der virtuellen CPU	Wenn Sie Hot-Add der virtuellen CPU aktivieren, können Sie der virtuellen Maschine virtuelle CPUs hinzufügen, während sie eingeschaltet ist. Sie können nur ein Vielfaches der Anzahl der Kerne pro Socket hinzufügen. Dieses Merkmal wird nur von bestimmten Gastbetriebssystemen und VM-Hardwareversionen unterstützt.
Anzahl der Sockets	<p>Zeigen Sie die Anzahl der Sockets an.</p> <p>Die Anzahl der Sockets wird durch die Anzahl der verfügbaren virtuellen CPUs bestimmt. Die Anzahl ändert sich, wenn Sie die Anzahl der virtuellen CPUs aktualisieren.</p>
Wechselmedien	Zeigt die verfügbaren Wechselmedien an, beispielsweise angeschlossene CD/DVD- und Diskettenlaufwerke.

5 Klicken Sie unter **Festplatten** auf **Hinzufügen**, um eine Festplatte hinzuzufügen.

Option	Beschreibung
Größe	<p>Geben Sie die Größe der Festplatte in MB ein. Sie können die Größe der Festplatte später erhöhen.</p> <p>Hinweis Sie können die Größe einer vorhandenen Festplatte erhöhen, wenn es sich bei der virtuellen Maschine nicht um einen verknüpften Klon handelt und keine Snapshots für sie vorhanden sind.</p>
Richtlinie	<p>Die Speicherrichtlinie für die virtuelle Maschine wird standardmäßig verwendet.</p> <p>Standardmäßig verwenden alle mit einer virtuellen Maschine verbundenen Festplatten die für die virtuelle Maschine angegebene Speicherrichtlinie. Sie können diese Standardeinstellung für alle diese Festplatten überschreiben, wenn Sie eine virtuelle Maschine erstellen oder zugehörige Eigenschaften ändern. Die Spalte „Größe“ für jede Festplatte enthält ein Dropdown-Menü, in dem alle für diese virtuelle Maschine verfügbaren Speicherrichtlinien aufgeführt werden.</p>
Bus-Typ	<p>Wählen Sie den Bus-Typ aus.</p> <p>Die Optionen sind Paravirtual (SCSI), LSI Logic parallel (SCSI), LSI Logic SAS (SCSI), IDE und SATA. Weitere Informationen zu Speicher-Controller-Typen und Kompatibilität finden Sie unter <i>vSphere-Administratorhandbuch für virtuelle Maschinen</i>.</p>

Option	Beschreibung
Bus-Nummer	Geben Sie die Bus-Nummer ein.
Einheitennummer	Geben Sie die Logical Unit Number für die Festplatte ein.

- 6 Klicken Sie unter **Netzwerkadapter** auf **Hinzufügen**, um einen neuen Netzwerkadapter hinzuzufügen.

Sie können bis zu 10 Netzwerkadapter hinzufügen. Informationen über die Anzahl der unterstützten Netzwerkadapter je nach Hardwareversion der virtuellen Maschine finden Sie unter: <http://kb.vmware.com/s/article/2051652>. vCloud Director unterstützt das Ändern von Netzwerkkarten virtueller Maschinen, während die virtuelle Maschine ausgeführt wird. Informationen zu unterstützten Netzwerkadaptertypen finden Sie unter <http://kb.vmware.com/kb/1001805>.

Option	Beschreibung
Primärer Netzwerkadapter	Wenn die primäre Netzwerkkarte ausgewählt ist, wird ein entsprechendes Kennzeichen angezeigt. Wählen Sie einen primären Netzwerkadapter aus. Die Einstellung der primären Netzwerkkarte legt das Standard-Gateway, d. h. das einzige Gateway, für die virtuelle Maschine fest. Die virtuelle Maschine kann jede beliebige Netzwerkkarte verwenden, um Verbindungen zu virtuellen und physischen Maschinen herzustellen, die direkt mit demselben Netzwerk wie die Netzwerkkarte verbunden sind. Sie kann jedoch nur die primäre Netzwerkkarte verwenden, um Verbindungen zu Maschinen auf Netzwerken herzustellen, für die eine Gateway-Verbindung erforderlich ist.
Netzwerkadapter	Anzahl der Netzwerkadapter.
Verbunden	Aktivieren Sie das Kontrollkästchen, um einen Netzwerkadapter anzuschließen.
Netzwerk	Wählen Sie ein Netzwerk aus dem Dropdown-Menü.
IP-Modus	Wählen Sie einen IP-Modus aus: <ul style="list-style-type: none"> ■ Statisch – IP-Pool Ruft eine statische IP-Adresse aus dem IP-Pool des Netzwerks ab. ■ Statisch – Manuell Ermöglicht Ihnen, eine bestimmte IP-Adresse manuell anzugeben. Wenn Sie diese Option auswählen, müssen Sie eine IP-Adresse in der Spalte IP-Adresse eingeben. ■ DHCP Ruft eine IP-Adresse aus einem DHCP-Server ab.
MAC-Adresse	Geben Sie die MAC-Adresse der Netzwerkschnittstelle ein.

- 7 Klicken Sie auf **Speichern**.

Ändern der Eigenschaften für die Gastbetriebssystem-Anpassung einer virtuellen Maschine


Die Gastbetriebssystem-Anpassung in vCloud Director ist für alle Plattformen optional. Für virtuelle Maschinen, die einer Windows-Domäne beitreten müssen, ist sie obligatorisch.

Einige der in diesem Menü angeforderten Informationen gelten nur für Windows-Plattformen. Der Fensterbereich „Gastbetriebssystem-Anpassung“ enthält die erforderlichen Informationen für den Beitritt der virtuellen Maschine zu einer Windows-Domäne. Ein **Organisationsadministrator** kann Standardwerte für eine Domäne angeben, der Windows-Gastbetriebssysteme in dieser Organisation beitreten können. Nicht alle Windows-VMs müssen einer Domäne beitreten, aber bei den meisten Unternehmensinstallationen kann eine virtuelle Maschine, die kein Domänenmitglied ist, auf viele der verfügbaren Netzwerkressourcen nicht zugreifen.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.
- Für die Gast-Anpassung muss die virtuelle Maschine VMware Tools ausführen.
- Bevor Sie ein Windows-Gastbetriebssystem anpassen können, muss Ihr **Systemadministrator** die entsprechenden Microsoft Sysprep-Dateien in der vCloud Director-Servergruppe installieren. Siehe *vCloud Director Installations- und Upgrade-Handbuch*.
- Das Anpassen von Linux-Gastbetriebssystemen setzt voraus, dass Perl auf dem Gastbetriebssystem installiert ist.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Klicken Sie in der Karte der zu bearbeitenden virtuellen Maschine auf **Details**.

- 4 Klicken Sie auf **Gastbetriebssystem-Anpassung und -Eigenschaften**, um die Liste der Gastbetriebssystem-Einstellungen zu erweitern.

Option	Beschreibung
Aktivieren der Gast-Anpassung	Wählen Sie diese Option aus, um die Gastanpassung zu aktivieren.
SID ändern	<p>Wählen Sie diese Option aus, um die Windows-Sicherheits-ID (SID) zu ändern.</p> <p>Diese Option steht nur virtuellen Maschinen zur Verfügung, die ein Windows-Gastbetriebssystem ausführen. Einige Windows-Betriebssysteme verwenden eine SID, um Systeme und Benutzer eindeutig identifizieren zu können. Wenn Sie diese Option nicht auswählen, erhält die neue virtuelle Maschine dieselbe SID wie die virtuelle Maschine oder die Vorlage, auf der sie basiert. Mehrfach vergebene SIDs verursachen keine Probleme, wenn die Computer zu einer Domäne gehören und nur Domänenbenutzerkonten verwendet werden. Sind die Maschinen allerdings Teil einer Arbeitsgruppe oder werden lokale Benutzerkonten verwendet, können solche SIDs die Dateizugriffssteuerung beeinträchtigen. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Microsoft Windows-Betriebssystem.</p>
Lokales Administratorkennwort zulassen	<p>Wählen Sie diese Option aus, um das Festlegen eines Administratorkennworts für das Gastbetriebssystem zuzulassen.</p> <p>a Geben Sie ein Kennwort für den lokalen Administrator an.</p> <p>Wenn das Textfeld Kennwort angeben leer gelassen wird, wird automatisch ein Kennwort generiert.</p> <p>b Geben Sie die zulässige Anzahl von automatischen Anmeldeversuchen an.</p> <p>Wenn Sie den Wert 0 eingeben, wird die automatische Anmeldung als Administrator deaktiviert.</p>
Administrator muss Kennwort bei der ersten Anmeldung ändern	Wählen Sie diese Option aus, um Administratoren aufzufordern, das Kennwort des Gastbetriebssystems bei der ersten Anmeldung zu ändern. Dies wird aus Sicherheitsgründen empfohlen.
Kennwort automatisch erstellen	Wählen Sie diese Option aus, um die automatische Generierung von Kennwörtern zuzulassen.

Option	Beschreibung
Dieser VM ermöglichen, einer Domäne beizutreten	<p>Sie können diese Option auswählen, um die virtuelle Maschine in eine Windows-Domäne aufzunehmen. Sie können die Domäne der Organisation verwenden oder diese überschreiben und die Domäneneigenschaften eingeben.</p> <ul style="list-style-type: none"> a Geben Sie den Domänennamen ein. b Geben Sie den Benutzernamen und das Kennwort ein. c Geben Sie die Kontoorganisationseinheit ein.
Skript	<p>Sie können ein Anpassungsskript verwenden, um das Gastbetriebssystem der virtuellen Maschine zu ändern. Wenn Sie ein Anpassungsskript zu einer virtuellen Maschine hinzufügen, wird das Skript nur für die erste Anpassung verwendet und eine Neuanpassung wird erzwungen. Wenn Sie den Befehlszeilenparameter <code>precustomization</code> festlegen, wird das Skript vor dem Starten der Gastanpassung aufgerufen. Wenn Sie den Befehlszeilenparameter <code>postcustomization</code> festlegen, wird das Skript nach Abschluss der Gastanpassung aufgerufen.</p> <ul style="list-style-type: none"> ■ Klicken Sie unterhalb des Textfelds „Skript“ auf die Schaltfläche „Hochladen“, um zu einem Anpassungsskript auf Ihrem lokalen Computer zu navigieren. ■ Geben Sie das Anpassungsskript direkt im Textfeld Skriptdatei ein. <p>Ein Anpassungsskript, das direkt im Textfeld Skriptdatei eingegeben wird, darf maximal 1500 Zeichen enthalten. Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel https://kb.vmware.com/kb/1026614.</p>

5 Klicken Sie auf **Speichern**, sobald Sie die gewünschten Änderungen vorgenommen haben.

Wissenswertes über die Gast-Anpassung

Bevor Sie das Gastbetriebssystem anpassen, sollten Sie einige Einstellungen und Optionen kennenlernen.

Kontrollkästchen "Gast-Anpassung aktivieren"

Dieses Kontrollkästchen befindet sich auf der Registerkarte **Gastbetriebssystem-Anpassung** der Seite **Eigenschaften** der virtuellen Maschine. Ziel der Gast-Anpassung ist, Einstellungen auf der Grundlage der auf der Seite **Eigenschaften** ausgewählten Optionen vorzunehmen. Wenn dieses Kontrollkästchen aktiviert ist, werden Gast-Anpassung und Neuanpassung bei Bedarf durchgeführt.

Dieser Prozess ist Voraussetzung dafür, dass alle Gast-Anpassungsfunktionen, z. B. Computernamen, Netzwerkeinstellungen, Einstellung und Ablauf des Administrator- und des Root-Kennworts und SID-Änderung für Windows-Betriebssysteme usw., ordnungsgemäß arbeiten. Diese Option muss aktiviert sein, damit **Einschalten und Neuanpassung des Gastbetriebssystems erzwingen** funktioniert.

Wenn das Kontrollkästchen aktiviert ist und die Konfigurationsparameter der virtuellen Maschine in vCloud Director nicht mit den Einstellungen im Gastbetriebssystem synchronisiert sind, wird auf der Registerkarte **Profil** der Seite **Eigenschaften** der virtuellen Maschine angezeigt, dass die Einstellungen nicht mit dem Gastbetriebssystem synchronisiert sind und die Gast-Anpassung für die virtuelle Maschine erforderlich ist.

Gast-Anpassungsverhalten für vApps und virtuelle Maschinen

Die Kontrollkästchen sind deaktiviert.

- **Gast-Anpassung aktivieren**
- Unter Windows-Gastbetriebssystemen **SID ändern**
- **Kennwort zurücksetzen**

Wenn Sie die Anpassung durchführen möchten (oder Änderungen an den Netzwerkeinstellungen vorgenommen haben, die im Gastbetriebssystem widergespiegelt werden müssen), können Sie das Kontrollkästchen **Gast-Anpassung aktivieren** aktivieren und die Optionen auf der Registerkarte **Gastbetriebssystem-Anpassung** der Seite **Eigenschaften** der virtuellen Maschine festlegen. Wenn virtuelle Maschinen auf der Basis von vApp-Vorlagen zum Erstellen einer vApp und anschließenden Hinzufügen einer virtuellen Maschine verwendet werden, fungieren die vApp-Vorlagen als Bausteine. Wenn Sie virtuelle Maschinen aus einem Katalog zu einer neuen vApp hinzufügen, werden die virtuellen Maschinen standardmäßig für die Gast-Anpassung aktiviert. Wenn Sie eine vApp-Vorlage aus einem Katalog als vApp speichern, werden virtuelle Maschinen nur dann für die Gast-Anpassung aktiviert, wenn das Kontrollkästchen **Gast-Anpassung aktivieren** aktiviert ist.

Die Gast-Anpassungseinstellungen haben die folgenden Standardwerte:

- Das Kontrollkästchen **Gast-Anpassung aktivieren** entspricht der virtuellen Quellmaschine im Katalog.
- Für virtuelle Gastmaschinen von Windows entspricht **SID ändern** der virtuellen Quellmaschine im Katalog.
- Die Einstellung "Kennwort zurücksetzen" entspricht der virtuellen Quellmaschine im Katalog.

Sie können bei Bedarf das Kontrollkästchen **Gast-Anpassung aktivieren** deaktivieren, bevor Sie die vApp starten.

Wenn leere virtuelle Maschinen, bei denen die Gastbetriebssysteminstallation noch aussteht, zu einer vApp hinzugefügt werden, wird das Kontrollkästchen **Gast-Anpassung aktivieren** standardmäßig deaktiviert, da diese virtuellen Maschinen noch nicht bereit für die Anpassung sind.

Nachdem Sie das Gastbetriebssystem und VMware Tools installiert haben, können Sie die virtuellen Maschinen ausschalten, die vApp beenden und das Kontrollkästchen **Gast-Anpassung aktivieren** aktivieren sowie die vApp und die virtuelle Maschine starten, um die Gast-Anpassung durchzuführen.

Werden der Name der virtuellen Maschine und die Netzwerkeinstellungen auf einer virtuellen Maschine aktualisiert, die angepasst wurde, wird die virtuelle Maschine beim nächsten Einschalten neu angepasst. Dabei wird die virtuelle Gastmaschine mit vCloud Director erneut synchronisiert.

Einschalten und Erzwingen der Neuanpassung für eine virtuelle Maschine

Sie können eine virtuelle Maschine einschalten und die Neuanpassung einer virtuellen Maschine erzwingen.


Wenn die Einstellungen auf einer virtuellen Maschine nicht mit vCloud Director synchronisiert sind oder ein Gast-Anpassungsversuch fehlgeschlagen ist, können Sie die Neuanpassung der virtuellen Maschine erzwingen.

Stellen Sie sicher, dass die Anwendung, die in der virtuellen Maschine ausgeführt wird, eine Neuanpassung unterstützt. Wenn Sie einen Domänencontroller mithilfe von Microsoft Sysprep ändern und auch die SID ändern, wird die virtuelle Maschine möglicherweise beschädigt. Um das Risiko einer Beschädigung der virtuellen Maschine zu verringern, erstellen Sie einen Snapshot, bevor Sie sie neu anpassen.

Voraussetzungen

- Sie müssen ein Organisationsadministrator sein.
- Die virtuelle Maschine muss ausgeschaltet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Stromversorgung** der virtuellen Maschine, die Sie einschalten und anpassen möchten, **Einschalten und Neuanpassung des Gastbetriebssystems erzwingen** aus.

Ergebnisse

Die virtuelle Maschine wird neu angepasst und eingeschaltet.

Ändern der erweiterten Eigenschaften einer virtuellen Maschine

In den **erweiterten** Einstellungen können Sie die Einstellungen für die Ressourcenzuweisung (Anteile, Reservierung und Grenzwerte) festlegen, um den Umfang der für eine virtuelle Maschine bereitgestellten CPU-, Arbeitsspeicher- und Speicherressourcen zu bestimmen.

Verwenden Sie die Einstellungen für die Ressourcenzuweisung (Anteile, Reservierung und Limit), um den Umfang der für eine virtuelle Maschine bereitgestellten Prozessor-, Arbeitsspeicher- und Speicherressourcen zu bestimmen.

Ressourcenzuweisung durch Anteile

Anteile kennzeichnen die relative Bedeutung einer virtuellen Maschine innerhalb eines virtuellen Datencenters. Falls eine virtuelle Maschine doppelt so viele Anteile einer Ressource wie eine andere virtuelle Maschine hat, darf sie doppelt so viel von der Ressource verbrauchen wie die andere, wenn beide um die Ressource konkurrieren. Anteile werden üblicherweise als „Hoch“, „Normal“ oder „Niedrig“ angegeben und diese Werte stehen für Anteilswerte in einem Verhältnis von 4:2:1. Sie können auch die Option „Benutzerdefiniert“ auswählen, um

jeder virtuellen Maschine eine bestimmte Anzahl von Anteilen (die ein proportionales Gewicht ausdrückt) zuzuweisen. Wenn Sie einer virtuellen Maschine Anteile zuweisen, legen Sie damit immer die Priorität dieser virtuellen Maschine relativ zu anderen eingeschalteten virtuellen Maschinen fest.

Ressourcenzuweisung durch Reservierung

Gibt die garantierte Mindestzuteilung für eine virtuelle Maschine an. vCloud Director ermöglicht es Ihnen, eine virtuelle Maschine nur dann einzuschalten, wenn ausreichend nicht reservierte Ressourcen zur Bereitstellung der Reservierungsmenge für die virtuelle Maschine verfügbar sind. Das virtuelle Datacenter garantiert diese Menge auch bei starker Auslastung seiner Ressourcen. Die Reservierung wird in konkreten Einheiten (Megahertz oder Megabyte) ausgedrückt.

Beispiel: Angenommen, es sind 2 GHz CPU-Leistung verfügbar, und Sie legen für VM1 und VM2 jeweils eine Ressourcenzuweisung durch Reservierung von 1 GHz fest. Dann wird jeder virtuellen Maschine garantiert, bei Bedarf 1 GHz CPU-Leistung zugewiesen zu erhalten. Wenn VM1 nur 500 MHz nutzt, stehen 1,5 GHz für VM2 zur Verfügung.

Reservierungen sind standardmäßig auf 0 gesetzt. Sie können eine Reservierung angeben, wenn Sie gewährleisten müssen, dass eine erforderliche Mindestmenge an CPU-Leistung und Arbeitsspeicher jederzeit für die virtuelle Maschine verfügbar ist.

Ressourcenzuweisung durch Limits

Gibt eine Obergrenze für CPU- und Arbeitsspeicherressourcen an, die einer virtuellen Maschine zugewiesen werden können. Ein virtuelles Datacenter kann einer virtuellen Maschine mehr als die Reservierung zuteilen, jedoch nie mehr als das Limit, selbst wenn es ungenutzte Ressourcen im System gibt. Das Limit wird in konkreten Einheiten (Megahertz oder Megabyte) ausgedrückt.

Die Standardeinstellung der Limits für CPU- und Arbeitsspeicherressourcen ist "Unbegrenzt". Bei einem unbegrenzten Arbeitsspeicher-Limit bildet die bei der Erstellung einer virtuellen Maschine konfigurierte Arbeitsspeichermenge in den meisten Fällen die effektive Obergrenze.


Meistens ist es jedoch nicht notwendig, ein Limit anzugeben. Durch Angabe eines Limits werden möglicherweise Leerlauf-Ressourcen verschwendet. Das System lässt nicht zu, dass eine virtuelle Maschine Ressourcen nutzt, die über den für sie festgelegten Grenzwert hinausgehen, auch wenn das System nicht voll ausgelastet ist und die im Leerlauf befindlichen Ressourcen verfügbar sind. Geben Sie ein Limit nur dann an, wenn Sie gute Gründe dafür haben.

Voraussetzungen

- Virtuelles Datacenter in einem Reservierungspool.
- Stellen Sie sicher, dass das virtuelle Datacenter eine bestimmte Menge von Arbeitsspeicher für eine virtuelle Maschine bereitstellt.

- Garantieren Sie, dass einer bestimmten virtuellen Maschine immer ein höherer Prozentsatz der VDC-Ressourcen zugewiesen wird als anderen virtuellen Maschinen.
- Legen Sie eine Obergrenze für die Ressourcen fest, die einer virtuellen Maschine zugewiesen werden können.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Klicken Sie in der Karte der zu bearbeitenden virtuellen Maschine auf **Details**.
- 4 Klicken Sie auf **Erweitert**.
- 5 Legen Sie die Anteile der Ressourcenzuweisungen für die CPU-Einstellungen fest, indem Sie eine Option aus dem Dropdown-Menü **Priorität** auswählen.

Option	Beschreibung
Niedrig	Teilt 500 Anteile pro virtueller CPU zu.
Normal	Teilt 1000 Anteile pro virtueller CPU zu.
Hoch	Teilt 2000 Anteile pro virtueller CPU zu.
Benutzerdefiniert	Sie können eine bestimmte Anzahl von Anteilen zuweisen, indem Sie die Anzahl von Anteilen (die ein proportionales Gewicht ausdrückt) für jede virtuelle Maschine eingeben. Wenn Sie einer virtuellen Maschine Anteile zuweisen, legen Sie damit immer die Priorität dieser virtuellen Maschine relativ zu anderen eingeschalteten virtuellen Maschinen fest.

- 6 Geben Sie die Reservierung für die CPU-Einstellungen durch Eingabe der Reservierung in MHz und optional das Limit für die CPU-Einstellungen in MHz an.

Option	Beschreibung
Unbegrenzt	Die Standardoption für die CPU-Ressource.
Maximum	Geben Sie eine Obergrenze für CPU-Ressourcen an, die einer virtuellen Maschine zugewiesen werden können.

- 7 Legen Sie die Anteile der Ressourcenzuweisungen für die Arbeitsspeichereinstellungen fest, indem Sie eine Option aus dem Dropdown-Menü **Priorität** auswählen.

Option	Beschreibung
Niedrig	Teilt 5 Anteile pro Megabyte konfigurierten VM-Arbeitsspeichers zu.
Normal	Teilt 10 Anteile pro Megabyte konfigurierten VM-Arbeitsspeichers zu.

Option	Beschreibung
Hoch	Teilt 20 Anteile pro Megabyte konfigurierten VM-Arbeitsspeichers zu.
Benutzerdefiniert	Sie können eine bestimmte Anzahl von Anteilen zuweisen, indem Sie die Anzahl der Anteile eingeben.

- 8 Geben Sie die Reservierung für die Arbeitsspeichereinstellungen in MB und optional das Limit für die Arbeitsspeichereinstellungen in MB an.

Option	Beschreibung
Unbegrenzt	Die Standardoption für die CPU-Ressource.
Maximum	Geben Sie eine Obergrenze für CPU- und Arbeitsspeicherressourcen an, die einer virtuellen Maschine zugewiesen werden können.

- 9 Klicken Sie unter **Metadaten** auf **Hinzufügen**, um die Metadaten anzugeben.
Beispielsweise können Sie Metadaten über das Erstellungsdatum oder den Besitzer hinzufügen.
- 10 Klicken Sie auf **Speichern**, sobald Sie die gewünschten Änderungen vorgenommen haben.


Medium einlegen

Sie können Medien einlegen, wie z. B. CD/DVD-Images aus Katalogen, und diese in einem Gastbetriebssystem für virtuelle Maschinen verwenden. Sie können diese Mediendateien verwenden, um ein Betriebssystem in der virtuellen Maschine, verschiedene Anwendungen, Treiber usw. zu installieren.

Voraussetzungen

Sie haben Zugriff auf einen Katalog mit Mediendateien.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie die virtuelle Maschine aus, auf der Sie die Medien hinzufügen möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Medium einlegen** aus.
- 5 Wählen Sie im Fenster **CD einlegen** die Mediendatei aus, die in die virtuelle Maschine eingefügt werden soll.
- 6 Klicken Sie auf **Einfügen**.


Medium auswerfen

Wenn Sie eine CD oder DVD nicht mehr in der virtuellen Maschine benötigen, können Sie die Mediendatei auswerfen.

Voraussetzungen

In die virtuelle Maschine wurde zuvor eine Mediendatei eingelegt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie die virtuelle Maschine aus, aus der Sie das Medium auswerfen möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Medium auswerfen** aus.

Ergebnisse

Die Mediendatei wird ausgeworfen.

Kopieren einer virtuellen Maschine in eine andere vApp


Sie können eine virtuelle Maschine in eine andere vApp kopieren. Wenn Sie eine virtuelle Maschine kopieren, verbleibt die ursprüngliche virtuelle Maschine in der Quell-vApp.

Wenn Sie eine virtuelle Maschine kopieren, sind die Snapshots in der Kopie nicht enthalten.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.
- Schalten Sie die VM aus.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, die Sie kopieren möchten, die Option **Kopieren nach** aus.

- 4 Wählen Sie die Ziel-vApp, in die Sie die virtuelle Maschine kopieren möchten, und klicken Sie auf **Weiter**.
- 5 Konfigurieren Sie die Ressourcen, wie z. B. den Namen der virtuellen Maschine und den Computernamen sowie optional die Speicherrichtlinie und die Netzwerkkarten, und klicken Sie auf **Weiter**.

Wichtig Der Computernamen darf nur alphanumerische Zeichen und Bindestriche enthalten. Er darf nicht nur aus Ziffern bestehen und darf keine Leerzeichen enthalten.

- 6 Überprüfen Sie auf der Seite **Bereit zum Abschließen** Ihre Einstellungen und klicken Sie auf **Fertig**.

Verschieben einer virtuellen Maschine in eine andere vApp

Sie können eine virtuelle Maschine in eine andere vApp verschieben. Wenn Sie eine virtuelle Maschine verschieben, wird die ursprüngliche virtuelle Maschine aus der Quell-vApp entfernt.

Wenn Sie eine virtuelle Maschine in eine andere vApp verschieben, gehen die erfassten Snapshots verloren.

Ab vCloud Director 9.5 basiert das Verschieben von VMs in verschiedene vApps auf VMware vSphere vMotion[®] und Enhanced vMotion Compatibility (EVC). Sie können eine VM in eine andere vApp verschieben, die zur gleichen oder einer anderen Organisations-VDC innerhalb desselben Provider-VDC gehört.

Während Sie eine virtuelle Maschine in eine andere vApp verschieben, können Sie Neukonfigurationen durchführen, wie zum Beispiel das Ändern des Netzwerks oder des Speicherprofils.

Tabelle 2-1. Neukonfigurationen beim Verschieben von virtuellen Maschinen und VM-Zustände


Neukonfiguration	VM-Zustand, wenn sich die Ziel-vApp im selben Organisations-VDC befindet	VM Zustand, wenn sich die Ziel-vApp in einem anderen Organisations-VDC innerhalb des gleichen Provider-VDC befindet
Ändern des Netzwerks	Ausgeschaltet	n. z.
Entfernen des Netzwerks	Ein- oder ausgeschaltet	n. z.
Ändern des Speicherprofils	Ein- oder ausgeschaltet	Ausgeschaltet

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.

- Vergewissern Sie sich, dass die zugrunde liegenden vSphere-Ressourcen vMotion und EVC unterstützen. Informationen zu den Anforderungen und Einschränkungen bei vMotion und EVC finden Sie unter *vCenter Server und Hostverwaltung*.
- Wenn Sie das VM-Netzwerk oder das Speicherprofil ändern möchten, überprüfen Sie, ob Sie die virtuelle Maschine ausschalten müssen. Weitere Informationen finden Sie in der Tabelle *Neukonfigurationen während VM-Verschiebungen und VM-Zuständen*.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der Maschine, die Sie verschieben möchten, die Option **Verschieben nach** aus.
- 4 Wählen Sie die Ziel-vApp aus und klicken Sie auf **Weiter**.
- 5 Konfigurieren Sie die Ressourcen, wie z. B. den Namen der virtuellen Maschine und den Computernamen sowie optional die Speicherrichtlinie und die Netzwerkkarten, und klicken Sie auf **Weiter**.

Wichtig Der Computernamen darf nur alphanumerische Zeichen und Bindestriche enthalten. Er darf nur aus Ziffern bestehen und darf keine Leerzeichen enthalten.

- 6 Überprüfen Sie auf der Seite **Bereit zum Abschließen** Ihre Einstellungen und klicken Sie auf **Fertig**.

Affinität und Anti-Affinität virtueller Maschinen

Mit Affinitäts- und Anti-Affinitätsregeln können Sie eine Gruppe virtueller Maschinen auf verschiedene ESXi-Hosts verteilen oder eine Gruppe virtueller Maschinen auf einem bestimmten Host beibehalten.

Eine Affinitätsregel platziert eine Gruppe virtueller Maschinen auf einem bestimmten Host, sodass Sie die Nutzung dieser virtuellen Maschinen problemlos überwachen können. Eine Anti-Affinitätsregel platziert eine Gruppe virtueller Maschinen auf verschiedenen Hosts, wodurch der gleichzeitige Ausfall aller virtuellen Maschinen beim Ausfall eines einzelnen Hosts verhindert wird.

Affinitäts- und Anti-Affinitätsregeln sind entweder erforderlich oder bevorzugt.

Erforderliche Regel

Wenn die Affinitäts- oder Anti-Affinitätsregeln nicht erfüllt werden können, werden die virtuellen Maschinen, die der Regel hinzugefügt wurden, nicht eingeschaltet.

Bevorzugte Regel

Wenn gegen die Affinitäts- oder Anti-Affinitätsregeln verstoßen wurde, werden die virtuellen Maschinen durch den Cluster oder den Host weiterhin eingeschaltet.

Beispiel: Wenn eine Anti-Affinitätsregel zwischen zwei virtuellen Maschinen eingerichtet ist, aber nur ein physischer Host verfügbar ist, gestattet eine erforderliche Regel (starke Affinität) nicht, dass beide virtuellen Maschinen eingeschaltet werden. Wenn es sich um eine bevorzugte Anti-Affinitätsregel handelt (schwache Affinität), dürfen beide virtuelle Maschinen eingeschaltet werden.

Verwandte Videos




VM-VM-Affinität in vCloud Director

(https://vmwaretv.vmware.com/media/t/1_we23vrud)

Anzeigen von Affinitäts- und Anti-Affinitätsregeln

Sie können vorhandene Affinitäts- und Anti-Affinitätsregeln und zugehörige Eigenschaften wie z. B. die von den Regeln betroffenen virtuellen Maschinen anzeigen und ob die Regeln aktiviert sind.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Affinitätsregeln** aus.
- 2 (Optional) Klicken Sie auf das **Raster-Editor**-Symbol () und wählen Sie aus, welche Details zu den Regeln angezeigt werden sollen.

Ergebnisse

Sie sehen die Liste der vorhandenen Affinitäts- und Anti-Affinitätsregeln, ob diese erforderlich sind oder nicht, virtuelle Maschinen und den Aktivierungsstatus jeder Regel.

Erstellen einer Affinitätsregel

Erstellen Sie eine Affinitätsregel, um eine bestimmte Gruppe virtueller Maschinen auf einem einzelnen Host zu platzieren, sodass Sie die Nutzung dieser virtuellen Maschinen überwachen können.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Affinitätsregeln** aus.

- 2 Klicken Sie unter **Affinitätsregeln** auf **Neu**.
- 3 Geben Sie einen Namen für die Regel ein.
- 4 Deaktivieren Sie das Kontrollkästchen **Aktiviert** auf, um die Regel zu erstellen, ohne sie zu aktivieren.

Standardmäßig ist das Kontrollkästchen aktiviert, und die Regeln werden nach deren Erstellung aktiviert.

- 5 Deaktivieren Sie die Option **Erforderlich**, um eine bevorzugte Regel zu erstellen, was bedeutet, dass die der Regel hinzugefügten virtuellen Maschinen eingeschaltet sind, auch wenn gegen die Regel verstoßen wird.

Standardmäßig ist das Kontrollkästchen aktiviert, und die Regel ist erforderlich. Wenn die Regel nicht erfüllt werden kann, werden die der Regel hinzugefügten virtuellen Maschinen nicht eingeschaltet.

- 6 Wählen Sie die virtuellen Maschinen aus, die Sie der Affinitätsregel hinzufügen möchten.
- 7 Klicken Sie auf **Speichern**.

Ergebnisse

vCloud Director platziert die virtuellen Maschinen, die der Affinitätsregel zugeordnet sind, auf einem einzelnen Host.

Erstellen einer Anti-Affinitätsregel

Erstellen Sie eine Anti-Affinitätsregel zum Platzieren einer bestimmten Gruppe virtueller Maschinen auf mehreren Hosts, um einen gleichzeitigen Ausfall dieser virtuellen Maschinen beim Ausfall eines einzelnen Hosts zu verhindern.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Affinitätsregeln** aus.
- 2 Klicken Sie unter **Anti-Affinitätsregeln** auf **Neu**.
- 3 Geben Sie einen Namen für die Regel ein.
- 4 Deaktivieren Sie das Kontrollkästchen **Aktiviert** auf, um die Regel zu erstellen, ohne sie zu aktivieren.

Standardmäßig ist das Kontrollkästchen aktiviert, und die Regeln werden nach deren Erstellung aktiviert.

- 5 Deaktivieren Sie die Option **Erforderlich**, um eine bevorzugte Regel zu erstellen, und aktivieren Sie den Cluster zum Einschalten der virtuellen Maschinen, selbst wenn die Regel verletzt wird.

Standardmäßig ist das Kontrollkästchen aktiviert, und die Regel ist erforderlich. Wenn die Regel nicht erfüllt werden kann, werden die der Regel hinzugefügten virtuellen Maschinen nicht eingeschaltet.

- 6 Wählen Sie die virtuellen Maschinen aus, die der Anti-Affinitäts-Regel hinzugefügt werden sollen.
- 7 Klicken Sie auf **Speichern**.

Ergebnisse

vCloud Director platziert die virtuellen Maschinen, die der Anti-Affinitätsregel zugeordnet sind, auf mehreren Hosts.

Bearbeiten einer Affinitäts- oder Anti-Affinitätsregel

Sie können eine Affinitäts- oder Anti-Affinitätsregel bearbeiten, um die Regel zu aktivieren oder zu deaktivieren, virtuelle Maschinen hinzuzufügen oder zu entfernen, den Regelnamen oder die Regeleinstellung zu ändern.

Voraussetzungen

Für diesen Vorgang ist das Recht `Organization vDC: VM-VM Affinity Edit` erforderlich. Dieses Recht ist in den vordefinierten Rollen **Katalogautor**, **vApp-Autor** und **Organisationsadministrator** enthalten.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Affinitätsregeln** aus.
- 2 Klicken Sie auf das Optionsfeld neben dem Namen der zu bearbeitenden Regel und klicken Sie auf **Bearbeiten**.
- 3 Bearbeiten Sie die Eigenschaften der Regel.
 - a Ändern Sie den Namen der Regel nach Bedarf.
 - b Wählen Sie aus, ob die Regel aktiviert oder deaktiviert werden soll.
 - c Wählen Sie aus, ob die Regel benötigt oder bevorzugt werden soll.
 - d Fügen Sie weitere virtuelle Maschinen hinzu oder entfernen Sie virtuelle Maschinen.
- 4 Klicken Sie auf **Speichern**.

Löschen einer Affinitäts- oder Anti-Affinitätsregel

Wenn Sie keine Affinitäts- oder Anti-Affinitätsregel mehr verwenden möchten, können Sie sie löschen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Affinitätsregeln** aus.
- 2 Klicken Sie auf das Optionsfeld neben dem Namen der zu löschenden Regel und klicken Sie auf **Löschen**.
- 3 Um zu bestätigen, dass Sie die Regel löschen möchten, klicken Sie auf **OK**.

Ergebnisse

vCloud Director löscht die Affinitäts- oder Anti-Affinitätsregel.

Überwachen von virtuellen Maschinen


Wenn Ihr vCloud Director-Administrator die Funktion zur Überwachung virtueller Maschinen aktiviert hat, können Sie das Überwachungsdiagramm über das Mandantenportal anzeigen.

Verwenden Sie diese Funktion, um den Status einer bestimmten virtuellen Maschine für einen bestimmten Zeitraum (Tage, Wochen oder Monate) zu analysieren.

Voraussetzungen

Diese Funktion ist nur verfügbar, wenn sie von Ihrem vCloud Director-Administrator aktiviert wurde.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie die virtuelle Maschine aus, die Sie überwachen möchten, und klicken Sie auf **Details**.
- 4 Klicken Sie auf **Überwachungsdiagramm**, um die Überwachungsansicht zu erweitern.
Das Überwachungsdiagramm wird angezeigt.

5

6 Wählen Sie eine Metrikooption zum Überwachen von virtuellen Maschinen aus.

Die Liste im Dropdown-Menü **Metrik** variiert je nach Auswahl Ihres **Systemadministrators**. Es werden Ihnen einige oder alle Optionen angezeigt.

Metrik	Beschreibung
Neueste bereitgestellte Festplatte	In KB angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.
Durchschnittliche Datenträger-Lesevorgänge	Wird als Prozentsatz angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.
Durchschnittliche Datenträger-Schreibvorgänge	Wird als Prozentsatz angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.
Durchschnittliche CPU-Auslastung	Wird als Prozentsatz angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.
Durchschnittliche CPU-Auslastung (in MHz)	In MHz angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.
Maximale CPU-Auslastung	Wird als Prozentsatz angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.
Durchschnittliche Speichernutzung	Wird als Prozentsatz angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.
Zuletzt verwendeter Datenträger	In KB angegeben. Aus Tages-, Wochen- oder Monatsansicht auswählen.

Jedes Mal, wenn Sie einen anderen Wert aus der Liste auswählen, wird ein neues Diagramm angezeigt.

7 (Optional) Ändern Sie den Zeitrahmen für die Metrikerfassung.

8 Klicken Sie auf **Aktualisieren**.

9 Klicken Sie zum Speichern der Änderungen auf **Speichern**.

Arbeiten mit Snapshots

Beim Erstellen eines Snapshots werden der gesamte Status und alle Daten der virtuellen Maschine zum Zeitpunkt der Snapshot-Erstellung erfasst. Die virtuelle Maschine ist von der Erstellung eines Snapshots nicht betroffen. Es wird lediglich ein Image der virtuellen Maschine in einem bestimmten Zustand kopiert und gespeichert. Snapshots sind hilfreich, wenn Sie wiederholt zu einem bestimmten Status der virtuellen Maschine zurückkehren müssen, aber nicht mehrere virtuelle Maschinen erstellen möchten.

Snapshots sind als kurzfristige Lösung zum Testen der Software mit unbekannten oder potenziell gefährlichen Auswirkungen hilfreich. Sie können einen Snapshot während eines linearen oder iterativen Prozesses als Wiederherstellungspunkt nutzen, beispielsweise beim Installieren von Update-Paketen oder während eines Verzweigungsprozesses, z. B. beim Installieren verschiedener Versionen eines Programms.

Sie können einen Snapshot beispielsweise verwenden, wenn Sie ein Upgrade des Betriebssystems einer virtuellen Maschinen durchführen. Bevor Sie das Upgrade der virtuellen Maschine durchführen, erstellen Sie beispielsweise einen Snapshot zum Beibehalten des Zeitpunkts vor dem Upgrade. Wenn während des Upgrades keine Probleme auftreten, können Sie den Snapshot entfernen. Damit werden die während des Upgrades vorgenommenen Änderungen übernommen. Wenn ein Problem aufgetreten ist, können Sie den Snapshot wiederherstellen und somit zu dem gespeicherten Zustand der virtuellen Maschine vor dem Upgrade zurückkehren.

Mit vCloud Director können Sie nur über einen einzigen Snapshot einer virtuellen Maschine verfügen. Durch jeden Versuch, einen neuen Snapshot einer virtuellen Maschine zu erstellen, wird der vorherige gelöscht.

Erstellen eines Snapshots einer virtuellen Maschine


Sie können einen Snapshot einer virtuellen Maschine erstellen. Nach dem Erstellen des Snapshots können Sie für die virtuelle Maschine den Snapshot wiederherstellen oder den Snapshot entfernen.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Maschine nicht mit einem unabhängigen Datenträger verbunden ist.

Hinweis Snapshots erfassen keine NIC-Konfigurationen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, für die Sie einen Snapshot erstellen möchten, die Option **Snapshot erstellen** aus.

Beim Erstellen eines Snapshots einer virtuellen Maschine wird der vorhandene Snapshot (sofern zutreffend) ersetzt.

- 4 (Optional) Wählen Sie aus, ob ein Snapshot des Arbeitsspeichers der virtuellen Maschine erstellt werden soll.

Wenn Sie den Speicherstatus einer virtuellen Maschine erfassen, behält der Snapshot den Live-Status der virtuellen Maschine bei. Mit Arbeitsspeicher-Snapshots wird ein Snapshot zu einem genau bestimmten Zeitpunkt erstellt, um beispielsweise ein Upgrade einer Software durchzuführen, die noch ausgeführt wird. Wenn Sie einen Arbeitsspeicher-Snapshot erstellen und das Upgrade nicht wie erwartet abgeschlossen wird oder die Software nicht Ihren Erwartungen entspricht, können Sie die virtuelle Maschine in ihrem vorherigen Zustand wiederherstellen.

Wenn Sie den Speicherstatus erfassen, müssen die Dateien der virtuellen Maschine nicht stillgelegt werden. Falls Sie den Speicherstatus nicht erfassen, wird der Live-Status der virtuellen Maschine vom Snapshot nicht gespeichert und die Festplatten sind absturzkonsistent, wenn sie nicht stillgelegt werden.

- 5 (Optional) Wählen Sie aus, ob das Gastdateisystem stillgelegt werden soll.

Für diesen Vorgang ist es erforderlich, dass VMware Tools auf der virtuellen Maschine installiert ist. Beim Stilllegen einer virtuellen Maschine legt VMware Tools das Dateisystem der virtuellen Maschine still. Ein Stilllegungsvorgang stellt sicher, dass eine Snapshot-Festplatte einen konsistenten Status der Gastdateisysteme darstellt. Stillgelegte Snapshots sind für automatisierte oder regelmäßige Sicherungen geeignet. Wenn Sie beispielsweise keine Informationen zu den Vorgängen der virtuellen Maschine haben, aber über mehrere kürzlich erstellte Sicherungen verfügen möchten, die Sie wiederherstellen können, können Sie die Dateiaktivitäten stilllegen.

Virtuelle Maschinen, die über Festplatten mit hoher Kapazität verfügen, können nicht stillgelegt werden.

- 6 Klicken Sie auf **OK**.

Ergebnisse

Mit dem Snapshot können Sie Ihre virtuelle Maschine auf den neuesten Snapshot zurücksetzen.

Zurücksetzen einer virtuellen Maschine auf einen Snapshot


Sie können eine virtuelle Maschine auf den Zustand zurücksetzen, den sie hatte, als der Snapshot erstellt wurde.

Voraussetzungen

Die virtuelle Quellmaschine hat einen Snapshot.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.

- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, für die Sie einen Snapshot wiederherstellen möchten, die Option **Snapshot wiederherstellen** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Die virtuelle Maschine wird auf den gespeicherten Snapshot zurückgesetzt.

Entfernen eines Snapshots einer virtuellen Maschine


Sie können einen Snapshot aus einer virtuellen Maschine entfernen.

Wenn Sie einen Snapshot entfernen, löschen Sie den Zustand der virtuellen Maschine, die Sie beibehalten haben. Im Anschluss daran können Sie nicht mehr zu diesem Zustand zurückkehren. Das Entfernen eines Snapshots wirkt sich nicht auf den aktuellen Zustand der virtuellen Maschine aus.

Voraussetzungen

Eine virtuelle Maschine mit einem gespeicherten Snapshot.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, für die Sie den Snapshot entfernen möchten, die Option **Snapshot entfernen** aus.
- 4 Klicken Sie auf **OK**.


Verlängern des Lease einer virtuellen Maschine

Sie können die Lease einer virtuellen Maschine verlängern, falls sie in Kürze abläuft.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, deren Lease abläuft, die Option **Lease verlängern** aus.

Ergebnisse

Der Lease wird verlängert. Der neue Lease-Zeitrahmen wird im Feld **Lease** angezeigt.


Löschen einer virtuellen Maschine

Sie können eine virtuelle Maschine aus Ihrer Organisation löschen.

Voraussetzungen

Die virtuelle Maschine muss ausgeschaltet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf  um die Liste in einer Kartenansicht anzuzeigen und optional die Liste der virtuellen Maschinen aus dem Dropdown-Menü **Nachsehen in** zu filtern.
- 3 Wählen Sie im Menü **Aktionen** der virtuellen Maschine, die Sie löschen möchten, die Option **Löschen** aus.
- 4 Bestätigen Sie den Löschvorgang.

Ergebnisse

Die virtuelle Maschine wird gelöscht.

Arbeiten mit vApps

3

Eine vApp besteht aus einer oder mehreren virtuellen Maschinen, die über ein Netzwerk kommunizieren und Ressourcen und Dienste in einer bereitgestellten Umgebung verwenden. Eine vApp kann mehrere virtuelle Maschinen enthalten.

Ab vCloud Director 9.5 unterstützen vApps IPv6-Konnektivität. Sie können IPv6-Adressen virtuellen Maschinen zuweisen, die mit IPv6-Netzwerken verbunden sind.

Wichtig Alle Schritte für das Arbeiten mit vApps werden in der Kartenansicht dokumentiert, wobei davon ausgegangen wird, dass Sie über mehrere Datacenter verfügen. Es ist auch möglich, die gleichen Verfahren über die Rasteransicht durchzuführen. Die Schritte können jedoch geringfügig variieren.

Dieses Kapitel enthält die folgenden Themen:





- [Anzeigen von vApps](#)
- [Erstellen einer neuen vApp](#)
- [Erstellen einer vApp von einem OVF-Paket aus](#)
- [Erstellen einer vApp aus einer vApp-Vorlage](#)
- [Öffnen einer vApp](#)
- [Ausführen von Energievorgängen auf vApps](#)
- [vApp-Eigenschaften bearbeiten](#)
- [Anzeigen eines vApp-Netzwerkdigramms](#)
- [Arbeiten mit Netzwerken in einer vApp](#)
- [Arbeiten mit Snapshots](#)
- [Ändern des Besitzers einer vApp](#)
- [Verschieben einer vApp in ein anderes virtuelles Datacenter](#)
- [Kopieren einer beendeten vApp in ein anderes virtuelles Datacenter](#)
- [Kopieren einer eingeschalteten vApp](#)
- [Hinzufügen einer virtuellen Maschine zu einer vApp](#)
- [Speichern einer vApp als vApp-Vorlage in einem Katalog](#)

- [Herunterladen einer vApp als OVF-Paket](#)
- [Verlängern eines vApp-Lease](#)
- [Löschen einer vApp](#)

Anzeigen von vApps

Sie können vApps in einer Rasteransicht oder in einer Kartenansicht anzeigen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Um die vApps in einer Rasteransicht anzuzeigen, klicken Sie auf . Um sie in einer Kartenansicht anzuzeigen, klicken Sie auf . Die Liste der vApps wird in einem Raster oder als eine Liste mit Karten angezeigt.
- 3 (Optional) Konfigurieren Sie die Rasteransicht so, dass sie die gewünschten Details enthält.
 - a Klicken Sie in der Rasteransicht auf das **Raster-Editor**-Symbol ().
 - b Wählen Sie die vApp-Details aus, die in der Rasteransicht enthalten sein sollen, indem Sie die Kontrollkästchen neben den gewünschten Details aktivieren. Die ausgewählten Details werden als Spalten für jede vApp angezeigt.
- 4 (Optional) Klicken Sie in der Rasteransicht auf der linken Seite einer vApp auf , um die Aktionen anzuzeigen, die Sie für die ausgewählte vApp durchführen können. Beispielsweise können Sie eine vApp herunterfahren.

Erstellen einer neuen vApp

Statt eine vApp auf der Basis einer vApp-Vorlage zu erstellen, können Sie mithilfe von virtuellen Maschinen eine neue vApp aus Katalogen und/oder neuen virtuellen Maschinen erstellen.

Beim Erstellen einer vApp müssen Sie einen Namen und optional eine Beschreibung der vApp angeben. Sie können zurückkehren und die virtuellen Maschinen zu einem späteren Zeitpunkt der vApp hinzufügen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf **Neue vApp**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für die vApp ein.
- 4 (Optional) Suchen Sie im Katalog nach virtuellen Maschinen, die zu dieser vApp hinzugefügt werden sollen, oder fügen Sie eine neue, leere virtuelle Maschine hinzu, indem Sie auf **Virtuelle Maschine hinzufügen** klicken.

Wenn es keine virtuellen Maschinen im Katalog gibt, erstellen Sie eine virtuelle Maschine und fügen Sie sie der vApp hinzu.

- a Geben Sie den Namen und den Computernamen für die virtuelle Maschine an.

Wichtig Der Computernamen darf nur alphanumerische Zeichen und Bindestriche enthalten. Ein Computernamen darf nur aus Ziffern bestehen und darf keine Leerzeichen enthalten.

- b (Optional) Geben Sie eine aussagekräftige Beschreibung ein.

- c Wählen Sie aus, wie die virtuelle Maschine bereitgestellt werden soll.

Option	Aktion
Neu	<p>Sie stellen eine neue virtuelle Maschine mit anpassbaren Einstellungen bereit.</p> <ol style="list-style-type: none"> 1 Wählen Sie eine Betriebssystemfamilie und ein Betriebssystem aus. 2 (Optional) Wählen Sie ein Boot-Image aus. 3 Wählen Sie die Computing-Richtlinie aus. 4 Wählen Sie die Größe der virtuellen Maschine aus oder klicken Sie auf Benutzerdefinierte Größenänderungsoptionen, um die Computing-, Arbeitsspeicher- und Speichereinstellungen manuell einzugeben. <p>Die vordefinierten Größen der virtuellen Maschine sind klein, mittel oder groß.</p> <ol style="list-style-type: none"> 5 Geben Sie die Speicheroptionen an, z. B. Speicherrichtlinie und Größe in GB. 6 Geben Sie die Netzwerkeinstellungen für die virtuelle Maschine an, z. B. Netzwerk, IP-Modus, IP-Adresse und primäre Netzwerkkarte.
Aus Vorlage	<p>Sie stellen eine virtuelle Maschine anhand einer Vorlage bereit, die Sie aus dem Vorlagenkatalog auswählen.</p> <ol style="list-style-type: none"> 1 Wählen Sie die VM-Vorlage aus dem Katalog aus. 2 (Optional) Geben Sie an, dass eine benutzerdefinierte Speicherrichtlinie verwendet werden soll, und wählen Sie die Richtlinie unter Zu verwendende benutzerdefinierte Speicherrichtlinie aus. 3 Wenn Nutzungsbedingungen verfügbar sind, müssen Sie diese überprüfen und akzeptieren.

- d Zum Hinzufügen der virtuellen Maschine zur vApp klicken Sie auf **OK**.

Die dem Katalog hinzugefügte virtuelle Maschine wird angezeigt.

- 5 (Optional) Wiederholen Sie [Schritt 4](#) für jede weitere virtuelle Maschine, die Sie in der vApp erstellen möchten.
- 6 Um die Erstellung der vApp abzuschließen, klicken Sie auf **Erstellen**.

Ergebnisse

Die vApp wird erstellt und befindet sich im ausgeschalteten Zustand. Wenn Sie die vApp einschalten, werden die virtuellen Maschinen darin erstellt und auch eingeschaltet.

Erstellen einer vApp von einem OVF-Paket aus

Sie können eine vApp erstellen und direkt über ein OVF-Paket bereitstellen, ohne eine vApp-Vorlage und das entsprechende Katalogelement erstellen zu müssen.


Voraussetzungen

Stellen Sie sicher, dass Sie über ein OVF-Paket zum Hochladen sowie über die Berechtigung verfügen, OVF-Pakete hochzuladen und vApps bereitzustellen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.

- 2 Klicken Sie auf **vApp aus OVF hinzufügen**.

- 3 Klicken Sie auf die Schaltfläche **Hochladen** () , um zu einem Speicherort zu gelangen, der von Ihrem Computer aus zugänglich ist, und wählen Sie die OVF/OVA-Vorlagendatei aus.

Der Speicherort kann Ihre lokale Festplatte, eine Netzwerkfreigabe oder ein CD/DVD-Laufwerk sein. Zu den unterstützten Dateierweiterungen gehören `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` und `.strings`. Wenn Sie eine OVF-Datei hochladen möchten, die mehr Dateien referenziert, als Sie hochladen möchten (z. B. eine VMDK-Datei), müssen Sie alle Dateien durchsuchen und auswählen.

- 4 Klicken Sie auf **Weiter**.

- 5 Überprüfen Sie die Details der OVF/OVA-Vorlage, die Sie bereitstellen möchten, und klicken Sie auf **Weiter**.

- 6 Geben Sie einen Namen und optional eine Beschreibung für die vApp ein und klicken Sie auf **Weiter**.

- 7 (Optional) Ändern Sie den Computernamen der vApp so, dass er nur alphanumerische Zeichen enthält.

Dieser Schritt ist nur dann erforderlich, wenn der Name der vApp Leerzeichen oder Sonderzeichen enthält. Standardmäßig ist der Computernamen bereits mit dem Namen der virtuellen Maschine ausgefüllt. Computernamen dürfen jedoch nur alphanumerische Zeichen enthalten.

- 8 Wählen Sie im Dropdown-Menü **Speicherrichtlinie** eine Speicherrichtlinie für jede der virtuellen Maschinen in der vApp aus und klicken Sie auf **Weiter**.

- 9 Wählen Sie die Netzwerke aus, mit denen jede virtuelle Maschine verbunden werden soll.

- Wählen Sie aus dem Dropdown-Menü **Netzwerk** ein Netzwerk für jede virtuelle Maschine aus.
- Sie können das Kontrollkästchen **Zum Workflow für erweiterte Netzwerke wechseln** aktivieren und die Netzwerkeinstellungen wie z. B. primärer Netzwerkadapter, Netzwerkadapbertyp, Netzwerk, IP-Zuweisung und IP-Adresseinstellungen für jede virtuelle Maschine in der vApp manuell eingeben.

Sie können weitere Eigenschaften für virtuelle Maschinen konfigurieren, nachdem Sie den Assistenten beendet haben.

- 10 Klicken Sie auf **Weiter**.

- 11 Passen Sie die Hardware der virtuellen Maschinen in der vApp an und klicken Sie auf **Weiter**.

Option	Beschreibung
Anzahl der virtuellen CPUs	Geben Sie die Anzahl virtueller CPUs für jede virtuelle Maschine in der vApp ein. Die maximale Anzahl von virtuellen CPUs, die Sie einer virtuellen Maschine zuweisen können, hängt von der Anzahl der logischen CPUs auf dem Host und dem Typ des Gastbetriebssystems ab, das auf der virtuellen Maschine installiert ist.
Kerne pro Socket	Geben Sie die Anzahl der Kerne pro Socket für jede virtuelle Maschine in der vApp ein. Sie können konfigurieren, wie die virtuellen CPUs in Bezug auf die Kerne und die Kerne pro Socket zugewiesen werden. Legen Sie die gewünschte Anzahl der CPU-Kerne in der virtuellen Maschine fest und wählen Sie anschließend die gewünschte Anzahl der Kerne in jedem Socket aus, je nachdem, ob Sie eine Single-Core-CPU, Dual-Core-CPU, Tri-Core-CPU usw. haben möchten.
Anzahl der Kerne	Zeigen Sie die Anzahl der Kerne für jede virtuelle Maschine in der vApp an. Die Anzahl ändert sich, wenn Sie die Anzahl der virtuellen CPUs aktualisieren.
Arbeitsspeicher gesamt (MB)	Geben Sie den Arbeitsspeicher in MB für jede virtuelle Maschine in der vApp ein. Diese Einstellung bestimmt, wie viel Arbeitsspeicher des ESXi-Hosts der virtuellen Maschine zugeteilt wird. Die Arbeitsspeichergröße der virtuellen Hardware legt fest, wie viel Arbeitsspeicher für die in der virtuellen Maschine ausgeführten Anwendungen verfügbar ist. Eine virtuelle Maschine kann Arbeitsspeicherressourcen nur in dem Umfang nutzen, der für die virtuelle Hardware konfiguriert wurde.

- 12 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Einstellungen und klicken Sie auf **Fertigstellen**.

Ergebnisse

Die neue vApp wird in der Kartenansicht angezeigt.

Erstellen einer vApp aus einer vApp-Vorlage

Sie können eine neue vApp auf der Basis einer vApp-Vorlage erstellen, die in einem Katalog gespeichert ist, auf den Sie Zugriff haben.


Wenn die vApp-Vorlage auf einer OVF-Datei basiert, die OVF-Eigenschaften zur Anpassung ihrer virtuellen Maschinen einschließt, werden diese Eigenschaften an die vApp weitergereicht. Sofern diese Eigenschaften vom Benutzer konfigurierbar sind, können Sie die Werte angeben.

Voraussetzungen


- Lediglich Organisationsadministratoren und vApp-Autoren können auf vApp-Vorlagen in öffentlichen Katalogen zugreifen.

- vApp-Benutzer und Benutzer mit weitergehenden Berechtigungen können auf vApp-Vorlagen in Organisationskatalogen zugreifen, die ihnen zur gemeinsamen Nutzung zur Verfügung stehen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **vApp-Vorlagen** aus.

Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf die Listenleiste () links neben der als vApp bereitzustellenden vApp-Vorlage und wählen Sie **vApp erstellen** aus.
- 3 Lesen Sie auf der Seite **Lizenzen akzeptieren** des Assistenten die Nutzungsbedingungen und klicken Sie auf **Akzeptieren**.
- 4 Klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung der vApp ein.
- 6 Geben Sie in Stunden oder Tagen an, wie lange diese vApp ausgeführt werden kann, bevor sie automatisch beendet wird.
- 7 Geben Sie in Stunden oder Tagen an, wie lange die beendete vApp verfügbar bleibt, bevor sie automatisch gelöscht wird.
- 8 Klicken Sie auf **Weiter**.
- 9 Wählen Sie das virtuelle Datacenter aus, in dem Sie die vApp erstellen möchten.
- 10 Wählen Sie eine Speicherrichtlinie aus.
- 11 Klicken Sie auf **Weiter**.
- 12 Wählen Sie die Netzwerke aus, mit denen jede virtuelle Maschine verbunden werden soll.
 - Wählen Sie aus dem Dropdown-Menü **Netzwerk** ein Netzwerk für jede virtuelle Maschine aus.
 - Sie können das Kontrollkästchen **Zum Workflow für erweiterte Netzwerke wechseln** aktivieren und die Netzwerkeinstellungen wie z. B. primärer Netzwerkadapter, Netzwerkadapbertyp, Netzwerk, IP-Zuweisung und IP-Adresseinstellungen für jede virtuelle Maschine in der vApp manuell eingeben.

Sie können weitere Eigenschaften für virtuelle Maschinen konfigurieren, nachdem Sie den Assistenten beendet haben.
- 13 Klicken Sie auf **Weiter**.

- 14 Passen Sie die Hardware der virtuellen Maschinen in der vApp an und klicken Sie auf **Weiter**.

Option	Beschreibung
Anzahl der virtuellen CPUs	Geben Sie die Anzahl virtueller CPUs für jede virtuelle Maschine in der vApp ein. Die maximale Anzahl von virtuellen CPUs, die Sie einer virtuellen Maschine zuweisen können, hängt von der Anzahl der logischen CPUs auf dem Host und dem Typ des Gastbetriebssystems ab, das auf der virtuellen Maschine installiert ist.
Kerne pro Socket	Geben Sie die Anzahl der Kerne pro Socket für jede virtuelle Maschine in der vApp ein. Sie können konfigurieren, wie die virtuellen CPUs in Bezug auf die Kerne und die Kerne pro Socket zugewiesen werden. Legen Sie die gewünschte Anzahl der CPU-Kerne in der virtuellen Maschine fest und wählen Sie anschließend die gewünschte Anzahl der Kerne in jedem Socket aus, je nachdem, ob Sie eine Single-Core-CPU, Dual-Core-CPU, Tri-Core-CPU usw. haben möchten.
Anzahl der Kerne	Zeigen Sie die Anzahl der Kerne für jede virtuelle Maschine in der vApp an. Die Anzahl ändert sich, wenn Sie die Anzahl der virtuellen CPUs aktualisieren.
Arbeitsspeicher gesamt (MB)	Geben Sie den Arbeitsspeicher in MB für jede virtuelle Maschine in der vApp ein. Diese Einstellung bestimmt, wie viel Arbeitsspeicher des ESXi-Hosts der virtuellen Maschine zugeteilt wird. Die Arbeitsspeichergröße der virtuellen Hardware legt fest, wie viel Arbeitsspeicher für die in der virtuellen Maschine ausgeführten Anwendungen verfügbar ist. Eine virtuelle Maschine kann Arbeitsspeicherressourcen nur in dem Umfang nutzen, der für die virtuelle Hardware konfiguriert wurde.
Festplatteneigenschaften	Geben Sie die Größe der Festplatte der virtuellen Maschine in MB ein.

- 15 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Einstellungen und klicken Sie auf **Fertigstellen**.


Ergebnisse

Die neue vApp wird in der Kartenansicht angezeigt.

Öffnen einer vApp

Sie können eine vApp öffnen, um die darin enthaltenen virtuellen Maschinen und Netzwerke anzuzeigen. Sie können auch ein Diagramm anzeigen, das zeigt, wie die virtuellen Maschinen und Netzwerke verbunden sind.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

- 3 In der Kartenansicht werden allgemeine Informationen angezeigt, wie z. B. die Anzahl der der vApp zugeordneten virtuellen Maschinen, Lease-Informationen, die Gesamtanzahl der CPUs, Gesamtspeicher und Arbeitsspeicher, zugehörige Netzwerke und die Angabe, ob ein Snapshot erstellt wird.
- 4 Um die detaillierten Einstellungen einer ausgewählten vApp anzuzeigen, klicken Sie auf der vApp-Karte auf **Details**.

Ausführen von Energievorgängen auf vApps

Sie können Energievorgänge für vApps durchführen, z. B. Ein- oder Ausschalten einer vApp, Anhalten oder Zurücksetzen einer vApp.


Einschalten einer vApp

Beim Einschalten einer vApp werden alle noch nicht eingeschalteten virtuellen Maschinen in der vApp eingeschaltet.

Voraussetzungen

Sie sind mindestens vApp-Autor.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie einschalten möchten, die Option **Einschalten** aus.

Ergebnisse

Die vApp wird eingeschaltet.


Ausschalten einer vApp

Durch das Ausschalten einer vApp werden alle virtuellen Maschinen in der vApp ausgeschaltet. Sie müssen eine vApp ausschalten, bevor Sie bestimmte Aktionen ausführen können. Beispiele: die vApp zu einem Katalog hinzufügen, sie kopieren oder in ein anderes VDC verschieben.

Voraussetzungen

Die vApp muss gestartet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie anhalten möchten, die Option **Ausschalten** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Alle virtuellen Maschinen in der vApp und die vApp selbst werden ausgeschaltet.


Beenden einer vApp

Beim Beenden einer vApp werden alle virtuellen Maschinen in der vApp ausgeschaltet oder heruntergefahren. Sie müssen eine vApp beenden, bevor Sie bestimmte Aktionen ausführen können. Beispiele: die vApp zu einem Katalog hinzufügen, sie kopieren oder in ein anderes VDC verschieben.

Voraussetzungen

Die vApp muss gestartet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie beenden möchten, die Option **Beenden** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Alle virtuellen Maschinen in der vApp und die vApp selbst werden ausgeschaltet oder heruntergefahren.


Zurücksetzen einer vApp

Durch Zurücksetzen einer vApp wird der Zustand (z. B. Arbeitsspeicher und Cache) gelöscht, aber die vApp wird weiterhin ausgeführt.

Voraussetzungen

Die vApp wurde gestartet, und die darin enthaltenen virtuellen Maschinen sind eingeschaltet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie zurücksetzen möchten, die Option **Zurücksetzen** aus.

Ergebnisse

Der Zustand wird gelöscht, und die vApp wird weiterhin ausgeführt.


Anhalten einer vApp

Beim Anhalten einer vApp wird deren aktueller Zustand durch Schreiben des Arbeitsspeichers auf die Festplatte beibehalten.

Voraussetzungen

Die vApp wird ausgeführt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie anhalten möchten, die Option **Anhalten** aus.

Ergebnisse

Die vApp wird angehalten, und der Zustand wird beibehalten.


Verwerfen des Zustands „Angehalten“ einer vApp

Wenn eine vApp den Zustand „Angehalten“ aufweist und die vApp nicht mehr verwendet werden muss, können Sie den Zustand „Angehalten“ verwerfen. Durch Verwerfen des Zustands „Angehalten“ wird der Speicher entfernt, und die vApp wird ausgeschaltet.

Voraussetzungen

Die vApp muss den Zustand „Angehalten“ aufweisen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der angehaltenen vApp die Option **Zustand „Angehalten“ verwerfen** aus.

Ergebnisse

Der Zustand wird verworfen, und die vApp wird ausgeschaltet.

vApp-Eigenschaften bearbeiten

Sie können die Eigenschaften einer vorhandenen vApp bearbeiten, einschließlich des Namens und der Beschreibung der vApp, der Lease-Einstellungen, der Reihenfolge, in der die virtuellen Maschinen in der vApp gestartet werden sollen, der Freigabeeinstellungen und der Netzwerkeinstellungen.


Bearbeiten der allgemeinen Eigenschaften der vApp

Sie können den Namen, die Beschreibung und andere allgemeine Eigenschaften einer vApp prüfen und ändern.

Voraussetzungen

Stellen Sie sicher, dass die vApp ausgeschaltet ist.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie auf der Karte der ausgewählten vApp auf **Details**, um die vApp-Eigenschaften anzuzeigen und zu bearbeiten.
- 4 Überprüfen und ändern Sie die Eigenschaften wie gewünscht und klicken Sie auf **Speichern**.

Option	Aktion
Name	Geben Sie einen neuen Namen für die vApp ein.
Beschreibung	Geben Sie eine optionale Beschreibung der vApp ein.
Virtuelles Datencenter	Der Name des Datencenters, zu dem die vApp gehört.

Option	Aktion
Snapshot	Wenn ein Snapshot vorhanden ist, werden dessen Details angezeigt.
Leases	<p>Wählen Sie Erneuern aus, um den Lease zu erneuern.</p> <p>a Planen Sie die Laufzeit-Lease in Stunden oder Tagen.</p> <p>Definiert, wie lange die vApp ausgeführt werden kann, bevor sie automatisch beendet wird.</p> <p>b Planen Sie die Speicher-Lease in Stunden oder Tagen.</p> <p>Legt fest, wie lange die vApp verfügbar bleibt, bevor sie automatisch gelöscht wird.</p>

Ergebnisse

Die allgemeinen Einstellungen werden gespeichert.

Bearbeiten der erweiterten vApp-Eigenschaften


Sie können die Start- und Endreihenfolge von virtuellen Maschinen in Ihrer vApp konfigurieren. Konfigurieren Sie die Start- und Beendigungsreihenfolge, falls Sie Anwendungen in den virtuellen Maschinen installiert haben, die in einer bestimmten Reihenfolge gestartet und beendet werden müssen.

Diese Einstellungen sind nützlich, wenn Sie Ihre virtuellen Maschinen in einer bestimmten Reihenfolge starten und beenden müssen. Beispiel: Eine virtuelle Maschine enthält einen Datenbankserver, eine andere einen Anwendungsserver und die letzte einen Webserver. Damit auf die zugehörigen Funktionen korrekt ausgeführt werden, muss der Datenbankserver zuerst gestartet, werden, dann der Anwendungsserver und zuletzt der Webserver.

Voraussetzungen

Stellen Sie sicher, dass die vApp ausgeschaltet ist.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie auf der Karte der ausgewählten vApp auf **Details** und blättern Sie nach unten zu den erweiterten Eigenschaften der vApp.


- 4 Geben Sie die Start- und Beendigungsreihenfolge für jede virtuelle Maschine ein und klicken Sie auf **Speichern**.

Option	Aktion
Startreihenfolge	Geben Sie die Reihenfolge ein, in der Sie die virtuellen Maschinen starten möchten. Sie müssen einen Wert für jede Maschine in der Reihenfolge eingeben.
Startaktion	Wählen Sie die gewünschte Startaktion aus. Die Startaktion bestimmt, was mit einer virtuellen Maschine geschieht, wenn Sie die vApp starten, die sie enthält. Diese Option ist standardmäßig auf Einschalten festgelegt.
Wartezeit beim Starten	Geben Sie die Wartezeit bis zum Start ein. Die Wartezeit bis zum Start ist die Zeitdauer (in Sekunden), für die Sie warten sollten, bevor vCloud Director die nächste Maschine in der Reihenfolge startet.
Beendigungsaktion	Wählen Sie die Beendigungsaktion aus. Die Beendigungsaktion ist die Aktion, die die virtuelle Maschine ausführt, wenn Sie die vApp, die sie enthält, beenden. Wenn Sie Ausschalten auswählen, wird die VM ausgeschaltet, ohne die Aktionen beim Herunterfahren auszuführen, die die Stabilität gewährleisten (dies entspricht dem Ziehen des Netzsteckers). Wählen Sie diese Aktion aus, wenn Sie VMware Tools nicht installiert haben. Wählen Sie anderenfalls Herunterfahren aus, wodurch Stabilität beim Herunterfahren sichergestellt wird.
Wartezeit beim Beenden	Geben Sie Wartezeit bis zum Beenden ein. Die Wartezeit bis zum Beenden ist die Zeitdauer (in Sekunden), für die Sie warten sollten, bevor vCloud Director die nächste virtuelle Maschine in der Reihenfolge herunterfährt.

Freigeben einer vApp

Sie können vApps mit anderen Gruppen oder Benutzern in der Organisation gemeinsam nutzen. Die Zugriffskontrollen, die Sie festlegen, bestimmen die Vorgänge, die mit den gemeinsam genutzten vApps durchgeführt werden können.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie auf der Karte der ausgewählten vApp auf **Details** und blättern Sie nach unten zu den Freigabeeigenschaften der vApp.

- 4 Wählen Sie die Benutzer aus, mit denen Sie die vApp gemeinsam nutzen möchten, und klicken Sie auf **Speichern**.

Option	Aktion
Mit allen in der Organisation gemeinsam nutzen	<p>Wählen Sie diese Option aus, um sie für alle Benutzer in der Organisation freizugeben, und wählen Sie die Zugriffsebene aus.</p> <ul style="list-style-type: none"> ■ Um vollständige Kontrolle zu gewähren, wählen Sie Vollständige Kontrolle aus. <p>Alle Benutzer in der Organisation können eine vApp öffnen, starten und als vApp-Vorlage speichern, die Vorlage zu einem Katalog hinzufügen, den Besitzer der vApp ändern, sie in einen Katalog kopieren und Eigenschaften ändern.</p> <ul style="list-style-type: none"> ■ Wählen Sie Schreibgeschützt aus, um schreibgeschützten Zugriff zu gewähren.
Mit bestimmten Benutzern oder Gruppen gemeinsam nutzen	<p>Wählen Sie diese Option aus, um eine gemeinsame Nutzung mit von Ihnen angegebenen Benutzern festzulegen.</p> <ol style="list-style-type: none"> Wählen Sie die Namen aus dem Bereich Benutzer und Gruppen ohne Zugriff aus, um sie in den Bereich Benutzer und Gruppen mit Zugriff zu verschieben. Wählen Sie für die angegebenen Benutzer und Gruppen eine Zugriffsebene aus. <ul style="list-style-type: none"> ■ Um vollständige Kontrolle zu gewähren, wählen Sie Vollständige Kontrolle aus. <p>Benutzer mit vollständiger Kontrolle können eine vApp öffnen, starten und als vApp-Vorlage speichern, die Vorlage zu einem Katalog hinzufügen, den Besitzer der vApp ändern, sie in einen Katalog kopieren und Eigenschaften ändern.</p> <ul style="list-style-type: none"> ■ Wählen Sie Schreibgeschützt aus, um schreibgeschützten Zugriff zu gewähren.

Ergebnisse

Sie können die vApp nun mit den angegebenen Benutzern oder Gruppen gemeinsam nutzen.

Anzeigen eines vApp-Netzwerkdiagramms

Ein vApp-Netzwerkdiagramm bietet eine grafische Ansicht der virtuellen Maschinen und Netzwerke in einer vApp.

Voraussetzungen

Um das vApp-Netzwerkdiagramm anzuzeigen, muss Ihre vApp weniger als 40 virtuelle Maschinen enthalten. Wenn die vApp mehr als 40 virtuelle Maschinen enthält, ist das Diagramm nicht verfügbar.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.

- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

- 3 Klicken Sie in der Karte der ausgewählten vApp auf **Details**.

- 4 Klicken Sie auf die Registerkarte **Netzwerkdiagramm**.

Das Diagramm, das zeigt, wie die virtuellen Maschinen und die Netzwerke in der vApp verbunden sind, wird angezeigt. Ein Sternsymbol steht für einen primären Netzwerkadapter. Wenn ein Netzwerkadapter verbunden ist, ist seine Farbe grün. Ist ein Netzwerkadapter nicht verbunden, ist die Farbe weiß.

- 5 (Optional) Um die verbundenen virtuellen Maschinen und Netzwerke hervorzuheben, klicken Sie auf ein Netzwerk oder eine virtuelle Maschine.

Die verbundenen Objekte und die Verbindungen zwischen ihnen werden hervorgehoben.

Nächste Schritte

Sie können über diese Seite virtuelle Maschinen oder Netzwerke hinzufügen.

Arbeiten mit Netzwerken in einer vApp

Die virtuellen Maschinen in einer vApp können eine Verbindung zu vApp-Netzwerken (isoliert oder mit Routing) und VDC-Organisationsnetzwerken (direkt oder mit Fencing) herstellen. Sie können verschiedene Typen von Netzwerken zu einer vApp hinzufügen, um auf mehrere Netzwerkszenarien einzugehen.

Virtuelle Maschinen in der vApp können eine Verbindung zu den Netzwerken herstellen, die in einer vApp verfügbar sind. Wenn Sie eine virtuelle Maschine mit einem anderen Netzwerk verbinden möchten, müssen Sie dieses zuerst zur vApp hinzufügen.

Eine vApp kann vApp-Netzwerke und VDC-Organisationsnetzwerke enthalten. Ein vApp-Netzwerk kann isoliert oder geroutet sein. Ein isoliertes vApp-Netzwerk ist in der vApp enthalten. Sie können ein vApp-Netzwerk auch an ein VDC-Organisationsnetzwerk weiterleiten, um Konnektivität für virtuelle Maschinen außerhalb der vApp bereitzustellen. Für vApp-Netzwerke mit Routing können Sie Netzwerkdienste, z. B. Firewall und statisches Routing, konfigurieren.

Sie können eine vApp direkt mit einem VDC-Organisationsnetzwerk verbinden. Wenn Sie mehrere vApps haben, die mit demselben VDC-Organisationsnetzwerk verbundene, identische virtuelle Maschinen enthalten, und die vApps gleichzeitig starten möchten, können Sie die vApp umgrenzen. Durch das Fencing der vApp können Sie die virtuellen Maschinen ohne Konflikt durch Isolierung ihrer MAC- und IP-Adressen einschalten.

Die Netzwerke, die Sie der vApp hinzufügen, verwenden den Netzwerkpool, der dem Organisations-VDC zugeordnet ist, in dem Sie die vApp erstellt haben.

Anzeigen von vApp-Netzwerken

Sie können auf die Netzwerke in einer vApp zugreifen und sie anzeigen.

Voraussetzungen

Verfahren


- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.

- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

- 3 Klicken Sie in der Karte der ausgewählten vApp auf **Details**.

- 4 Klicken Sie auf die Registerkarte **Netzwerke**.

Die Liste der Netzwerke (sofern vorhanden) wird angezeigt. Sie können Informationen zu den einzelnen Netzwerken anzeigen, z. B. Name, Gateway, Netzmaske und Verbindung, und die IP-Adresse und NAT-Ressourcen beibehalten.

- 5 (Optional) Um die anzuzeigenden Spalten zu bearbeiten, klicken Sie auf das **Raster-Editor**-Symbol () und aktivieren oder deaktivieren Sie die Kontrollkästchen der Spalten, die angezeigt oder ausgeblendet werden sollen.

Fencing eines vApp-Netzwerks


Das Einschalten identischer virtueller Maschinen, die in verschiedenen vApps enthalten sind, kann zu einem Konflikt führen. Um das Einschalten von identischen virtuellen Maschinen in unterschiedlichen vApps ohne Konflikte zu ermöglichen, müssen Sie das Fencing der vApp durchführen.

Durch das Fencing einer vApp werden die MAC- und IP-Adressen der virtuellen Maschinen isoliert und der Verbindungstyp der VDC-Organisationsnetzwerke wird von „Direkt“ in „Mit Fencing“ geändert. Die Firewall der Netzwerke mit Fencing wird automatisch aktiviert und so konfiguriert, dass nur ausgehender Datenverkehr zulässig ist. Wenn Sie Fencing für eine vApp durchführen, können Sie auch NAT und Firewallregeln für die Netzwerke mit Fencing konfigurieren.

Voraussetzungen

- Fencing ist nur für direkte vApp-Netzwerke möglich. Wenn die vApp mehrere Netzwerke verwendet und die anderen Netzwerke beispielsweise geroutet werden, erfolgt das Fencing nur für das direkte Netzwerk.
- Die virtuellen Maschinen in der vApp, die das direkte Netzwerk nutzen, müssen angehalten werden, damit das direkte vApp-Netzwerk derzeit nicht verwendet wird.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie in der Karte der ausgewählten vApp auf **Details**.
- 4 Klicken Sie auf die Registerkarte **Netzwerke**.
- 5 Wurde für die vApp kein Fencing durchgeführt, klicken Sie auf die Schaltfläche **Bearbeiten**.
- 6 Aktivieren Sie die Option **vApp-Fencing** und klicken Sie auf **OK**.

Ergebnisse

Die IP- und MAC-Adressen der virtuellen Maschinen werden isoliert. Sie können identische virtuelle Maschinen in unterschiedlichen vApps ohne Konflikt einschalten.

Hinzufügen eines Netzwerks zu einer vApp

Sie können einer vApp ein Netzwerk hinzufügen, um das Netzwerk den virtuellen Maschinen in der vApp zur Verfügung zu stellen. Sie können einer vApp ein vApp-Netzwerk oder ein VDC-Organisationsnetzwerk hinzufügen.


Verbindungen können direkt oder per Fencing hergestellt werden. Mit der Funktion „Fencing“ können identische virtuelle Maschinen in verschiedenen vApps ohne Konflikte durch Isolation ihrer MAC- und IP-Adressen eingeschaltet werden.

Wenn Fencing aktiviert ist und die vApp eingeschaltet ist, wird ein isoliertes Netzwerk aus dem Netzwerkpool des Organisations-VDC erstellt. Ein Edge-Gateway wird erstellt und an das isolierte Netzwerk und das VDC-Organisationsnetzwerk angehängt. Der Datenverkehr von und zu den virtuellen Maschinen läuft über das Edge-Gateway, das die IP-Adresse mittels NAT und Proxy-AR übersetzt. Dadurch kann ein Router den Datenverkehr zwischen zwei Netzwerken unter Verwendung desselben IP-Bereichs weiterleiten.

Voraussetzungen

Um ein VDC-Organisationsnetzwerk hinzuzufügen, muss Ihr Administrator ein solches Netzwerk erstellt haben.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

- 3 Klicken Sie in der Karte der ausgewählten vApp auf **Aktionen** und wählen Sie **Netzwerk hinzufügen** aus.
- 4 Wählen Sie den Typ des hinzuzufügenden Netzwerks aus.

Option	Aktion
VDC-Organisationsnetzwerk	Wählen Sie ein VDC-Organisationsnetzwerk in der Liste der verfügbaren Netzwerke aus.
vApp-Netzwerk	<ol style="list-style-type: none"> a Geben Sie einen Namen und optional eine Beschreibung für das Netzwerk ein. b Geben Sie das Netzwerk-Gateway-CIDR ein. c (Optional) Geben Sie den primären und sekundären DNS und das DNS-Suffix ein. d (Optional) Wählen Sie aus, ob Gast-VLAN zugelassen wird. e (Optional) Geben Sie statische IP-Pool-Einstellungen, wie z. B. IP-Bereiche, ein. f (Optional) Um eine Verbindung mit einem VDC-Organisationsnetzwerk herstellen zu können, aktivieren Sie die Umschaltoption Verbindung mit einem VDC-Organisationsnetzwerk herstellen und wählen Sie ein Netzwerk aus der Liste aus.

- 5 Klicken Sie auf **Hinzufügen**.

Ergebnisse

Das Netzwerk wird der vApp hinzugefügt.

Nächste Schritte

Verbinden Sie eine virtuelle Maschine in der vApp mit dem Netzwerk.

Konfigurieren von Netzwerkdiensten für ein vApp-Netzwerk

Sie können für bestimmte vApp-Netzwerke Netzwerkdienste wie DHCP, Firewalls, NAT (Network Address Translation, Netzwerkadressenübersetzung) und statisches Routing konfigurieren.

Die verfügbaren Netzwerkdienste hängen vom Typ des vApp-Netzwerks ab.


Tabelle 3-1. Verfügbare Netzwerkdienste nach Netzwerktypen

vApp-Netzwerktyp	DHCP	Firewall	NAT	Statisches Routing
Direkt				
Weitergeleitet	X	X	X	X
Isoliert	X			

Anzeigen und Bearbeiten von allgemeinen Netzwerkdetails

Sie können die allgemeinen vApp-Netzwerkdetails anzeigen und bearbeiten, zum Beispiel den Namen und die Beschreibung des Netzwerks.


Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.
- 4 Klicken Sie auf der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Überprüfen Sie die Netzwerkinformationen auf der Registerkarte **Allgemein**.
- 6 Klicken Sie auf **Bearbeiten**.
- 7 Bearbeiten Sie den Namen und die Beschreibung des vApp-Netzwerks.
- 8 Klicken Sie auf **Speichern**.

Bearbeiten der Einstellungen des statischen IP-Pools eines vApp-Netzwerks

Sie können ein vApp-Netzwerk konfigurieren, um statische IP-Adressen für die virtuellen Maschinen in der vApp bereitzustellen. Ziehen Sie sie dazu aus einem statischen IP-Adressenpool.


Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.
- 4 Klicken Sie auf der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Klicken Sie auf der Registerkarte **IP-Verwaltung** auf **Statische Pools**.
- 6 Klicken Sie auf **Bearbeiten**.
- 7 Geben Sie einen IP-Bereich ein und klicken Sie auf **Hinzufügen**.
- 8 Klicken Sie auf **Speichern**.

Bearbeiten der DNS-Einstellungen eines vApp-Netzwerks

Nachdem Sie ein vApp-Netzwerk erstellt haben, können Sie die DNS-Einstellungen jederzeit anzeigen und bearbeiten.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.
- 4 Klicken Sie auf der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Klicken Sie auf der Registerkarte **IP-Verwaltung** auf **DNS**.
Die DNS-Einstellungen werden angezeigt.
- 6 Klicken Sie auf **Bearbeiten**.
- 7 Bearbeiten Sie den primären und sekundären DNS und das DNS-Suffix.
- 8 Klicken Sie auf **Speichern**.

Konfigurieren von DHCP für ein vApp-Netzwerk

Sie können bestimmte vApp-Netzwerke so konfigurieren, dass für die virtuellen Maschinen in der vApp DHCP-Dienste zur Verfügung stehen.

Wenn Sie für ein vApp-Netzwerk DHCP aktivieren, über eine Netzwerkkarte auf einer virtuellen Maschine in der vApp eine Verbindung mit diesem Netzwerk herstellen und als IP-Modus für diese Netzwerkkarte DHCP festlegen, weist vCloud Director der virtuellen Maschine beim Einschalten per DHCP eine IP-Adresse zu.

Voraussetzungen

Ein vApp-Netzwerk mit Routing oder ein isoliertes vApp-Netzwerk.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.
- 4 Klicken Sie auf der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Klicken Sie auf der Registerkarte **IP-Verwaltung** auf **DHCP**.
Der DHCP-Status wird angezeigt.
- 6 Klicken Sie auf **Bearbeiten**.

7 Klicken Sie auf **Aktiviert**.

8 Geben Sie einen Bereich von IP-Adressen in das Textfeld **IP-Pool** ein.

vCloud Director verwendet diese Adressen, um auf DHCP-Anforderungen zu antworten. Die IP-Adressbereiche für DHCP und der statische IP-Pool für das vApp-Netzwerk dürfen sich nicht überlagern.

9 Legen Sie die standardmäßige und maximale Lease-Zeit in Sekunden fest.

10 Klicken Sie auf **Speichern**.

Anzeigen der IP-Zuweisungen für das vApp-Netzwerk

Sie können die IP-Zuweisungen für die Netzwerke in Ihrer vApp überprüfen.

Verfahren

1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.

2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.

4 Klicken Sie auf der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.

5 Klicken Sie auf der Registerkarte **IP-Verwaltung** auf **IP-Zuweisungen**.

Die zugewiesenen IP-Adressen werden angezeigt.

Konfigurieren des statischen Routings für ein vApp-Netzwerk

Sie können bestimmte vApp-Netzwerke so konfigurieren, dass statische Routing-Dienste bereitgestellt werden, damit virtuelle Maschinen auf verschiedenen vApp-Netzwerken kommunizieren können.

Alle statischen Routen, die Sie erstellen, werden automatisch aktiviert.

Voraussetzungen

Ein vApp-Netzwerk mit Routing.

Verfahren

1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.

2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.

- 4 Klicken Sie auf der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Klicken Sie auf der Registerkarte **Routing** auf **Bearbeiten**.

Sie können statisches Routing für das Netzwerk aktivieren oder deaktivieren.

Hinzufügen des statischen Routings für ein vApp-Netzwerk

Sie können statische Routen zwischen zwei vApp-Netzwerken mit Routing zum selben VDC-Organisationsnetzwerk hinzufügen. Statische Routen ermöglichen den Datenverkehr zwischen den Netzwerken.


Sie können statische Routen nicht zu einem vApp-Netzwerk mit Fencing oder zwischen überlappenden Netzwerken hinzufügen. Nachdem Sie eine statische Route zu einem vApp-Netzwerk hinzugefügt haben, konfigurieren Sie die Netzwerkfirewallregeln so, dass sie Datenverkehr auf der statischen Route zulassen. Legen Sie für vApps mit statischen Routen fest, dass zugeordnete IP-Adressen bis zum Löschen der vApp oder der zugehörigen Netzwerke verwendet werden.

Statische Routen funktionieren nur, wenn die vApps ausgeführt werden, die die Routen enthalten. Wenn Sie das übergeordnete Netzwerk einer vApp ändern, eine vApp löschen oder ein vApp-Netzwerk löschen und die vApp statische Routen enthält, können diese Routen nicht funktionieren. Sie müssen sie dann manuell entfernen.

Voraussetzungen

- Zwei vApp-Netzwerke werden zum selben VDC-Organisationsnetzwerk weitergeleitet.
- Die vApp-Netzwerke befinden sich in vApps, die mindestens ein Mal gestartet wurden.
- Das statische Routing ist auf beiden vApp-Netzwerken aktiviert.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.
- 4 Klicken Sie auf der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Klicken Sie auf der Registerkarte **Routing** unter „Statisches Routing“ auf **Hinzufügen**.
Die zugewiesenen IP-Adressen werden angezeigt.
- 6 Geben Sie einen Namen für die statische Route ein.

7 Geben Sie die Netzwerkadresse im CIDR-Format ein.

Die Netzwerkadresse gilt für das vApp-Netzwerk, zu dem eine statische Route hinzugefügt werden soll.

8 Geben Sie die IP-Adresse des nächsten Hops ein.

Die IP-Adresse des nächsten Hops ist die externe IP-Adresse des Routers des vApp-Netzwerks.

9 Klicken Sie auf **Speichern**.**10** Wiederholen Sie diesen Vorgang für das zweite vApp-Netzwerk.**Beispiel: Statisches Routing – Beispiel**

vApp-Netzwerk 1 und vApp-Netzwerk 2 werden beide zum freigegebenen Organisationsnetzwerk weitergeleitet. Sie können auf jedem vApp-Netzwerk eine statische Route erstellen, um den Datenverkehr zwischen den Netzwerken zuzulassen. Sie können die statischen Routen mithilfe von Informationen über die vApp-Netzwerke erstellen.

Tabelle 3-2. Netzwerkinformationen

Netzwerkname	Netzwerkspezifikation	Externe IP-Adresse des Routers
vApp-Netzwerk 1	192.168.1.0/24	192.168.0.100
vApp-Netzwerk 2	192.168.2.0/24	192.168.0.101
Freigegebenes Organisationsnetzwerk	192.168.0.0/24	n.v.

Erstellen Sie auf vApp-Netzwerk 1 eine statische Route zu vApp-Netzwerk 2. Erstellen Sie auf vApp-Netzwerk 2 eine statische Route zu vApp-Netzwerk 1.

Tabelle 3-3. Statisches Routing – Einstellungen

vApp-Netzwerk	Name der Route	Netzwerk	IP-Adresse des nächsten Hops
vApp-Netzwerk 1	tovapp2	192.168.2.0/24	192.168.0.101
vApp-Netzwerk 2	tovapp1	192.168.1.0/24	192.168.0.100

Löschen eines vApp-Netzwerks

Wenn Sie ein Netzwerk nicht mehr in der vApp benötigen, können Sie es löschen.

Voraussetzungen

Die vApp wird angehalten, und keine der virtuellen Maschinen in der vApp ist mit dem Netzwerk verbunden.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Klicken Sie in der Karte der ausgewählten virtuellen Appliance auf **Details**.
- 4 Wählen Sie auf der Registerkarte **Netzwerke** das zu löschende Netzwerk aus, klicken Sie auf **Löschen** und bestätigen Sie den Löschvorgang.

Arbeiten mit Snapshots

Beim Erstellen eines Snapshots werden der Zustand und die Daten der virtuellen Maschinen innerhalb einer vApp zu einem bestimmten Zeitpunkt beibehalten. Ein Snapshot ist nicht für die Verwendung über einen längeren Zeitraum oder anstelle der Sicherung der vApp vorgesehen.

Sie können einen Snapshot beispielsweise verwenden, wenn Sie ein Upgrade der virtuellen Maschinen in einer vApp durchführen. Bevor Sie das Upgrade der virtuellen Maschinen durchführen, können Sie beispielsweise einen Snapshot zum Beibehalten des Zeitpunkts vor dem Upgrade erstellen. Zu diesem Zweck speichern Sie einen Snapshot vor dem Upgrade und führen dann das Upgrade durch. Wenn während des Upgrades keine Probleme auftreten, können Sie den Snapshot entfernen. Damit werden die während des Upgrades vorgenommenen Änderungen übernommen. Wenn ein Problem aufgetreten ist, können Sie den Snapshot wiederherstellen und somit zu dem gespeicherten vApp-Zustand vor dem Upgrade zurückkehren.


Erstellen eines Snapshots einer vApp

Indem Sie einen Snapshot einer vApp erstellen, erstellen Sie Snapshots von allen virtuellen Maschinen in der vApp. Nachdem Sie den Snapshot erstellt haben, können Sie alle virtuellen Maschinen in der vApp auf den Snapshot zurücksetzen oder den Snapshot entfernen, wenn Sie ihn nicht benötigen.

Für vApp-Snapshots gelten einige Einschränkungen.

- vApp-Snapshots erfassen keine NIC-Konfigurationen.
- Wenn eine virtuelle Maschine in der vApp mit einem unabhängigen Laufwerk verbunden ist, können Sie keinen vApp-Snapshot erstellen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

- 3 Wählen Sie im Menü **Aktionen** der vApp, für die Sie einen Snapshot erstellen möchten, die Option **Snapshot erstellen** aus.

Beim Erstellen eines Snapshots einer vApp wird der vorhandene Snapshot (sofern zutreffend) ersetzt.

- 4 (Optional) Wählen Sie aus, ob ein Snapshot des Arbeitsspeichers der vApp erstellt werden soll.

Wenn Sie den vApp-Arbeitsspeicherstatus erfassen, behält der Snapshot den Live-Status der vApp und der virtuellen Maschinen in der vApp bei. Mit Arbeitsspeicher-Snapshots wird ein Snapshot zu einem genau bestimmten Zeitpunkt erstellt, um beispielsweise ein Upgrade einer Software durchzuführen, die noch ausgeführt wird. Wenn Sie einen Arbeitsspeicher-Snapshot erstellen und das Upgrade nicht wie erwartet abgeschlossen wird oder die Software nicht Ihren Erwartungen entspricht, können Sie die virtuelle Maschine in ihrem vorherigen Zustand wiederherstellen.

Wenn Sie den Speicherstatus erfassen, müssen die Dateien der vApp nicht stillgelegt werden. Falls Sie den Speicherstatus nicht erfassen, wird der Live-Status der vApp vom Snapshot nicht gespeichert und die Festplatten sind absturzkonsistent, wenn sie nicht stillgelegt werden.

- 5 (Optional) Wählen Sie aus, ob das Gastdateisystem stillgelegt werden soll.

Für diesen Vorgang ist es erforderlich, dass VMware Tools auf den virtuellen Maschinen in der vApp installiert ist. Beim Stilllegen einer virtuellen Maschine legt VMware Tools das Dateisystem der virtuellen Maschine still. Ein Stilllegungsvorgang stellt sicher, dass eine Snapshot-Festplatte einen konsistenten Status der Gastdateisysteme darstellt. Stillgelegte Snapshots sind für automatisierte oder regelmäßige Sicherungen geeignet. Wenn Sie beispielsweise keine Informationen zu den Vorgängen der virtuellen Maschine haben, aber über mehrere kürzlich erstellte Sicherungen verfügen möchten, die Sie wiederherstellen können, können Sie die Dateiaktivitäten stilllegen.

vApps, die über Festplatten mit hoher Kapazität verfügen, können nicht stillgelegt werden.

- 6 Klicken Sie auf **OK**.

Ergebnisse

Ein Snapshot der vApp wird erstellt.

Nächste Schritte

Sie können alle virtuellen Maschinen in der vApp auf den neuesten Snapshot wiederherstellen.


Zurücksetzen einer vApp auf einen Snapshot

Sie können alle virtuellen Maschinen in einer vApp auf den Zustand zurücksetzen, den sie hatten, als der vApp-Snapshot erstellt wurde.

Voraussetzungen

Überprüfen Sie, ob die vApp über einen Snapshot verfügt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie zurücksetzen möchten, die Option **Snapshot wiederherstellen** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Alle virtuellen Maschinen in der vApp werden auf den Snapshot-Zustand zurückgesetzt.

Entfernen eines Snapshots einer vApp


Sie können einen Snapshot aus einer vApp entfernen.

Wenn Sie einen vApp-Snapshot entfernen, löschen Sie den Zustand der virtuellen Maschinen im vApp-Snapshot und können nicht mehr zu diesem Zustand zurückkehren. Das Entfernen eines Snapshots wirkt sich nicht auf den aktuellen Zustand der vApp aus.

Voraussetzungen

Sie haben einen Snapshot der vApp erstellt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, für die Sie einen Snapshot entfernen möchten, die Option **Snapshot entfernen** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Der Snapshot wird entfernt.


Ändern des Besitzers einer vApp

Sie können den Besitzer einer vApp ändern. Dies ist beispielsweise sinnvoll, wenn ein Besitzer einer vApp das Unternehmen verlässt oder eine andere Rolle erhält.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, deren Besitzer Sie ändern möchten, die Option **Besitzer ändern** aus.
- 4 Wählen Sie einen Benutzer aus der Liste aus.
- 5 Klicken Sie auf **OK**.

Ergebnisse

Der Besitzer der vApp wird geändert.


Verschieben einer vApp in ein anderes virtuelles Datencenter

Wenn Sie eine vApp in ein anderes virtuelles Datencenter verschieben, wird die vApp aus dem virtuellen Quelldatencenter entfernt.

Voraussetzungen

- Sie sind mindestens **vApp-Autor**.
- Ihre vApp ist ausgeschaltet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie verschieben möchten, die Option **Verschieben nach** aus.
- 4 Wählen Sie das virtuelle Datencenter aus, in das Sie die vApp verschieben möchten, und klicken Sie auf **OK**.
- 5 (Optional) Wählen Sie die Speicherrichtlinie aus.

- 6 Klicken Sie auf **OK**.

Ergebnisse

Die vApp wird aus dem Quelldatencenter entfernt und in das Zieldatencenter verschoben.


Kopieren einer beendeten vApp in ein anderes virtuelles Datencenter

Wenn Sie eine vApp in ein anderes VDC kopieren, verbleibt die ursprüngliche vApp im Quell-VDC.

Voraussetzungen

- Sie sind mindestens **vApp-Autor**.
- Die vApp ist ausgeschaltet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie kopieren möchten, die Option **Kopieren nach** aus.
- 4 Geben Sie einen Namen und eine Beschreibung ein.
- 5 Wählen Sie das virtuelle Datencenter aus, in dem Sie die Kopie der vApp erstellen möchten.
- 6 (Optional) Wählen Sie eine Speicherrichtlinie aus.
- 7 Klicken Sie auf **OK**.

Ergebnisse

Die vApp wird mit dem von Ihnen angegebenen Namen und der Beschreibung in das angegebene virtuelle Datencenter kopiert.

Kopieren einer eingeschalteten vApp


Um eine neue vApp auf der Grundlage einer vorhandenen vApp zu erstellen, können Sie eine Kopie der vorhandenen vApp erstellen und diese Kopie an Ihre Bedürfnisse anpassen. Sie müssen die virtuellen Maschinen in der vApp nicht ausschalten, bevor Sie die vApp kopieren. Der Arbeitsspeicherzustand laufender virtueller Maschinen wird in der kopierten vApp beibehalten.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Sie sind mindestens **vApp-Benutzer**.
- Das Organisations-VDC wird von vCenter Server 5.5 oder höher unterstützt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie kopieren möchten, die Option **Kopieren nach** aus.
- 4 Geben Sie einen Namen und eine Beschreibung ein.
- 5 Wählen Sie das virtuelle Datencenter aus, in dem Sie die Kopie der vApp erstellen möchten.
- 6 (Optional) Wählen Sie eine Speicherrichtlinie aus.
- 7 Klicken Sie auf **OK**.

Ergebnisse

Eine Kopie der vApp wird erstellt, und die vApp-Kopie weist den Zustand „Angehalten“ auf. Die kopierte vApp ist für das Netzwerk-Fencing aktiviert.

Nächste Schritte

Modifizieren Sie die Netzwerkeigenschaften der neuen vApp oder schalten Sie sie ein.


Hinzufügen einer virtuellen Maschine zu einer vApp

Sie können einer vApp eine virtuelle Maschine hinzufügen.

Voraussetzungen

Sie müssen **Organisationsadministrator** oder **vApp-Autor** sein, um auf virtuelle Maschinen in öffentlichen Katalogen zugreifen zu können.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.

- 3 Wählen Sie im Menü **Aktionen** der vApp, der Sie eine virtuelle Maschine hinzufügen möchten, die Option **VM hinzufügen** aus.

Die Liste der virtuellen Maschinen, die der vApp zugeordnet sind, wird im Fenster **VM hinzufügen** angezeigt.

- 4 Um eine neue virtuelle Maschine zu erstellen und sie automatisch mit der vApp zu verknüpfen, klicken Sie auf **Virtuelle Maschine hinzufügen**.
- 5 Geben Sie den Namen und den Computernamen für die virtuelle Maschine an.

Wichtig Der Computernamen darf nur alphanumerische Zeichen und Bindestriche enthalten. Ein Computernamen darf nur aus Ziffern bestehen und darf keine Leerzeichen enthalten.

- 6 (Optional) Geben Sie eine aussagekräftige Beschreibung ein.
- 7 Wählen Sie aus, ob die virtuelle Maschine gleich nach der Erstellung eingeschaltet werden soll.
- 8 Wählen Sie aus, wie die virtuelle Maschine bereitgestellt werden soll.

Option	Aktion
Neu	<p>Sie stellen eine neue virtuelle Maschine mit anpassbaren Einstellungen bereit.</p> <ol style="list-style-type: none"> a Wählen Sie eine Betriebssystemfamilie und ein Betriebssystem aus. b (Optional) Wählen Sie ein Boot-Image aus. c Wählen Sie die Computing-Richtlinie aus. d Wählen Sie die Größe der virtuellen Maschine aus oder klicken Sie auf Benutzerdefinierte Größenänderungsoptionen, um die Computing-, Arbeitsspeicher- und Speichereinstellungen manuell einzugeben. <p>Die vordefinierten Größenänderungsoptionen sind klein, mittel oder groß.</p> <ol style="list-style-type: none"> e Geben Sie die Speichereinstellungen der virtuellen Maschine an, z. B. Speicherrichtlinie und Größe in GB. f Geben Sie die Netzwerkeinstellungen für die virtuelle Maschine an, z. B. Netzwerk, IP-Modus, IP-Adresse und primäre Netzwerkkarte.
Aus Vorlage	<p>Sie stellen eine virtuelle Maschine anhand einer Vorlage bereit, die Sie aus dem Vorlagenkatalog auswählen.</p> <ol style="list-style-type: none"> a Wählen Sie die VM-Vorlage aus dem Katalog aus. b (Optional) Geben Sie an, dass eine benutzerdefinierte Speicherrichtlinie verwendet werden soll, und wählen Sie die Richtlinie unter Zu verwendende benutzerdefinierte Speicherrichtlinie aus. c Wenn Nutzungsbedingungen verfügbar sind, müssen Sie diese überprüfen und akzeptieren.

- 9 Klicken Sie auf **OK**, um die virtuelle Maschine zu erstellen.
- 10 Klicken Sie auf **Hinzufügen**, um der vApp die virtuelle Maschine hinzuzufügen.


Speichern einer vApp als vApp-Vorlage in einem Katalog

Wenn Sie eine vApp einem Katalog hinzufügen, konvertieren Sie diese vApp in eine vApp-Vorlage.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.
- Ihre Organisation muss über einen Katalog und ein virtuelles Datacenter mit freiem Speicherplatz verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datacenter** auf die Karte des virtuellen Datacenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die zum Katalog hinzugefügt werden soll, die Option **Zu Katalog hinzufügen** aus.

Hinweis Sie können einem Katalog vApps hinzufügen, selbst wenn die zu der jeweiligen vApp gehörenden virtuellen Maschinen den Zustand „Wird ausgeführt“ aufweisen. Wenn Sie jedoch eine ausgeführte vApp auswählen, wird diese dem Katalog als vApp-Vorlage hinzugefügt, und alle virtuellen Maschinen weisen den Zustand „Angehalten“ auf.

- 4 Wählen Sie den Zielkatalog aus dem Dropdown-Menü **Katalog** aus.
- 5 Geben Sie einen Namen und optional eine Beschreibung für die vApp-Vorlage ein.
- 6 (Optional) Wählen Sie **Katalogelement überschreiben** aus, wenn das neue Katalogelement eine vorhandene vApp-Vorlage überschreiben soll, und wählen Sie das zu überschreibende Katalogelement aus.

Wenn Sie z. B. eine neue Version einer vApp in den Katalog hochladen, sollten Sie die alte Version überschreiben.

- 7 Geben Sie an, wie die Vorlage verwendet wird.

Die Einstellung wird angewendet, wenn Sie eine vApp erstellen, die auf der vApp-Vorlage basiert. Sie wird ignoriert, wenn Sie eine vApp unter Verwendung einzelner virtueller Maschinen aus dieser Vorlage erstellen.

Option	Beschreibung
Identische Kopie erstellen	Wählen Sie diese Option aus, um aus der vApp-Vorlage eine identische Kopie der vApp zu erstellen.
VM-Einstellungen anpassen	Wählen Sie diese Option aus, um die Anpassung von Einstellungen der virtuellen Maschine zu ermöglichen, wenn Sie eine vApp aus der vApp-Vorlage erstellen.

- 8 Klicken Sie auf **OK**, um die Erstellung der vApp-Vorlage abzuschließen.

Ergebnisse

Die vApp wird als vApp-Vorlage gespeichert und im angegebenen Katalog angezeigt.


Herunterladen einer vApp als OVF-Paket

Sie können eine vApp als OVF-Paket herunterladen oder als OVA, bei der es sich um eine Verteilung einer einzelnen Datei desselben OVF-Dateipakets handelt.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.
- Stellen Sie sicher, dass die vApp ausgeschaltet und nicht bereitgestellt ist.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
- 3 Wählen Sie im Menü **Aktionen** der vApp, die Sie herunterladen möchten, die Option **Herunterladen** aus.
- 4 Wählen Sie das Format aus, in dem die vApp heruntergeladen werden soll.
- 5 (Optional) Wählen Sie **Identitätsinformationen beibehalten** aus, damit die UUIDs und die MAC-Adressen der in der vApp enthaltenen virtuellen Maschinen in das heruntergeladene OVF-Paket aufgenommen werden.

Dies schränkt die Portabilität des Pakets ein und darf nur verwendet werden, wenn dies erforderlich ist.
- 6 Klicken Sie auf **OK**, um die Auswahl zu bestätigen und den Download zu starten.

Ergebnisse

Standardmäßig wird das Paket in den Ordner `Downloads` für Ihren Browser heruntergeladen.

Verlängern eines vApp-Lease

Wenn der Lease einer vApp abgelaufen ist oder demnächst abläuft, können Sie ihn verlängern.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Benutzer** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Wählen Sie die vApp aus, für die Sie den Lease verlängern möchten.
- 3 Wählen Sie im Menü **Aktionen** die Option **Lease verlängern** aus.

Ergebnisse

Der Lease wird verlängert. Der neue Lease-Zeitrahmen wird im Feld **Lease** angezeigt.

Löschen einer vApp

Sie können eine vApp löschen, wodurch sie aus der Organisation entfernt wird.

Voraussetzungen

Ihre vApp muss beendet sein.

Sie müssen mindestens **vApp-Autor** sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie untersuchen möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Wählen Sie die zu löschende vApp aus.
- 3 Wählen Sie im Menü **Aktionen** die Option **Löschen** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Die vApp wird gelöscht.

Verwalten von VDC-Organisationsnetzwerken

4

VDC-Organisationsnetzwerke werden von einem **Systemadministrator** oder **Organisationsadministrator** erstellt und Ihrem Organisations-VDC zugewiesen. Ein **Organisationsadministrator** kann Informationen zu Netzwerken anzeigen, Netzwerkdienste konfigurieren usw.

Hinweis In diesem Kapitel wird davon ausgegangen, dass Ihre zugrunde liegenden Netzwerkressourcen von NSX Data Center for vSphere gestützt werden. Für Organisations-VDCs, die von NSX-T Data Center unterstützt werden, kann nur Ihr **Dienstanbieter** VDC-Organisationsnetzwerke erstellen.

Sie können direkte, geroutete, interne oder VDC-übergreifende VDC-Organisationsnetzwerke verwenden.

Tabelle 4-1. VDC-Organisationsnetzwerktypen

Netzwerk vom Typ „Datencenter“	Beschreibung
Direkt	<p>Zugriff durch mehrere Organisations-VDCs. Zu verschiedenen Organisations-VDCs gehörende virtuelle Maschinen können sich mit diesem Netzwerk verbinden und den Datenverkehr dieses Netzwerkes sehen.</p> <p>Dieses Netzwerk stellt die direkte Layer-2-Konnektivität für virtuelle Maschinen außerhalb des Organisations-VDCs zur Verfügung. Virtuelle Maschinen außerhalb dieses Organisations-VDCs können direkt eine Verbindung zu den virtuellen Maschinen im Organisations-VDC herstellen.</p> <hr/> <p>Hinweis Nur Ihr Systemadministrator kann ein direktes VDC-Organisationsnetzwerk hinzufügen.</p> <hr/> <p>Entweder IPv4 oder IPv6 ist möglich.</p>
Isoliert (intern)	<p>Zugriff nur über dasselbe Organisations-VDC möglich. Nur virtuelle Maschinen in diesem Organisations-VDC können sich mit dem internen VDC-Organisationsnetzwerk verbinden und den Datenverkehr im internen Netzwerk sehen.</p> <p>Das isolierte VDC-Organisationsnetzwerk stellt einem Organisations-VDC ein isoliertes, privates Netzwerk bereit, mit dem sich mehrere virtuelle Maschinen und vApps verbinden können. Dieses Netzwerk bietet keine Konnektivität für virtuelle Maschinen außerhalb des Organisations-VDCs. Maschinen außerhalb des Organisations-VDCs können keine Verbindung zu den Maschinen im Organisations-VDC herstellen.</p> <p>Kann durch einen Netzwerkpool oder einen logischen NSX-T-Switch unterstützt werden.</p> <hr/> <p>Hinweis Nur Ihr Dienstleister kann NSX-T-VDC-Organisationsnetzwerke hinzufügen. Sie können ein isoliertes VDC-Organisationsnetzwerk hinzufügen, das nur von einem Netzwerkpool unterstützt wird.</p> <hr/> <p>Nur IPv4 ist möglich.</p>
Weitergeleitet	<p>Zugriff nur über dasselbe Organisations-VDC möglich. Nur virtuelle Maschinen in diesem Organisations-VDC können sich mit diesem Netzwerk verbinden.</p> <p>Dieses Netzwerk bietet auch den kontrollierten Zugriff auf ein externes Netzwerk.</p> <p>Als Systemadministrator oder Organisationsadministrator können Sie NAT-, Firewall- und VPN-Einstellungen so konfigurieren, dass der Zugriff vom externen Netzwerk auf ausgewählte virtuelle Maschinen ermöglicht wird.</p> <p>Entweder IPv4 oder IPv6 ist möglich.</p>
VDC-übergreifend	<p>Dieses Netzwerk ist Teil eines ausgeweiteten Netzwerks, das sich über eine Datencenter-Gruppe erstreckt. Eine Datencenter-Gruppe kann zwei bis vier virtuelle Organisations-Datencenter in einer vCloud Director-Bereitstellung mit einer einzigen oder mit mehreren Sites umfassen.</p> <p>Die mit diesem Netzwerk verbundenen virtuellen Maschinen sind mit dem zugrunde liegenden ausgeweiteten Netzwerk verbunden.</p> <p>Nur IPv4 ist möglich.</p> <p>Informationen zu VDC-übergreifenden Netzwerken finden Sie unter Kapitel 5 Verwalten von VDC-übergreifenden Netzwerken.</p>

Alle Schritte für die Verwaltung Ihrer VDC-Organisationsnetzwerke werden unter der Annahme dokumentiert, dass Sie über mehrere virtuelle Datencenter verfügen.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen der verfügbaren VDC-Organisationsnetzwerke](#)

- Hinzufügen eines isolierten VDC-Organisationsnetzwerks
- Hinzufügen eines VDC-Organisationsnetzwerks mit Routing
- Hinzufügen eines direkten VDC-Organisationsnetzwerks
- Bearbeiten der allgemeinen Einstellungen eines VDC-Organisationsnetzwerks
- Konvertieren eines VDC-Organisationsnetzwerks
- Konvertieren der Schnittstelle eines VDC-Organisationsnetzwerks mit Routing
- Anzeigen der für ein VDC-Organisationsnetzwerk verwendeten IP-Adressen
- Hinzufügen von IP-Adressen zum IP-Pool eines VDC-Organisationsnetzwerks
- Bearbeiten oder Entfernen von IP-Bereichen, die in einem VDC-Organisationsnetzwerk verwendet werden
- Bearbeiten der DNS-Einstellungen eines VDC-Organisationsnetzwerks
- Konfigurieren von DHCP-Einstellungen für ein isoliertes VDC-Organisationsnetzwerk
- Bearbeiten oder Löschen eines vorhandenen DHCP-Pools für ein Netzwerk
- Zurücksetzen eines VDC-Organisationsnetzwerks
- Löschen eines VDC-Organisationsnetzwerks

Anzeigen der verfügbaren VDC-Organisationsnetzwerke

Sie können die verfügbaren VDC-Organisationsnetzwerke anzeigen.

Voraussetzungen

Für diesen Vorgang sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.

Verfahren

- ◆ Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.

Ergebnisse

Ihnen wird eine Liste der verfügbaren Netzwerke angezeigt, die Sie nach Name sortieren können.

Nächste Schritte

Sie können ein neues Netzwerk hinzufügen. Sie können auch ein vorhandenes Netzwerk bearbeiten, löschen oder zurücksetzen.

Hinzufügen eines isolierten VDC-Organisationsnetzwerks

Sie können ein isoliertes VDC-Organisationsnetzwerk hinzufügen, auf das nur durch diese Organisation zugegriffen werden kann. Dieses Netzwerk bietet keine Konnektivität für virtuelle Maschinen außerhalb dieser Organisation. Virtuelle Maschinen außerhalb dieser Organisation können keine Verbindung mit den virtuellen Maschinen in der Organisation herstellen.

Sie können eine Kombination von isolierten und gerouteten VDC-Organisationsnetzwerken hinzuzufügen, um die Anforderungen Ihrer Organisation zu erfüllen. Sie können beispielsweise ein Netzwerk mit vertraulichen Informationen isolieren und gleichzeitig ein separates Netzwerk haben, das einem Edge-Gateway zugeordnet und mit dem Internet verbunden ist.

Sie können ein isoliertes VDC-Organisationsnetzwerk erstellen, das von einem Netzwerkpool unterstützt wird. Ihr Dienstanbieter kann auch ein isoliertes VDC-Netzwerk erstellen, das durch einen logischen NSX-T-Switch unterstützt wird.

Mit IPv4 können Sie nur ein isoliertes VDC-Organisationsnetzwerk erstellen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie auf der Seite **Netzwerktyp auswählen** die Option **Isoliert** aus und klicken Sie auf **Weiter**.
- 4 Geben Sie einen aussagekräftigen Namen für das VDC-Organisationsnetzwerk ein.
- 5 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das isolierte Netzwerk ein.

Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.

- 6 (Optional) Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 7 (Optional) Um das VDC-Organisationsnetzwerk für andere Organisations-VDCs innerhalb derselben Organisation verfügbar zu machen, aktivieren Sie die Option **Gemeinsam genutzt**.

Ein potenzieller Anwendungsfall für diese Option liegt vor, wenn innerhalb eines Organisations-VDC eine Anwendung vorhanden ist, für die ein Reservierungs- oder

Zuweisungspool als Zuweisungsmodell festgelegt wurde. In diesem Fall ist für die Ausführung weiterer VMs möglicherweise nicht genügend Platz vorhanden. Als Lösung können Sie ein sekundäres Organisations-VDC mit nutzungsbasierter Bezahlung erstellen und weitere VMs in diesem Netzwerk auf temporärer Basis ausführen.

Hinweis Die Organisations-VDCs müssen vom selben Provider-VDC gestützt werden.

- 8 Klicken Sie auf **Weiter**.
- 9 (Optional) Um eine oder mehrere IP-Adressen für die Zuweisung zu virtuellen Maschinen zu reservieren, die statische IP-Adressen erfordern, konfigurieren Sie die **statischen IP-Pools** für dieses Netzwerk.
 - a Geben Sie die IP-Adresse oder den Bereich der IP-Adressen ein und klicken Sie auf **Hinzufügen**.
 - b Um mehrere statische IP-Adressen oder -Bereiche hinzuzufügen, wiederholen Sie diesen Schritt.
 - c (Optional) Um IP-Adressen und Bereiche zu ändern oder zu entfernen, klicken Sie auf **Ändern** oder **Entfernen**.
- 10 Klicken Sie auf **Weiter**.
- 11 (Optional) Konfigurieren Sie die DNS-Einstellungen.

Option	Aktion
Primäres DNS	Geben Sie die IP-Adresse für den primären DNS-Server ein.
Sekundäres DNS	Geben Sie die IP-Adresse für den sekundären DNS-Server ein.
DNS-Suffix	Geben Sie das DNS-Suffix ein. Beim DNS-Suffix handelt es sich um den DNS-Namen, allerdings ohne Einbeziehung des Hostnamens.

- 12 Klicken Sie auf **Weiter**.
- 13 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die von Ihnen angegebenen Einstellungen für das VDC-Organisationsnetzwerk und klicken Sie auf **Fertigstellen**.

Hinzufügen eines VDC-Organisationsnetzwerks mit Routing

Um den Zugriff auf ein externes Netzwerk zu steuern, können Sie ein geroutetes VDC-Organisationsnetzwerk hinzufügen. **Systemadministratoren** und **Organisationsadministratoren** können NAT-, Firewall- und VPN-Einstellungen so konfigurieren, dass der Zugriff vom externen Netzwerk auf ausgewählte virtuelle Maschinen ermöglicht wird.

Sie können eine Kombination von gerouteten und isolierten VDC-Organisationsnetzwerken hinzufügen, um die Anforderungen Ihrer Organisation zu erfüllen. Beispielsweise können Sie ein Netzwerk hinzufügen, das einem Edge-Gateway zugeordnet und mit dem Internet verbunden ist, während ein isoliertes Netzwerk vertrauliche Informationen enthält.

Sie können ein geroutetes VDC-Organisationsnetzwerk mit IPv4 oder IPv6 hinzufügen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie auf der Seite **Netzwerktyp auswählen** die Option **Weitergeleitet** aus und klicken Sie auf **Weiter**.
- 4 Geben Sie einen aussagekräftigen Namen für das VDC-Organisationsnetzwerk ein.
- 5 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das geroutete VDC-Organisationsnetzwerk ein.

Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.

- 6 (Optional) Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 7 (Optional) Um das VDC-Organisationsnetzwerk für andere Organisations-VDCs innerhalb derselben Organisation verfügbar zu machen, aktivieren Sie die Option **Gemeinsam genutzt**.

Ein potenzieller Anwendungsfall liegt vor, wenn für eine Anwendung innerhalb eines Organisations-VDC ein Reservierungs- oder Zuweisungspool als Zuweisungsmodell festgelegt wurde. In diesem Fall ist für die Ausführung weiterer VMs möglicherweise nicht genügend Platz vorhanden. Als Lösung können Sie ein sekundäres Organisations-VDC mit nutzungsbasierter Bezahlung erstellen und weitere VMs in diesem Netzwerk auf temporärer Basis ausführen.

Hinweis Die Organisations-VDCs müssen denselben Netzwerkpool gemeinsam nutzen.

- 8 Klicken Sie auf **Weiter**.
- 9 Wählen Sie auf der Seite **Edge-Verbindung** ein Edge-Gateway aus, mit dem das VDC-Organisationsnetzwerk verknüpft werden soll.

Wenn das Organisations-VDC über mehrere Edge-Gateways verfügt, müssen Sie ein Edge-Gateway auswählen, mit dem dieses Netzwerk eine Verbindung herstellt. Zur Unterstützung eines weiteren gerouteten Netzwerks muss das Edge-Gateway mindestens den Wert 1 in der Spalte „Anzahl verfügbarer Netzwerke“ aufweisen.

10 Wählen Sie im Dropdown-Menü **Schnittstellentyp** den Schnittstellentyp aus.

Option	Beschreibung
Intern	Stellt eine Verbindung zu einer der internen Schnittstellen des Edge-Gateways her. Die maximal zulässige Anzahl Netzwerke ist 9.
Verteilt	Erstellt das Netzwerk auf einem Distributed Logical Router, der mit diesem Edge-Gateway verbunden ist. Die maximal zulässige Anzahl Netzwerke ist 400.
Teilschnittstelle	Erweitert ein VDC-Organisationsnetzwerk. vCloud Director ermittelt das Netzwerk, das zur Erweiterung über L2 VPN verwendet werden soll. vCloud Director erstellt mithilfe der NSX-Netzwerkvirtualisierung einen Trunk-Schnittstellentyp für dieses Netzwerk. Die maximal zulässige Anzahl Netzwerke ist 200.

11 (Optional) Um das Tagging von Gast-VLANs in diesem Netzwerk zu aktivieren, aktivieren Sie die Option **Gast-VLAN zulässig**.

12 Klicken Sie auf **Weiter**.

13 (Optional) Um eine oder mehrere IP-Adressen für die Zuweisung zu virtuellen Maschinen zu reservieren, die statische IP-Adressen erfordern, konfigurieren Sie die **statischen IP-Pools** für dieses Netzwerk.

- Geben Sie die IP-Adresse oder den Bereich der IP-Adressen ein und klicken Sie auf **Hinzufügen**.
- Um mehrere statische IP-Adressen oder -Bereiche hinzuzufügen, wiederholen Sie diesen Schritt.
- (Optional) Um IP-Adressen und Bereiche zu ändern oder zu entfernen, klicken Sie auf **Ändern** oder **Entfernen**.

14 Klicken Sie auf **Weiter**.

15 (Optional) Konfigurieren Sie die DNS-Einstellungen.

Option	Aktion
Primäres DNS	Geben Sie die IP-Adresse für den primären DNS-Server ein.
Sekundäres DNS	Geben Sie die IP-Adresse für den sekundären DNS-Server ein.
DNS-Suffix	Geben Sie das DNS-Suffix ein. Beim DNS-Suffix handelt es sich um den DNS-Namen, allerdings ohne Einbeziehung des Hostnamens.

16 Klicken Sie auf **Weiter**.

17 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die von Ihnen angegebenen Einstellungen für das VDC-Organisationsnetzwerk und klicken Sie auf **Fertigstellen**.

Hinzufügen eines direkten VDC-Organisationsnetzwerks

Um eine Verbindung mit einem externen Netzwerk über eine direkte Route herzustellen, können **Systemadministratoren** eine direkte Verbindung einrichten.

Wenn Sie sich beim vCloud Director-Mandantenportal als **Organisationsadministrator** anmelden und versuchen, ein direktes VDC-Organisationsnetzwerk zu erstellen, erhalten Sie eine Warnmeldung, die besagt, dass Sie über unzureichende Rechte verfügen.

Voraussetzungen

Dieser Vorgang ist Systemadministratoren vorbehalten.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie auf der Seite **Netzwerktyp auswählen** die Option **Direkt** aus und klicken Sie auf **Weiter**.
- 4 Geben Sie einen aussagekräftigen Namen für das VDC-Organisationsnetzwerk ein.
- 5 (Optional) Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 6 (Optional) Um das VDC-Organisationsnetzwerk für andere Organisations-VDCs innerhalb derselben Organisation verfügbar zu machen, aktivieren Sie die Option **Gemeinsam genutzt**.
- 7 Wählen Sie auf der Seite **Externe Netzwerkverbindung** das externe Netzwerk aus, zu dem das neue VDC-Organisationsnetzwerk eine direkte Verbindung herstellen soll, und klicken Sie auf **Weiter**.
- 8 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die von Ihnen angegebenen Einstellungen für das VDC-Organisationsnetzwerk und klicken Sie auf **Fertigstellen**.

Bearbeiten der allgemeinen Einstellungen eines VDC-Organisationsnetzwerks

Sie können die Eigenschaften von VDC-Organisationsnetzwerken ändern.

Voraussetzungen

Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf den Namen des VDC-Organisationsnetzwerks, das Sie anzeigen oder bearbeiten möchten.
- 3 Klicken Sie auf der Registerkarte **Allgemein** auf **Bearbeiten**.
 - a Bearbeiten Sie den Namen und die Beschreibung des Netzwerks.
 - b Aktivieren oder deaktivieren Sie die Option **Gemeinsam genutzt**, um das VDC-Organisationsnetzwerk mit anderen virtuellen Datencentern innerhalb derselben Organisation gemeinsam zu nutzen oder nicht gemeinsam zu nutzen.
- 4 Klicken Sie auf **Speichern**.

Konvertieren eines VDC-Organisationsnetzwerks

Nachdem Sie ein VDC-Organisationsnetzwerk erstellt haben, können Sie das Netzwerk von „isoliert“ in „geroutet“ und umgekehrt konvertieren.

Voraussetzungen

Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf den Namen des VDC-Organisationsnetzwerks, das Sie konvertieren möchten.
- 3 Klicken Sie auf der Registerkarte **Allgemein** auf **Bearbeiten**.
- 4 Klicken Sie auf **Verbindung**.

- 5 Um eine Verbindung mit einem Edge-Gateway herzustellen oder um das Netzwerk von allen anderen Netzwerken zu isolieren, aktivieren Sie die Option **Verbindung zu einem Edge-Gateway herstellen** oder deaktivieren Sie diese Option.

Option	Aktion
Konvertieren eines isolierten Netzwerks in ein geroutetes Netzwerk	1 Aktivieren Sie die Option Verbindung zu einem Edge-Gateway herstellen .
	2 Wählen Sie in der Liste der verfügbaren Edge-Gateways das Edge-Gateway aus, mit dem eine Verbindung hergestellt werden soll.
	3 Wählen Sie den Schnittstellentyp aus.
	4 Um ein Gast-VLAN zuzulassen, aktivieren Sie die Option Gast-VLAN zulässig .
Konvertieren eines gerouteten Netzwerks in ein isoliertes Netzwerk	Deaktivieren Sie die Option Verbindung zu einem Edge-Gateway herstellen .

- 6 Klicken Sie auf **Speichern**.

Ergebnisse

Sie haben das VDC-Organisationsnetzwerk konvertiert.

Konvertieren der Schnittstelle eines VDC-Organisationsnetzwerks mit Routing

Sie können die Schnittstelle eines Netzwerks beispielsweise von „Intern“ in „Teilschnittstelle“ oder „Distributed Routing“ ändern, indem Sie die Netzwerkeigenschaften bearbeiten.

Hinweis VDC-übergreifende Netzwerke können nicht konvertiert werden.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie konvertieren möchten.
- 3 Klicken Sie auf den Namen des VDC-Organisationsnetzwerks, das Sie bearbeiten möchten.
- 4 Klicken Sie auf der Registerkarte **Allgemein** auf **Bearbeiten**.
- 5 Klicken Sie auf **Verbindung**.

- 6 Wählen Sie im Dropdown-Menü **Schnittstellentyp** den Schnittstellentyp aus.

Option	Beschreibung
Intern	Stellt eine Verbindung zu einer der internen Schnittstellen des Edge-Gateways her. Die maximal zulässige Anzahl Netzwerke ist 9.
Verteilt	Erstellt das Netzwerk auf einem Distributed Logical Router, der mit diesem Edge-Gateway verbunden ist. Die maximal zulässige Anzahl Netzwerke ist 400.
Teilschnittstelle	Erweitert ein VDC-Organisationsnetzwerk. vCloud Director identifiziert das zu verwendende Netzwerk zum Erweitern über L2 VPN. vCloud Director erstellt mithilfe der NSX-Netzwerkvirtualisierung einen Trunk-Schnittstellentyp für dieses Netzwerk. Die maximal zulässige Anzahl Netzwerke ist 200.

- 7 Klicken Sie auf **Speichern**.

Anzeigen der für ein VDC-Organisationsnetzwerk verwendeten IP-Adressen

Sie können im IP-Pool eines VDC-Organisationsnetzwerks eine Liste der IP-Adressen anzeigen, die aktuell verwendet werden.

Voraussetzungen

- Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf den Namen des Netzwerks, für das Sie die verwendeten IP-Adressen anzeigen möchten.
- 3 Klicken Sie auf die Registerkarte **IP-Verwaltung**.
- 4 Klicken Sie auf **IP-Zuweisungen**, um festzustellen, welche IP-Adressen aktuell verwendet werden.

Hinzufügen von IP-Adressen zum IP-Pool eines VDC-Organisationsnetzwerks

Wenn in einem VDC-Organisationsnetzwerk nicht mehr genügend IP-Adressen verfügbar sind, können Sie dem zugehörigen IP-Pool weitere IP-Adressen hinzufügen.

Sie können IP-Adressen nicht zu externen VDC-Organisationsnetzwerken hinzufügen, die eine direkte Verbindung haben.

Voraussetzungen

- Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.

- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.

- 3 Klicken Sie auf die Registerkarte **IP-Verwaltung**.

Die Option **Statische IP-Pools** ist standardmäßig ausgewählt.

- 4 Klicken Sie auf der rechten Seite auf die Schaltfläche **Bearbeiten**.

Im Fenster **Netzwerk bearbeiten** sehen Sie ggf. das Gateway-CIDR und die IP-Adressbereiche.

- 5 Geben Sie im Textfeld **Statische IP-Pools** die IP-Adresse oder den Bereich der IP-Adressen ein und klicken Sie auf **Hinzufügen**.

Hinweis Für VDC-übergreifende Netzwerke dürfen sich die IP-Adressen nicht mit den IP-Adressen überschneiden, die den anderen VDC-Organisationsnetzwerken aus demselben ausgeweiteten Netzwerk zugeordnet sind.

- 6 Klicken Sie auf **Speichern**.

Ergebnisse

Die IP-Adresse oder der Bereich von IP-Adressen wird dem IP-Pool des Netzwerks hinzugefügt.

Bearbeiten oder Entfernen von IP-Bereichen, die in einem VDC-Organisationsnetzwerk verwendet werden

Wenn ein VDC-Organisationsnetzwerk IP-Adressen enthält, die Sie nicht mehr benötigen, können Sie die Adressen bearbeiten oder aus dem IP-Pool löschen.

Voraussetzungen

- Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **IP-Verwaltung**.
Die Option **Statische IP-Pools** ist standardmäßig ausgewählt.
- 4 Klicken Sie auf der rechten Seite auf die Schaltfläche **Bearbeiten**.
 - Um einen IP-Bereich zu ändern, wählen Sie den Bereich aus, nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Ändern**.
 - Um einen IP-Bereich zu entfernen, wählen Sie den Bereich aus und klicken Sie auf **Entfernen**.
- 5 Klicken Sie auf **Speichern**.

Bearbeiten der DNS-Einstellungen eines VDC-Organisationsnetzwerks

Sie können die DNS-Einstellungen eines VDC-Organisationsnetzwerks bearbeiten.

Voraussetzungen

- Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **IP-Verwaltung**.
- 4 Wählen Sie **DNS** aus und klicken Sie auf die Schaltfläche **Bearbeiten** auf der rechten Seite.

- 5 Bearbeiten Sie die primären DNS-, sekundären DNS- und DNS-Suffix-Informationen nach Bedarf.
- 6 Klicken Sie auf **Speichern**.

Konfigurieren von DHCP-Einstellungen für ein isoliertes VDC-Organisationsnetzwerk

Sie können die DHCP-Einstellungen eines isolierten VDC-Organisationsnetzwerks bearbeiten. Der DHCP-Dienst eines VDC-Organisationsnetzwerks stellt IP-Adressen aus dem Adressenpool für VM-Netzwerkkarten bereit, die so konfiguriert sind, dass eine Adresse von DHCP angefordert wird. Der Dienst stellt die Adresse bereit, wenn die virtuelle Maschine eingeschaltet wird.

Voraussetzungen

- Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.

- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.

- 3 Klicken Sie auf die Registerkarte **IP-Verwaltung**.

- 4 Wählen Sie **DHCP** aus.

Die DHCP-Einstellungen werden auf der rechten Seite angezeigt.

- 5 Klicken Sie zum Aktivieren von DHCP rechts von **DHCP-Pool-Dienst** auf **Bearbeiten**.

- 6 Aktivieren Sie den **DHCP-Pool-Dienst** und klicken Sie auf **Speichern**.

Von DHCP-Clients angeforderte Adressen werden aus einem DHCP-Pool abgerufen.

- 7 Erstellen Sie einen DHCP-Pool für das Netzwerk.

- a Klicken Sie auf **Hinzufügen**.

- b Geben Sie einen IP-Adressbereich für den Pool ein.

Der von Ihnen angegebene IP-Adressbereich darf sich nicht mit dem statischen IP-Adresspool für das Organisations-VDC überlappen.

- c Geben Sie die Standard-Lease-Dauer für die DHCP-Adressen in Sekunden an.

Die Standardeinstellung beträgt 3.600 Sekunden.

- d Geben Sie die maximale Lease-Dauer für die DHCP-Adressen in Sekunden an.

Dies ist der maximale Zeitraum, für den die über DHCP zugewiesenen IP-Adressen an die virtuellen Maschinen geleast werden. Die Standardeinstellung beträgt 7.200 Sekunden.

- 8 Klicken Sie auf **Speichern**.

Bearbeiten oder Löschen eines vorhandenen DHCP-Pools für ein Netzwerk

Wenn Sie in Ihrem isolierten VDC-Organisationsnetzwerk keinen DHCP-Pool mehr benötigen, können Sie den Pool entweder löschen oder bearbeiten.

Voraussetzungen

- Für diese Vorgänge sind die vordefinierten Rollen **Organisationsadministrator** oder **Systemadministrator** oder eine Rolle, die entsprechende Rechte beinhaltet, erforderlich.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie auf die Registerkarte **IP-Verwaltung**.
- 4 Wählen Sie **DHCP** aus.

Die DHCP-Einstellungen werden auf der rechten Seite angezeigt.

- 5 Bearbeiten oder löschen Sie einen vorhandenen DHCP-Pool.

Option	Aktion
Bearbeiten eines DHCP-Pools	<ol style="list-style-type: none"> 1 Wählen Sie den DHCP-Pool aus, den Sie bearbeiten möchten. 2 Klicken Sie auf die Schaltfläche Bearbeiten. 3 Aktualisieren Sie den IP-Adressbereich für den Pool. 4 Bearbeiten Sie die Standard-Lease-Dauer für die DHCP-Adressen in Sekunden. 5 Bearbeiten Sie die maximale Lease-Dauer für die DHCP-Adressen in Sekunden. 6 Klicken Sie auf Speichern.
Löschen eines DHCP-Pools	<ol style="list-style-type: none"> 1 Wählen Sie den DHCP-Pool aus, den Sie löschen möchten. 2 Klicken Sie auf die Schaltfläche Löschen.

Zurücksetzen eines VDC-Organisationsnetzwerks

Wenn die Netzwerkdienste, z. B. DHCP-Einstellungen oder Firewall-Einstellungen, die einem VDC-Organisationsnetzwerk zugewiesen sind, nicht wie erwartet funktionieren, können Sie das Netzwerk zurücksetzen.

Wenn Sie das VDC-Organisationsnetzwerk zurücksetzen, wird die erneute Bereitstellung des DHCP-Dienst-Gateway des Netzwerks erzwungen. Dieser Vorgang führt zu einer temporären Unterbrechung der DHCP-Dienste, und es sind keine Netzwerkdienste verfügbar, während das Netzwerk zurückgesetzt wird.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Das Netzwerk ist nicht mit virtuellen Maschinen, vApps oder anderen Netzwerken verbunden.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Wählen Sie ein VDC-Organisationsnetzwerk aus.
- 3 Klicken Sie auf **Zurücksetzen** und bestätigen Sie den Vorgang zum Zurücksetzen.

Löschen eines VDC-Organisationsnetzwerks

Wird ein VDC-Organisationsnetzwerk nicht mehr benötigt, können Sie das Netzwerk löschen.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Das Netzwerk ist nicht mit virtuellen Maschinen, vApps oder anderen Netzwerken verbunden.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Netzwerke** aus.
- 2 Wählen Sie ein VDC-Organisationsnetzwerk aus.
- 3 Klicken Sie auf **Löschen** und bestätigen Sie den Löschvorgang.

Verwalten von VDC-übergreifenden Netzwerken

5

Um ein Netzwerk über mehrere Organisations-VDCs zu erstellen, gruppieren Sie zuerst die virtuellen Datacenter und erstellen dann ein ausgeweitetes Netzwerk in der Datacenter-Gruppe. Eine Datacenter-Gruppe kann entweder eine gemeinsame Egress-Punkte-Konfiguration oder eine Egress-Punkte-Konfiguration für jede Netzwerk-Fehlerdomäne aufweisen.

Datacenter-Gruppe

Eine Gruppe aus bis zu vier virtuellen Datacentern, die für die gemeinsame Nutzung mehrerer Egress-Punkte konfiguriert sind. Eine Datacenter-Gruppe kann eine der folgenden Egress-Punktekonfigurationen aufweisen:

Egress-Punkte-Konfigurationstyp	Beschreibung
Konfiguration gemeinsamer Egress-Punkte	Die Datacenter-Gruppe kann mit einem aktiven Egress-Punkt und einem Standby-Egress-Punkt konfiguriert werden. Die beiden Egress-Punkte werden von allen beteiligten virtuellen Datacentern in allen Netzwerk-Fehlerdomänen in der Datacenter-Gruppe gemeinsam verwendet.
Egress-Punktekonfiguration pro Fehlerdomäne	Die Datacenter-Gruppe kann mit einem aktiven Egress-Punkte für jede Netzwerk-Fehlerdomäne in der Datacenter-Gruppe konfiguriert werden. Standby-Egress-Punkte können nicht erstellt werden.

Eine Organisation kann mehrere Datacenter-Gruppen aufweisen. Ein Organisations-VDC kann an mehreren Datacenter-Gruppen beteiligt sein.

Die teilnehmenden virtuellen Organisations-Datacenter können zu unterschiedlichen vCloud Director-Sites gehören. Weitere Informationen finden Sie unter [Konfigurieren und Verwalten von Multisite-Bereitstellungen](#).

Netzwerk-Fehlerdomäne

Der Netzwerkanbieter-Bereich; dieser stellt in der Regel die zugrunde liegende vCenter Server-Instanz beim zugehörigen NSX Manager dar.

Egress-Punkt

Ein Edge-Gateway, das eine Datencenter-Gruppe oder Netzwerk-Fehlerdomäne mit dem Internet verbindet. Das Edge-Gateway muss einem virtuellen Datencenter aus der Datencenter-Gruppe angehören. BGP-Routen werden auf dem Edge-Gateway konfiguriert, das den Egress-Punkt und den allgemeinen Router der virtuellen Datencenter-Gruppe oder Netzwerk-Fehlerdomäne darstellt. Dies hat keine Auswirkungen auf vorhandene Routen auf dem Edge-Gateway.

Ausgeweitetes Netzwerk

Ein Layer-2-Netzwerk, das auf alle virtuellen Datencenter in einer Datencenter-Gruppe ausgeweitet wird. Nur IPv4 ist möglich.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von Datencenter-Gruppen](#)
- [Verwalten von ausgeweiteten Netzwerken](#)

Verwalten von Datencenter-Gruppen

Nachdem Sie eine Datencenter-Gruppe erstellt haben, können Sie die Netzwerktopologie einer Datencenter-Gruppe bearbeiten. Sie können virtuelle Datencenter zu der Gruppe hinzufügen und aus ihr entfernen. Sie können Egress-Punkte tauschen, ersetzen und entfernen. Außerdem haben Sie die Möglichkeit, Konfigurationsfehler durch die Ausführung verschiedener Synchronisierungsaufgaben zu beheben.

Eine gemeinsame Egress-Konfiguration kann nicht in eine Egress-Konfiguration pro Fehlerdomäne umgewandelt werden oder umgekehrt.

Erstellen und Konfigurieren einer Datencenter-Gruppe mit einer gemeinsamen Egress-Konfiguration

Sie können eine virtuelle Datencenter-Gruppe mit einer gemeinsamen Egress-Konfiguration erstellen, bei der Sie ein Edge-Gateway-Paar aus aktivem und Standby-Egress-Punkt für alle beteiligten virtuellen Datencenter einrichten.

Voraussetzungen

- Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.
- Sie haben die gewünschten virtuellen Datencenter für VDC-übergreifende Netzwerke aktiviert. Informationen zum Konfigurieren von VDC-übergreifenden Netzwerken finden Sie im *vCloud Director-Administratorhandbuch*.

Verfahren

1 [Erstellen einer Datencenter-Gruppe mit einer gemeinsamen Egress-Konfiguration](#)

Sie können zwei bis vier virtuelle Datencenter in einer Datencenter-Gruppe mit einer gemeinsamen Egress-Konfiguration zusammenfassen.

2 Hinzufügen eines aktiven Egress-Punkts

Um Ihre Datencenter-Gruppe mit dem Internet zu verbinden, müssen Sie ihrer Netzwerktopologie einen aktiven Egress-Punkt hinzufügen.


3 Hinzufügen eines Standby-Egress-Punkts

In virtuellen Datencenter-Gruppen mit gemeinsamen Egress-Konfigurationen können Sie einen sekundären Egress-Punkt hinzufügen, der als Standby-Egress-Punkt für Fault Tolerance-Szenarien fungiert.

Erstellen einer Datencenter-Gruppe mit einer gemeinsamen Egress-Konfiguration

Sie können zwei bis vier virtuelle Datencenter in einer Datencenter-Gruppe mit einer gemeinsamen Egress-Konfiguration zusammenfassen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie auf **Neue Datencenter-Gruppe**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für die neue Datencenter-Gruppe ein.
- 4 Wählen Sie **Gemeinsame Egress-Punkte** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite **Datencenter** mindestens zwei und höchstens vier Datencenter für die neue Datencenter-Gruppe aus und klicken Sie auf **Weiter**.
Die Seite **Datencenter** enthält eine Liste der virtuellen Datencenter, die vom **Systemadministrator** für VDC-übergreifende Netzwerke aktiviert wurden.
- 6 Überprüfen Sie die Details der Datencenter-Gruppe und klicken Sie auf **Fertig stellen**.

Ergebnisse

Die neu erstellte virtuelle Datencenter-Gruppe ist in der Ansicht **Datencenter-Gruppen** aufgeführt.


Hinzufügen eines aktiven Egress-Punkts

Um Ihre Datencenter-Gruppe mit dem Internet zu verbinden, müssen Sie ihrer Netzwerktopologie einen aktiven Egress-Punkt hinzufügen.

Voraussetzungen

Der **Systemadministrator** hat mindestens ein Edge-Gateway in einem der virtuellen Datencenter erstellt, die Teil der Datencenter-Gruppe sind.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie auf **Egress-Punkt hinzufügen**.
Die Seite **Aktiven Egress-Punkt hinzufügen** wird geöffnet. Sie enthält eine Liste der Edge-Gateways, die zu den teilnehmenden virtuellen Datencentern gehören.
- 4 Wählen Sie das Edge-Gateway aus, das als aktiver Egress-Punkt für diese Datencenter-Gruppe fungieren soll, und klicken Sie auf **Hinzufügen**.

Ergebnisse

BGP-Routen werden auf dem Edge-Gateway, das den Egress-Point darstellt, und dem globalen Router der virtuellen Datencenter-Gruppe konfiguriert. Dies hat keine Auswirkungen auf vorhandene Routen auf dem Edge-Gateway.

Das Diagramm der Netzwerktopologie wird mit dem neu hinzugefügten Egress-Punkt aktualisiert. Der Datenverkehr von den teilnehmenden virtuellen Datencentern zum Internet ist durch eine durchgezogene blaue Linie dargestellt.


Hinzufügen eines Standby-Egress-Punkts

In virtuellen Datencenter-Gruppen mit gemeinsamen Egress-Konfigurationen können Sie einen sekundären Egress-Punkt hinzufügen, der als Standby-Egress-Punkt für Fault Tolerance-Szenarien fungiert.

Voraussetzungen

Abgesehen von dem Edge-Gateway, das als aktiver Egress-Punkt fungiert, muss mindestens ein weiteres Edge-Gateway in einem der virtuellen Datencenter vorhanden sein, die Teil der Gruppe sind.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.

- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.

Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.

- 3 Klicken Sie auf **Standby-Egress-Punkt hinzufügen**.

Die Seite **Standby-Egress-Punkt hinzufügen** wird geöffnet. Sie enthält eine Liste der nicht verwendeten Edge-Gateways, die zu den teilnehmenden virtuellen Datencentern gehören. Das Edge-Gateway, das vom aktiven Egress-Punkt in dieser virtuellen Datencenter-Gruppe verwendet wird, wird nicht angezeigt.

- 4 Wählen Sie das Edge-Gateway aus, das als Standby-Egress-Punkt für diese Datencenter-Gruppe fungieren soll, und klicken Sie auf **Hinzufügen**.

Ergebnisse

BGP-Routen werden auf dem Edge-Gateway, das den Egress-Point darstellt, und dem globalen Router der virtuellen Datencenter-Gruppe konfiguriert. Dies hat keine Auswirkungen auf vorhandene Routen auf dem Edge-Gateway.

Das Diagramm der Netzwerktopologie wird mit dem neu hinzugefügten Egress-Punkt aktualisiert. Der Datenverkehr, der in Fault Tolerance-Szenarien von den teilnehmenden virtuellen Datencentern zum Internet übertragen wird, ist durch eine gestrichelte blaue Linie dargestellt.

Erstellen und Konfigurieren einer Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration

Sie können eine virtuelle Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration erstellen und konfigurieren. Dabei können Sie ein Edge-Gateway konfigurieren, das als aktive Egress-Punkte für jede Netzwerk-Fehlerdomäne in der Gruppe fungiert. In einer Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration können keine Standby-Egress-Punkte erstellt werden.

Voraussetzungen

Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.

Verfahren

- 1 Erstellen einer Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration

Sie können zwei bis vier virtuelle Datencenter in einer Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration zusammenfassen.

2 Hinzufügen eines Egress-Punkts für eine Fehlerdomäne

Wenn Sie die virtuellen Datacenter aus einer Netzwerk-Fehlerdomäne in einer Datacenter-Gruppe mit dem Internet verbinden möchten, müssen Sie dieser Netzwerk-Fehlerdomäne einen Egress-Punkt hinzufügen. Sie können jeder Netzwerk-Fehlerdomäne in der Datacenter-Gruppe einen Egress-Punkt hinzufügen. Standby-Egress-Punkte werden in einer Datacenter-Gruppe mit einer Egress-Konfiguration für Fehlerdomänen nicht unterstützt.


Erstellen einer Datacenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration

Sie können zwei bis vier virtuelle Datacenter in einer Datacenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration zusammenfassen.

Voraussetzungen

Der **Systemadministrator** hat die gewünschten virtuellen Datacenter für VDC-übergreifende Netzwerke aktiviert.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datacenter-Gruppen** aus.
Die Liste der Vorlagen für Datacenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie auf **Neue Datacenter-Gruppe**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für die neue Datacenter-Gruppe ein.
- 4 Wählen Sie **Egress-Punkte pro Fehlerdomäne** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite **Datacenter** mindestens zwei und höchstens vier Datacenter für die neue Datacenter-Gruppe aus und klicken Sie auf **Weiter**.
Die Seite **Datacenter** enthält eine Liste der virtuellen Datacenter, die vom **Systemadministrator** für VDC-übergreifende Netzwerke aktiviert wurden.
- 6 Überprüfen Sie die Details der Datacenter-Gruppe und klicken Sie auf **Fertig stellen**.

Ergebnisse

Die neu erstellte virtuelle Datacenter-Gruppe ist in der Ansicht **Datacenter-Gruppen** aufgeführt.


Hinzufügen eines Egress-Punkts für eine Fehlerdomäne

Wenn Sie die virtuellen Datacenter aus einer Netzwerk-Fehlerdomäne in einer Datacenter-Gruppe mit dem Internet verbinden möchten, müssen Sie dieser Netzwerk-Fehlerdomäne einen Egress-Punkt hinzufügen. Sie können jeder Netzwerk-Fehlerdomäne in der Datacenter-Gruppe einen Egress-Punkt hinzufügen. Standby-Egress-Punkte werden in einer Datacenter-Gruppe mit einer Egress-Konfiguration für Fehlerdomänen nicht unterstützt.

Voraussetzungen

Abgesehen von den Edge-Gateways, die in dieser Datencenter-Gruppe als Egress-Punkte verwendet werden, muss mindestens ein nicht verwendetes Edge-Gateway in einem der teilnehmenden virtuellen Datencenter vorhanden sein.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie im Diagramm der Netzwerktopologie auf die Fehlerdomäne des Zielnetzwerks.
Netzwerk-Fehlerdomänen werden durch durchgezogene Linien dargestellt. Ihre Namen sind im unteren Bereich des Diagramms angegeben.
Die ausgewählte Fehlerdomäne ist blau markiert.
- 4 Klicken Sie auf **Egress-Punkt hinzufügen**.
Die Seite **Aktiven Egress-Punkt hinzufügen** wird geöffnet. Sie enthält eine Liste der Edge-Gateways, die zu den teilnehmenden virtuellen Datencentern gehören.
- 5 Wählen Sie das Edge-Gateway aus, das als Egress-Punkt für diese Fehlerdomäne fungieren soll, und klicken Sie auf **Hinzufügen**.

Ergebnisse

BGP-Routen werden auf dem Edge-Gateway, das den Egress-Point darstellt, und dem globalen Router der Netzwerk-Fehlerdomäne konfiguriert. Dies hat keine Auswirkungen auf vorhandene Routen auf dem Edge-Gateway.

Das Diagramm der Netzwerktopologie wird mit dem neu hinzugefügten Egress-Punkt aktualisiert. Der Datenverkehr von den virtuellen Datencentern in der Netzwerk-Fehlerdomäne zum Internet ist durch eine durchgezogene blaue Linie dargestellt.


Anzeigen einer Datencenter-Gruppe

Sie können die Datencenter-Gruppen in Ihrer Organisation und die Details zu deren aktueller Konfiguration anzeigen.

Voraussetzungen

Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: VDC-Gruppe anzeigen**, das für die Organisation veröffentlicht wurde.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.


Hinzufügen eines virtuellen Datencenters zu einer Datencenter-Gruppe

Sie können einer Datencenter-Gruppe ein virtuelles Datencenter hinzufügen und hierdurch die vorhandenen Netzwerke auf das neue virtuelle Datencenter ausdehnen.

Voraussetzungen

- Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.
- Die Datencenter-Gruppe enthält weniger als vier virtuelle Datencenter.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie auf **Datencenter hinzufügen**.
- 4 Wählen Sie auf der Seite **Datencenter** das Datencenter aus, das Sie der Datencenter-Gruppe hinzufügen möchten, und klicken Sie auf **Fertigstellen**.
Die Seite **Datencenter** enthält eine Liste virtueller Datencenter, die vom Systemadministrator für VDC-übergreifende Netzwerke aktiviert wurden.

Hinweis Eine Datencenter-Gruppe kann bis zu vier virtuelle Datencenter enthalten.


Entfernen eines virtuellen Datacenters aus einer Datacenter-Gruppe

Sie können ein virtuelles Datacenter aus einer Datacenter-Gruppe entfernen. Die vorhandenen Netzwerke aus diesem virtuellen Datacenter sind dann nicht mehr ausgeweitet.

Voraussetzungen

- Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.
- Die Datacenter-Gruppe muss mindestens drei virtuelle Datacenter enthalten.
- Das virtuelle Datacenter, das Sie entfernen möchten, darf keinen Egress-Punkt für die Datacenter-Gruppe bereitstellen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datacenter-Gruppen** aus.
Die Liste der Vorlagen für Datacenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datacenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datacenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datacenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie rechts oben in der Ecke der Karte des gewünschten virtuellen Datacenters auf die drei Punkte und anschließend auf **Entfernen**.
- 4 Klicken Sie zur Bestätigung auf **Entfernen**.

Ergebnisse

Das virtuelle Datacenter wird aus dem Netzwerktopologie-Diagramm der Datacenter-Gruppe entfernt.

Synchronisieren einer Datacenter-Gruppe


Um die Netzwerkkonfigurationen der Datacenter-Gruppe erneut anzuwenden und sicherzustellen, dass alle beteiligten virtuellen Datacenter aktiv sind, können Sie die Datacenter-Gruppe synchronisieren.

Hinweis Während des Synchronisierungsvorgangs der Datacenter-Gruppe ist die Datacenter-Gruppe für einige Sekunden nicht verfügbar, da der allgemeine Router in NSX synchronisiert wird.

Voraussetzungen

Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie auf **Datencenter-Gruppe synchronisieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.


Tauschen der Egress-Punkte in einer Datencenter-Gruppe mit einer gemeinsamen Egress-Konfiguration

Nachdem Sie einen aktiven Egress-Punkt und einen Standby-Egress-Punkt in einer Datencenter-Gruppe mit gemeinsamer Egress-Konfiguration konfiguriert haben, können Sie die Rollen der Egress-Punkte tauschen. Der aktive Egress-Punkt kann zu einem Standby-Egress-Punkt werden und umgekehrt.

Voraussetzungen

Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie auf **Egress-Punkte tauschen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Ergebnisse

Das Diagramm der Netzwerktopologie wird mit den neuen Datenverkehrsrouten aktualisiert. Der Datenverkehr zum Internet wird jetzt zum neuen aktiven Egress-Punkt umgeleitet.


Ersetzen des Edge-Gateway eines Egress-Punkts

Sie können das Edge-Gateway ersetzen, das einen aktiven oder Standby-Egress-Punkt in einer Datencenter-Gruppe darstellt.

Voraussetzungen

- Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.
- Das neue Edge-Gateway darf nicht von anderen Egress-Punkten in der Datencenter-Gruppe verwendet werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Wenn Sie einen Egress-Punkt aus der Konfiguration einer Netzwerk-Fehlerdomäne ersetzen möchten, wählen Sie im Netzwerktopologie-Diagramm die Netzwerk-Fehlerdomäne des gewünschten Egress-Punkts aus.
Netzwerk-Fehlerdomänen werden mit durchgehenden Linien und Domänennamen am unteren Rand des Diagramms dargestellt.
Die ausgewählte Netzwerk-Fehlerdomäne ist blau markiert.
- 4 Klicken Sie rechts oben in der Ecke der Karte des gewünschten Egress-Punkts auf die drei Punkte und anschließend auf **Ersetzen**.
Die Seite **Egress-Punkt ersetzen** wird geöffnet. Sie enthält eine Liste der Edge-Gateways, die zu den beteiligten virtuellen Datencentern gehören.
- 5 Wählen Sie das neue Edge-Gateway aus und klicken Sie auf **Ersetzen**.

Ergebnisse

BGP-Routen werden aus dem alten Edge-Gateway entfernt und auf dem neuen Edge-Gateway konfiguriert, das den Egress-Punkt und den allgemeinen Router der virtuellen Datencenter-Gruppe darstellt.

Das Netzwerktopologie-Diagramm wird mit dem Namen des neuen Edge-Gateways aktualisiert.


Entfernen eines Egress-Punkts

Um eine Datencenter-Gruppe oder eine Netzwerk-Fehlerdomäne vom Internet zu trennen, können Sie ihren Egress-Punkt entfernen.

Voraussetzungen

- Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.
- Wenn Sie einen aktiven Egress-Punkt entfernen möchten, der mit einem Standby-Egress-Punkt gekoppelt ist, müssen Sie die Egress-Punkte tauschen oder den Standby-Egress-Punkt entfernen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Wenn Sie einen Egress-Punkt aus der Konfiguration einer Netzwerk-Fehlerdomäne entfernen möchten, wählen Sie im Netzwerktopologie-Diagramm die Netzwerk-Fehlerdomäne des gewünschten Egress-Punkts aus.
Netzwerk-Fehlerdomänen werden mit durchgehenden Linien und Domänennamen am unteren Rand des Diagramms dargestellt.
Die ausgewählte Netzwerk-Fehlerdomäne ist blau markiert.
- 4 Klicken Sie rechts oben in der Ecke der Karte des gewünschten Egress-Punkts auf die drei Punkte und anschließend auf **Löschen**.
- 5 Klicken Sie zur Bestätigung auf **OK**.

Ergebnisse

BGP-Routen werden aus dem Edge-Gateway, das den Egress-Punkt darstellt, entfernt, wenn dieser nicht von anderen allgemeinen Routern verwendet wird.

Der Egress-Punkt wird aus der Netzwerktopologie-Diagramm entfernt.

Synchronisieren von Routen und Egress-Punkten


Sie können die Konfiguration für dynamisches Routing erneut auf eine Datencenter-Gruppe oder Netzwerk-Fehlerdomäne und ihre zugehörigen Egress-Punkte anwenden, indem Sie die

Routen synchronisieren. Durch die Synchronisierung des Egress-Punkts stellen Sie sicher, dass ein Egress-Punkt korrekt mit der Datencenter-Gruppe verbunden ist.

Voraussetzungen

- Dieser Vorgang erfordert die Rolle **Systemadministrator** oder eine Rolle mit dem Recht **VDC-Gruppe: vDC-Gruppe konfigurieren**, das für die Organisation veröffentlicht wurde.
- Sie haben einen Egress-Punkt für die gewünschte Datencenter-Gruppe oder Netzwerk-Fehlerdomäne erstellt.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Wenn Sie eine Netzwerk-Fehlerdomäne in einer Datencenter-Gruppe synchronisieren möchten, wählen Sie im Netzwerktopologie-Diagramm die gewünschte Netzwerk-Fehlerdomäne aus.
Netzwerk-Fehlerdomänen werden mit durchgehenden Linien und Domänennamen am unteren Rand des Diagramms dargestellt.
Die ausgewählte Netzwerk-Fehlerdomäne ist blau markiert.
- 4 Klicken Sie zum erneuten Anwenden der Konfiguration für das dynamische Routing auf die Gruppe oder Netzwerk-Fehlerdomäne und ihre zugehörigen Egress-Punkte auf **Routen synchronisieren** und anschließend auf **OK**.
- 5 Um einen Egress-Punkt mit seiner Datencenter-Gruppe zu synchronisieren, klicken Sie oben rechts in der Ecke der Karte des gewünschten Egress-Punkts auf die drei Punkte, klicken Sie auf **Sync** und dann auf **OK**.

Verwalten von ausgeweiteten Netzwerken

Nachdem Sie eine Datencenter-Gruppe erstellt und konfiguriert haben, können Sie ausgeweitete Layer-2-Netzwerke erstellen und verwalten, die die beteiligten virtuellen Datencenter umfassen. Auf einer VDC-Ebene erscheinen ausgeweitete Netzwerke als VDC-Organisationsnetzwerke mit VDC-übergreifendem Routingtyp.

Hinzufügen eines ausgeweiteten Netzwerks


Sie können ein ausgeweitetes Netzwerk für alle virtuellen Datacenter erstellen, die Teil einer Datacenter-Gruppe sind.

Sie können nur ein ausgeweitetes IPv4-Netzwerk hinzufügen.

Voraussetzungen

Für diesen Vorgang ist die vordefinierte Rolle **Organisationsadministrator** oder eine Rolle mit dem Recht **VDC-Organisationsnetzwerk: Eigenschaften bearbeiten** erforderlich.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datacenter-Gruppen** aus.
Die Liste der Vorlagen für Datacenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datacenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datacenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datacenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie im linken Bereich auf **Ausgeweitete Netzwerke**.
Die Liste der ausgeweiteten Netzwerke wird in einer Rasteransicht angezeigt.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für das neue ausgeweitete Netzwerk ein.
- 6 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein und klicken Sie auf **Erstellen**.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.

Ergebnisse

Das neu erstellte Netzwerk wird in der Liste der ausgeweiteten Netzwerke für die Datacenter-Gruppe angezeigt.

Für jedes teilnehmende virtuelle Datacenter wird ein VDC-Organisationsnetzwerk mit VDC-übergreifendem Routing erstellt. Sie können die neu erstellten Netzwerke in der Ansicht **Datacenter** der teilnehmenden virtuellen Datacenter anzeigen, indem Sie auf **Netzwerke** klicken. Wenn eine virtuelle Maschine oder eine vApp eine Verbindung mit einem VDC-Organisationsnetzwerk dieses Typs herstellt, wird diese virtuelle Maschine oder vApp mit dem ausgeweiteten Netzwerk verbunden.

Nächste Schritte

Für jedes entsprechende VDC-übergreifende VDC-Organisationsnetzwerk können Sie statische IP-Adressen und IP-Pools zuweisen. Weitere Informationen finden Sie unter [Hinzufügen von IP-Adressen zum IP-Pool eines VDC-Organisationsnetzwerks](#).

Bei DNS- und DHCP-Konfigurationen für virtuelle Maschinen, die an ein ausgeweitetes Netzwerk angehängt sind, können Sie vCloud OpenAPI verwenden. Wenn Sie sich die Dokumentation zu vCloud OpenAPI ansehen möchten, wechseln Sie zu `https://vCloud_Director_IP_address_or_host_name/docs`. Um sich Codebeispiele anzusehen und vCloud OpenAPI-Aufrufe zu testen, wechseln Sie zu `https://vCloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name`.

Anzeigen oder Bearbeiten eines ausgeweiteten Netzwerks


Sie können den Namen, die Beschreibung und die CIDR-Einstellungen eines ausgeweiteten Netzwerks anzeigen. Sie können nur den Namen und die Beschreibung eines ausgeweiteten Netzwerks bearbeiten.

Informationen zum Bearbeiten der statischen IP-Poolzuweisung für ein ausgeweitetes Netzwerk auf der Ebene eines virtuellen Datacenters finden Sie unter [Hinzufügen von IP-Adressen zum IP-Pool eines VDC-Organisationsnetzwerks](#).

Voraussetzungen

- Für das Anzeigen von erweiterten Netzwerken ist die vordefinierte Rolle **Organisationsadministrator** oder eine Rolle mit dem Recht **VDC-Organisationsnetzwerk: Eigenschaften anzeigen** erforderlich.
- Für das Bearbeiten von erweiterten Netzwerken ist die vordefinierte Rolle **Organisationsadministrator** oder eine Rolle mit dem Recht **VDC-Organisationsnetzwerk: Eigenschaften bearbeiten** erforderlich.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datacenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie im linken Bereich auf **Ausgeweitete Netzwerke**.
Die Liste der ausgeweiteten Netzwerke wird in einer Rasteransicht angezeigt.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Netzwerks und anschließend auf **Bearbeiten**.

- 5 Bearbeiten Sie die Netzwerkdetails und klicken Sie auf **Speichern**.


Löschen eines ausgeweiteten Netzwerks

Sie können ein ausgeweitetes Netzwerk entfernen, das Sie nicht mehr verwenden.

Voraussetzungen

- Für diesen Vorgang ist die vordefinierte Rolle **Organisationsadministrator** oder eine Rolle mit dem Recht **VDC-Organisationsnetzwerk: Eigenschaften bearbeiten** erforderlich.
- Die entsprechenden Netzwerke der Organisations-VDCs dürfen nicht mit virtuellen Maschinen oder vApps verbunden sein.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie im linken Bereich auf **Ausgeweitete Netzwerke**.
Die Liste der ausgeweiteten Netzwerke wird in einer Rasteransicht angezeigt.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Netzwerks und dann auf **Löschen**.
- 5 Klicken Sie zur Bestätigung auf **Löschen**.

Ergebnisse

Die entsprechenden Netzwerke der Organisations-VDCs werden aus allen beteiligten virtuellen Datencentern entfernt.


Synchronisieren eines ausgeweiteten-Netzwerks

Damit alle beteiligten virtuellen Datencenter garantiert auf ihr ausgeweitetes Netzwerk zugreifen können, können Sie das ausgeweitete Netzwerk synchronisieren.

Voraussetzungen

Für diesen Vorgang ist die vordefinierte Rolle **Organisationsadministrator** oder eine Rolle mit dem Recht **VDC-Organisationsnetzwerk: Eigenschaften bearbeiten** erforderlich.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter-Gruppen** aus.
Die Liste der Vorlagen für Datencenter-Gruppen wird in einer Kartenansicht angezeigt.
- 2 Klicken Sie in der Karte der gewünschten Datencenter-Gruppe auf **Details**.
Sie werden zur **Netzwerktopologie**-Ansicht für diese Datencenter-Gruppe weitergeleitet. Sie sehen ein Diagramm der aktuellen Netzwerktopologie. Darin sind die beteiligten virtuellen Datencenter mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.
- 3 Klicken Sie im linken Bereich auf **Ausgeweitete Netzwerke**.
Die Liste der ausgeweiteten Netzwerke wird in einer Rasteransicht angezeigt.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Netzwerks und anschließend auf **Sync**.
- 5 Klicken Sie zur Bestätigung auf **OK**.

Erweiterte Netzwerkfunktionen für vCloud Director-Mandanten

6

vCloud Director stellt die von der NSX-Netzwerk-Virtualisierungssoftware unterstützten erweiterten Netzwerkfunktionen bereit, die in einer Cloud-Umgebung bessere Sicherheitskontrollen sowie Routing- und Netzwerkskalierungsfunktionen bieten.

Mit diesen Netzwerkfunktionen können Sie in Ihrem Organisations-VDC beispiellose Sicherheit und Isolierung erzielen. Diese Funktionen bieten folgende Vorteile:

- **Dynamisches Routing:** Die NSX-Funktionen in Ihrer vCloud Director-Umgebung unterstützen Routing-Protokolle wie BGP (Border Gateway Protocol) und OSPF (Open Shortest Path First), um die Netzwerkintegration zwischen Systemen zu vereinfachen und so in der durch die Cloud-gehosteten Anwendungsbereitstellung Redundanz und Kontinuität bereitzustellen.
- **Differenzierte Netzwerksicherheit und Isolierung:** Die NSX-Funktionen in der vCloud Director-Umgebung unterstützen die Verwendung von objektbasierten Regeldefinitionen, um eine statusbehaftete Isolierung des Netzwerkdatenverkehrs bereitzustellen, ohne dass mehrere virtuelle Netzwerke erforderlich sind. Dieses Zero-Trust-Sicherheitsmodell verhindert, dass Eindringlinge vollständigen Netzwerkzugriff erhalten, falls eine Anwendung oder eine virtuelle Maschine kompromittiert wird. Die Netzwerkkonfiguration wurde vereinfacht, da dieselben Netzwerksicherheitsrichtlinien verwendet werden, um Anwendungen zu schützen, wenn sie sich physisch in der vCloud Director-Umgebung befinden, und um das Zero-Trust-Sicherheitsmodell für portierbare Sicherheit unabhängig vom Bereitstellungsort einer Anwendung zu erweitern.
- Weitere Funktionen, die von NSX bereitgestellt werden, sind die erweiterte VPN-Unterstützung für Punkt-zu-Site-Konnektivität (IPsec-VPN) und Benutzerkonnektivität (SSL-VPN-Plus), der erweiterte Lastausgleich für HTTPS sowie die erweiterte Netzwerkskalierbarkeit.

Sie können zwei Typen von Firewalls konfigurieren: die Edge-Gateway-Firewall und die Distributed Firewall. Weitere Informationen zu den Unterschieden zwischen diesen Firewalls finden Sie unter [Firewallkonfiguration über das Mandantenportal](#).

Sie können auf diese erweiterten Netzwerkfunktionen über das vCloud Director-Mandantenportal oder das vCloud Director Service Provider Admin Portal zugreifen. Das Edge-Gateway muss über die vCloud Director-Webkonsole zuerst in ein erweitertes Edge-Gateway konvertiert werden. Die Schritte zum Konvertieren eines Edge-Gateways in ein erweitertes Edge-Gateway finden Sie im *vCloud Director-Administratorhandbuch*.

Wichtig IPv6-Edge-Gateways unterstützen eingeschränkte Dienste. IPv6-Edge-Gateways unterstützen Edge-Firewalls, Distributed Firewalls und statisches Routing.

Dieses Kapitel enthält die folgenden Themen:

- [Erste Schritte mit erweiterten vCloud Director-Netzwerken](#)
- [Firewallkonfiguration über das Mandantenportal](#)
- [Verwalten des DHCP-Protokolls für Edge-Gateways](#)
- [Verwalten der Netzwerkadressübersetzung mithilfe des Mandantenportals](#)
- [Konfiguration für erweitertes Routing](#)
- [Lastausgleich](#)
- [Sicherer Zugriff mit virtuellen privaten Netzwerken](#)
- [SSL-Zertifikatsverwaltung](#)
- [Benutzerdefiniertes Gruppieren von Objekten](#)
- [Statistiken und Protokolle für ein Edge-Gateway](#)
- [Aktivieren des SSH-Befehlszeilenzugriffs auf ein Edge-Gateway](#)
- [Arbeiten mit Sicherheitstags](#)
- [Arbeiten mit Sicherheitsgruppen](#)

Erste Schritte mit erweiterten vCloud Director-Netzwerken

Sie verwenden erweiterte vCloud Director-Netzwerke, um Verwaltungsaufgaben für eine Organisation in einem vCloud Director-System auszuführen. Sie können Distributed Firewalls und andere erweiterte Netzwerkfunktionen verwalten, die von den VMware NSX[®] - Softwarekomponenten bereitgestellt werden, die der Organisation von einem vCloud Director-Systemadministrator zur Verfügung gestellt werden.

Eine Einführung in die allgemeinen Funktionen des vCloud Director-Produkts sowie die Einrichtung einer Organisation und ihrer Ressourcen in einem vCloud Director-System finden Sie im *vCloud Director-Benutzerhandbuch*.

Die typischen Benutzer der erweiterten Netzwerkfunktionen sind:

- vCloud Director **-Systemadministratoren**, die das Mandantenportal verwenden, um die Distributed Firewall und andere erweiterte Netzwerkfunktionen für eine Organisation zu konfigurieren.

- **Organisationsadministratoren**, die das Mandantenportal zum Verwalten der Distributed Firewall und anderer erweiterter Netzwerkfunktionen nutzen, die der **Systemadministrator** dieser Organisation zur Verfügung gestellt hat.

Firewallkonfiguration über das Mandantenportal

Im Mandantenportal können Sie die Firewallfunktionen konfigurieren, die von der NSX-Software in Ihrem vCloud Director-Organisations-VDC zur Verfügung gestellt werden. Sie können Firewallregeln für Distributed Firewalls erstellen, um für die Sicherheit zwischen den virtuellen Maschinen in einem Organisations-VDC zu sorgen. Außerdem können Sie Firewallregeln für eine Edge-Gateway-Firewall einrichten, um die virtuellen Maschinen in einem Organisations-VDC vor externem Netzwerkverkehr zu schützen.

Hinweis Im Mandantenportal können sowohl Edge-Gateway-Firewalls als auch Distributed Firewalls konfiguriert werden.

Die NSX-Technologie für logische Firewalls besteht aus zwei Komponenten für die verschiedenen Bereitstellungsszenarien. Die Edge-Gateway-Firewall konzentriert sich auf die Erzwingung des vertikalen Datenverkehrs, während sich die Distributed Firewall auf die horizontale Zugriffssteuerung konzentriert.

Wichtige Unterschiede zwischen Edge-Gateway-Firewalls und Distributed Firewalls

Eine Edge-Gateway-Firewall überwacht den Nord-Süd-Datenverkehr, um Perimetersicherheitsfunktionen einschließlich Firewall, Netzwerkadressübersetzung (Network Address Translation, NAT) sowie Site-to-Site-IPSec und SSL-VPN-Funktionalität zur Verfügung zu stellen.

Eine Distributed Firewall bietet die Möglichkeit, jede virtuelle Maschine und jede Anwendung bis zur Ebene 2 (L2) zu isolieren und zu sichern. Durch die Konfiguration von Distributed Firewalls werden alle externen oder internen Bedrohungen der Netzwerksicherheit effektiv unter Quarantäne gestellt, wobei der horizontale Datenverkehr zwischen virtuellen Maschinen im selben Netzwerksegment isoliert wird. Sicherheitsrichtlinien werden zentral verwaltet, sind vererbbar und schachtelbar, sodass Netzwerk- und Sicherheitsadministratoren diese bedarfsgerecht verwalten können. Nachdem die definierten Sicherheitsrichtlinien bereitgestellt wurden, gelten diese auch für die virtuellen Maschinen oder Anwendungen, wenn diese zwischen verschiedenen virtuellen Datacentern verschoben werden.

Firewallregeln

Wie in der NSX-Produktdokumentation beschrieben, werden die auf zentraler Ebene definierten Firewallregeln in NSX als Vorabregeln bezeichnet. Sie können Regeln auf einer einzelnen Edge-Gateway-Ebene hinzufügen. Diese Regeln werden dann als lokale Regeln bezeichnet.

Jede Datenverkehrssitzung wird anhand der obersten Regel in der Firewalltabelle überprüft, bevor die nachfolgenden Regeln in der Tabelle überprüft werden. Die erste Regel in der Tabelle, die den Datenverkehrsparametern entspricht, wird erzwungen. Regeln werden in der folgenden Reihenfolge angezeigt:

- 1 Benutzerdefinierte Vorabregeln haben die höchste Priorität und werden in der Reihenfolge von oben nach unten durchgesetzt, wobei einzelne virtuelle NIC-Ebenen Vorrang haben.
- 2 Automatisch konfigurierte Regeln (Regeln, mit denen der Datenfluss für Edge-Gateway-Dienste gesteuert werden kann).
- 3 Auf Edge-Gateway-Ebene definierte lokale Regeln.
- 4 Standardmäßige Distributed Firewall-Regel

Weitere Informationen dazu, wie die NSX-Software Firewallregeln erzwingt, finden Sie unter *Ändern der Reihenfolge einer Firewallregel* in der Dokumentation für *NSX-Administratoren*.

Edge-Gateway-Firewall

Die Firewall für das Edge-Gateway hilft Ihnen dabei, die wesentlichen Anforderungen an die Perimetersicherheit zu erfüllen, wie z. B. das Erstellen von DMZs basierend auf IP/VLAN-Konstrukten, die Mandant-zu-Mandant-Isolation in virtuellen Datencentern mit mehreren Mandanten, die Netzwerkadressübersetzung (Network Address Translation, NAT), Partner-VPNs (Extranet) und benutzerbasierte SSL VPNs.

Die Edge-Gateway-Firewallfunktion in der vCloud Director-Umgebung wird von der NSX-Software zur Verfügung gestellt. In NSX wird diese Firewallfunktion auch als Edge-Firewall bezeichnet. Die Edge-Gateway-Firewall überwacht den Nord-Süd-Datenverkehr, um Perimetersicherheitsfunktionen einschließlich Firewall, Netzwerkadressübersetzung (Network Address Translation, NAT) sowie Site-to-Site-IPSec und SSL-VPN-Funktionalität zur Verfügung zu stellen.

Detaillierte Informationen über die von der Edge-Gateway-Firewall der NSX-Software zur Verfügung gestellten Funktionen finden Sie in der Dokumentation für *NSX-Administratoren*.

Verwalten einer Edge-Gateway-Firewall

Um den Datenverkehr zu und von einem Edge-Gateway zu schützen, können Sie Firewallregeln auf diesem Edge-Gateway erstellen und verwalten.

Informationen zum Schützen des Datenverkehrs zwischen virtuellen Maschinen in einem virtuellen Organisations-Datencenter finden Sie unter [Verwalten der Distributed Firewall-Regeln mithilfe des Mandantenportals](#).

Auf dem Bildschirm „Distributed Firewall“ erstellte Regeln, für die in der Spalte „Angewendet auf“ ein erweitertes Gateway angegeben ist, werden auf dem Bildschirm „Firewall“ für dieses erweiterte Edge-Gateway nicht angezeigt.

Die Firewallregeln für ein Edge-Gateway werden im Bildschirm **Firewall** angezeigt und in folgender Reihenfolge durchgesetzt:

- 1 Interne Regeln, auch bekannt als automatisch verbundene Regeln. Mit diesen internen Regeln können Datenflüsse für Edge-Gateway-Dienste gesteuert werden.
- 2 Benutzerdefinierte Regeln.
- 3 Standardregel.

Die Einstellungen für die Standardregel gelten für Datenverkehr, der keiner der benutzerdefinierten Firewallregeln entspricht. Die Standardregel wird am unteren Rand der Regeln auf dem Bildschirm „Firewall“ angezeigt.

Verwenden Sie im Mandantenportal die Umschaltoption **Aktivieren** des Edge-Gateway-Bildschirms „Firewall-Regeln“, um eine Edge-Gateway-Firewall zu aktivieren oder zu deaktivieren.

Konvertieren eines Edge-Gateways in ein erweitertes Edge-Gateway

Um mit einem Edge-Gateway im Mandantenportal zu arbeiten, müssen Sie es in ein erweitertes Edge-Gateway konvertieren. Sobald Sie es in ein erweitertes Edge-Gateway konvertiert haben, können Sie das Mandantenportal verwenden, um die statischen und dynamischen Routing-Funktionen zu konfigurieren, die von der NSX-Software für diese erweiterten Edge-Gateways bereitgestellt werden.

Voraussetzungen

Sie haben ein vorhandenes Edge-Gateway.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Edges** aus.
- 2 Wählen Sie das zu bearbeitende Edge-Gateway aus.
- 3 Klicken Sie auf **Konvertieren in erweitertes**.

Ergebnisse

Ihr Edge-Gateway wird in ein erweitertes Edge-Gateway konvertiert.

Nächste Schritte

Sobald Sie es in ein erweitertes Edge-Gateway konvertiert haben, können Sie Einstellungen konfigurieren, indem Sie das Gateway auswählen und auf **Dienste konfigurieren** klicken.

Hinzufügen einer Firewallregel für Edge-Gateways

Sie können den Bildschirm „Firewall“ des Edge-Gateways verwenden, um Firewallregeln für das jeweilige Edge-Gateway hinzuzufügen. Sie können mehrere NSX Edge-Schnittstellen und mehrere IP-Adressgruppen als Quelle und Ziel für diese Firewallregeln hinzufügen.

Durch Festlegen von **intern** für eine Quelle oder ein Ziel einer Regel wird Datenverkehr für alle Subnetze in den Portgruppen angegeben, die mit dem NSX-Edge-Gateway verbunden sind. Falls Sie als Quelle **intern** auswählen, wird die Regel automatisch aktualisiert, wenn auf dem NSX Edge Gateway weitere interne Schnittstellen konfiguriert werden.

Hinweis Edge-Gateway-Firewallregeln für interne Schnittstellen funktionieren nicht, wenn das Edge-Gateway für dynamisches Routing konfiguriert ist.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.

- 2 Falls der Bildschirm „Firewallregeln“ noch nicht angezeigt wird, klicken Sie auf die Registerkarte **Firewall**.

- 3 Um eine Regel unter einer vorhandenen Regel in der Firewallregeltabelle hinzuzufügen, klicken Sie auf die vorhandene Zeile und dann auf die Schaltfläche **Erstellen**.

Unter der ausgewählten Regel wird eine Zeile für die neue Regel eingefügt. Standardmäßig werden ihr alle Ziele, Dienste und die Aktion **Zulassen** zugewiesen. Wenn die Firewalltabelle nur die systemdefinierte Standardregel enthält, wird die neue Regel über der Standardregel eingefügt.

- 4 Klicken Sie in die Zelle **Name** und geben Sie einen Namen ein.

- 5 Klicken Sie in die Zelle **Quelle** und wählen Sie mithilfe der jetzt sichtbaren Symbole eine Quelle aus, die der Regel hinzugefügt werden soll:

Option	Beschreibung
Auf das IP-Symbol klicken	Geben Sie den Quellwert an, den Sie verwenden möchten. Gültige Werte sind eine IP-Adresse, CIDR, ein IP-Bereich oder das Schlüsselwort Beliebig . Die Edge-Gateway-Firewall unterstützt sowohl das IPv4- als auch das IPv6-Format.
Auf das Plussymbol (+) klicken	<p>Über das Plussymbol (+) können Sie die Quelle als ein Objekt angeben, bei dem es sich um keine spezifische IP-Adresse handelt:</p> <ul style="list-style-type: none"> ■ Fügen Sie im Fenster Objekte auswählen Objekte hinzu, die mit Ihrer Auswahl übereinstimmen, und klicken Sie auf Behalten, um sie der Regel hinzuzufügen. ■ Um eine Quelle aus der Regel auszuschließen, fügen Sie sie dieser Regel im Fenster Objekte auswählen hinzu und klicken Sie dann auf das Symbol „Ausschluss umschalten“, um diese Quelle aus dieser Regel auszuschließen. <p>Wenn „Ausschluss umschalten“ für die Quelle ausgewählt ist, wird die Regel auf den Datenverkehr angewendet, der aus allen Quellen außer der ausgeschlossenen Quelle stammt. Ist „Ausschluss umschalten“ nicht ausgewählt, so wird die Regel auf den Datenverkehr angewendet, der aus der im Fenster Objekte auswählen angegebenen Quelle stammt.</p>

- 6 Klicken Sie in die Zelle **Ziel** und führen Sie eine der folgenden Aktionen durch:

Option	Beschreibung
Auf das IP-Symbol klicken	Geben Sie den Zielwert an, den Sie verwenden möchten. Gültige Werte sind eine IP-Adresse, CIDR, ein IP-Bereich oder das Schlüsselwort Beliebig . Die Edge-Gateway-Firewall unterstützt sowohl das IPv4- als auch das IPv6-Format.
Auf das Plussymbol (+) klicken	<p>Über das Plussymbol (+) können Sie die Quelle als ein Objekt angeben, bei dem es sich um keine spezifische IP-Adresse handelt:</p> <ul style="list-style-type: none"> ■ Fügen Sie im Fenster Objekte auswählen Objekte hinzu, die mit Ihrer Auswahl übereinstimmen, und klicken Sie auf Behalten, um sie der Regel hinzuzufügen. ■ Um eine Quelle aus der Regel auszuschließen, fügen Sie sie dieser Regel im Fenster „Objekte auswählen“ hinzu und klicken Sie dann auf das Symbol „Ausschluss umschalten“, um diese Quelle aus dieser Regel auszuschließen. <p>Wenn „Ausschluss umschalten“ für die Quelle ausgewählt ist, wird die Regel auf den Datenverkehr angewendet, der aus allen Quellen außer der ausgeschlossenen Quelle stammt. Ist „Ausschluss umschalten“ nicht ausgewählt, so wird die Regel auf den Datenverkehr angewendet, der aus der im Fenster Objekte auswählen angegebenen Quelle stammt.</p>

- 7 Klicken Sie in die Zelle **Dienst** der neuen Regel und dann auf das Plussymbol (+), um den Dienst als Port-Protokoll-Kombination anzugeben:
 - a Wählen Sie das Dienstprotokoll aus.
 - b Geben Sie die Portnummern für die Quell- und Zielports oder **Beliebig** an.
 - c Klicken Sie auf **Behalten**.
- 8 Konfigurieren Sie in der Zelle **Aktion** der neuen Regel die Aktion für die Regel.

Option	Beschreibung
Annehmen	Lässt Datenverkehr von den angegebenen Quellen, Zielen und Diensten oder zu diesen zu.
Verweigern	Blockiert Datenverkehr von den angegebenen Quellen, Zielen und Diensten oder zu diesen.

- 9 Klicken Sie auf **Änderungen speichern**.
Der Speichervorgang kann eine Minute dauern.

Ändern der Firewallregeln für Edge-Gateways

Sie können nur benutzerdefinierte Firewallregeln, die einem Edge-Gateway hinzugefügt wurden, bearbeiten und löschen. Sie können eine automatisch erzeugte Regel oder Standardregel (mit Ausnahme der Aktionseinstellung der Standardregel) weder bearbeiten noch löschen. Sie können die Reihenfolge der Priorität von benutzerdefinierten Regeln ändern.

Weitere Informationen zu den verfügbaren Einstellungen für die verschiedenen Zellen einer Regel finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Firewall**.
- 3 Verwalten Sie die Firewall-Regeln.
 - Deaktivieren Sie eine Regel durch Klicken auf das grüne Häkchen in der Zelle **Nein**. Das grüne Häkchen verwandelt sich in ein rotes Deaktiviert-Symbol. Wenn die Regel deaktiviert ist und Sie die Regel aktivieren möchten, klicken Sie auf das rote Deaktiviert-Symbol.
 - Bearbeiten Sie einen Regelnamen, indem Sie auf die Zelle **Name** doppelklicken und den neuen Namen eingeben.

- Ändern Sie die Einstellungen für eine Regel, z. B. die Quell- oder Aktionseinstellungen, indem Sie die entsprechende Zelle auswählen und die angezeigten Steuerelemente verwenden.
- Löschen Sie eine Regel, indem Sie sie auswählen und auf die Schaltfläche **Löschen** oberhalb der Regeltabelle klicken.
- Blenden Sie vom System generierte Regeln mithilfe der Option **Nur benutzerdefinierte Regeln anzeigen** aus.
- Verschieben Sie eine Regel in der Regeltabelle nach oben oder unten, indem Sie die Regel auswählen und oberhalb der Regeltabelle auf eine der Schaltflächen mit dem Pfeil nach oben oder unten klicken.

4 Klicken Sie auf **Änderungen speichern**.

Distributed Firewall

Die Distributed Firewall ermöglicht es Ihnen, Elemente des virtuellen Datacenters der Organisation (beispielsweise virtuelle Maschinen) basierend auf den Namen und Attributen virtueller Maschinen zu segmentieren.

vCloud Director unterstützt Dienste für verteilte Firewalls in von NSX Data Center for vSphere gestützten Organisations-VDCs. Wie in der Dokumentation für *NSX-Administratoren* erläutert, handelt es sich bei dieser Distributed Firewall um eine Kernel-Embedded-Hypervisor-Firewall, die Transparenz und Kontrolle für virtualisierte Arbeitslasten und Netzwerke bietet. Sie können Zugriffssteuerungsrichtlinien basierend auf Objekten wie Namen virtueller Maschinen und auf Netzwerkstrukturen wie IP-Adressen oder IP-Set-Adressen erstellen. Firewallregeln werden auf der vNIC-Ebene jeder virtuellen Maschine durchgesetzt, um eine konsistente Zugriffssteuerung zu bieten, selbst wenn die virtuelle Maschine durch vSphere vMotion zu einem neuen ESXi-Host verschoben wird. Diese Distributed Firewall unterstützt ein Sicherheitsmodell mit Mikrosegmentierung, bei dem der Ost-West-Datenverkehr bei fast maximal möglicher Verarbeitungsrate untersucht werden kann.

Wie in der Dokumentation für *NSX-Administratoren* erläutert, erstellt die Distributed Firewall für Pakete der Ebene 2 (L2) einen Cache zur Leistungssteigerung. Pakete der Ebene 3 (L3) werden in der folgenden Reihenfolge verarbeitet:

- 1 Alle Pakete werden auf ihren gegenwärtigen Zustand überprüft.
 - 2 Wird eine Zustandsübereinstimmung gefunden, werden die Pakete verarbeitet.
 - 3 Wenn keine Zustandsübereinstimmung gefunden wird, werden die Pakete anhand der Regeln verarbeitet, bis eine Übereinstimmung gefunden wird.
- Für TCP-Pakete wird ein Zustand nur für Pakete mit einem SYN-Flag festgelegt. Regeln, in denen kein Protokoll angegeben ist (BELIEBIGER Dienst) können jedoch TCP-Pakete mit einer beliebigen Kombination von Flags abgleichen.

- Für UDP-Pakete werden 5-Tupel-Details aus dem Paket extrahiert. Wenn ein Zustand in der Zustandstabelle nicht vorhanden ist, wird ein neuer Zustand mit den extrahierten 5-Tupel-Details erstellt. Nachfolgend empfangene Pakete werden mit dem soeben erstellten Zustand abgeglichen.
- Für ICMP-Pakete werden ICMP-Typ, Code und Paketrichtung zum Erstellen eines Zustands verwendet.

Die Distributed Firewall kann ebenfalls die Erstellung identitätsbasierter Regeln unterstützen. Administratoren können die Zugriffssteuerung anhand der Gruppenmitgliedschaft des Benutzers gemäß der Definition im Active Directory (AD) des Unternehmens erzwingen. Einige Anwendungsfälle für die Verwendung identitätsbasierter Firewallregeln:

- Benutzer, die auf einem Laptop oder mobilen Gerät auf virtuelle Anwendungen zugreifen, wobei AD für die Benutzerauthentifizierung verwendet wird
- Benutzer, die über die VDI-Infrastruktur auf virtuelle Anwendungen zugreifen, wobei die virtuellen Maschinen auf Microsoft Windows basieren

Detaillierte Informationen über die Funktionen, die von der Distributed Firewall der NSX-Software zur Verfügung gestellt werden, finden Sie in der Dokumentation für *NSX Administratoren*.

Aktivieren der Distributed Firewall in einem Organisations-VDC mithilfe des Mandantenportals

Bevor Sie das Mandantenportal verwenden, um mit den Distributed Firewall-Funktionen in einem Organisations-VDC zu arbeiten, muss die Distributed Firewall für dieses Organisations-VDC aktiviert werden. Ein vCloud Director-Systemadministrator oder ein Benutzer, dem die Berechtigung `ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE` zugewiesen wurde, kann die Distributed Firewall für das Organisations-VDC aktivieren.

Sie verwenden den Bildschirm „Distributed Firewall“ im Mandantenportal, um die Distributed Firewall für ein Organisations-VDC zu aktivieren.

Voraussetzungen

vCloud Director unterstützt Dienste für verteilte Firewalls in von NSX Data Center for vSphere gestützten Organisations-VDCs.

Stellen Sie sicher, dass der Organisation, zu der das Organisations-VDC gehört, die folgenden Rechte zugewiesen wurden:

- Distributed Firewall für Organisations-VDC: Aktivieren/Deaktivieren
- Distributed Firewall für Organisations-VDC: Regeln konfigurieren
- Distributed Firewall für Organisations-VDC: Regeln anzeigen

Der vCloud Director-Systemadministrator weist einer Organisation Rechte zu. Das Recht „Distributed Firewall für Organisations-VDC: Aktivieren/Deaktivieren“ ist erforderlich, um die Distributed Firewall über die Benutzeroberfläche des Mandantenportals zu aktivieren. Das Recht „Distributed Firewall für Organisations-VDC: Regeln anzeigen“ ist für die Anzeige von Firewallregeln im Mandantenportal erforderlich, und das Recht „Distributed Firewall für Organisations-VDC: Regeln konfigurieren“ ist erforderlich, um die Firewallregeln über das Mandantenportal zu konfigurieren.

Stellen Sie sicher, dass Ihnen eine Rolle zugewiesen wurde, die Ihnen das Recht „Distributed Firewall für Organisations-VDC: Aktivieren/Deaktivieren“ gewährt. Unter den vordefinierten Rollen in einem vCloud Director-System hat nur die Rolle „Systemadministrator“ dieses Recht standardmäßig.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie das Organisations-VDC aus, für das Sie Distributed Firewall-Regeln konfigurieren möchten.
- 3 Klicken Sie auf **Dienste konfigurieren**.
- 4 Aktivieren Sie die Distributed Firewall auf der Registerkarte **Distributed Firewall**.

Nächste Schritte

Eine Beschreibung der Distributed Firewall-Standardregel finden Sie unter [Verwalten der Distributed Firewall-Regeln mithilfe des Mandantenportals](#).

Verwalten der Distributed Firewall-Regeln mithilfe des Mandantenportals

Wie im *Administratorhandbuch für NSX* erläutert, werden die standardmäßigen Firewall-Einstellungen auf Datenverkehr angewendet, der keiner der benutzerdefinierten Firewallregeln entspricht. Im vCloud Director Tenant Portal hat die Distributed Firewall-Standardregel die Bezeichnung „Zulässige Standardregel“.

Die Distributed Firewall-Funktion muss in einem Organisations-VDC aktiviert werden, bevor Sie die Distributed Firewall-Einstellungen im vCloud Director Tenant Portal verwalten können.

Die Distributed Firewall-Standardregel ist so konfiguriert, dass der gesamte Ebene-2- und Ebene-3-Datenverkehr über das Organisations-VDC geleitet werden kann. Diese Einstellung wird angegeben, indem in der Spalte „Aktion“ der Benutzeroberfläche die Option „Zulassen“ ausgewählt wird. Die Standardregel befindet sich immer am Ende der Regeltabelle.

Wichtig Sie können die Standardregeln für Distributed Firewalls weder löschen noch ändern.

Zugreifen auf Einstellungen für Distributed Firewall-Regeln

Die Distributed Firewall-Standardregel wird im Bildschirm „Distributed Firewall“ im Mandantenportal angezeigt, wenn Sie sie über die vCloud Director-Webkonsole öffnen.

Verfahren

- 1 Navigieren Sie zu einem Organisations-VDC in der vCloud Director-Webkonsole.
- 2 Klicken Sie mit der rechten Maustaste auf das Organisations-VDC und wählen Sie **Firewall verwalten** aus.

Sowohl die Registerkarte „Allgemein“ für Ebene-3-Datenverkehr als auch die Registerkarte „Ethernet“ für Ebene-2-Datenverkehr haben eine Distributed Firewall-Standardregel.

Hinzufügen einer Distributed Firewall-Regel

Sie fügen eine Distributed Firewall-Regel zuerst dem Bereich des virtuellen Datacenters der Organisation (Organisations-VDC) hinzu. Anschließend können Sie den Bereich einschränken, auf den Sie die Regel anwenden möchten. Mit der Distributed Firewall können Sie auf Quell- und Zielebene für jede Regel mehrere Objekte hinzufügen und so die Gesamtanzahl der hinzuzufügenden Firewallregeln verringern.

Informationen zu den vordefinierten Diensten und Dienstgruppen, die Sie in einer Regel verwenden können, finden Sie unter [Anzeigen der für Firewallregeln verfügbaren Dienste](#) und [Anzeigen der für Firewallregeln verfügbaren Dienstgruppen](#).

Voraussetzungen

- [Aktivieren der Distributed Firewall in einem Organisations-VDC mithilfe des Mandantenportals](#)
- Wenn Sie ein IP Set als Quelle oder Ziel in einer Regel verwenden möchten, nutzen Sie das Verfahren unter [Erstellen eines IP Sets zur Verwendung in Firewallregeln und bei der DHCP-Relay-Konfiguration](#).
- Wenn Sie ein MAC Set als Quelle oder Ziel in einer Regel verwenden möchten, nutzen Sie das Verfahren unter [Erstellen eines MAC Sets für die Verwendung in Firewallregeln](#).
- Wenn Sie eine Sicherheitsgruppe als Quelle oder Ziel in einer Regel verwenden möchten, nutzen Sie das Verfahren unter [Erstellen einer Sicherheitsgruppe](#).


Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie das VDC-Netzwerk für Sicherheitsdienste aus, für das Sie Firewallregeln ändern möchten, und klicken Sie auf **Dienste konfigurieren**.

Der Bildschirm „Sicherheitsdienste“ wird angezeigt.

- 3 Wählen Sie den Typ der zu erstellenden Regel aus. Sie haben die Möglichkeit, eine allgemeine Regel oder eine Ethernet-Regel zu erstellen.

Layer-3-(L3-)Regeln werden auf der Registerkarte **Allgemein** konfiguriert. Layer-2-(L2-)Regeln werden auf der Registerkarte **Ethernet** konfiguriert.

- 4 Um eine Regel unter einer vorhandenen Regel in der Firewalltabelle hinzuzufügen, klicken Sie auf die vorhandene Zeile und dann auf die Schaltfläche **Erstellen** ().

Unter der ausgewählten Regel wird eine Zeile für die neue Regel eingefügt. Standardmäßig werden ihr alle Ziele, Dienste und die Aktion **Zulassen** zugewiesen. Wenn die Firewalltabelle nur die systemdefinierte Standardregel „Zulassen“ enthält, wird die neue Regel über der Standardregel eingefügt.

- 5 Klicken Sie in die Zelle **Name** und geben Sie einen Namen ein.
- 6 Klicken Sie in die Zelle **Quelle** und wählen Sie mithilfe der jetzt sichtbaren Symbole eine Quelle aus, die der Regel hinzugefügt werden soll:

Aktion	Beschreibung
Auf das IP-Symbol klicken	Gilt für Regeln, die auf der Registerkarte Allgemein definiert sind. Geben Sie den Quellwert an, den Sie verwenden möchten. Gültige Werte sind eine IP-Adresse, CIDR, ein IP-Bereich oder das Schlüsselwort Beliebig . Die Distributed Firewall unterstützt nur das IPv4-Format.
Auf das Plussymbol (+) klicken	Über das Plussymbol (+) können Sie die Quelle als ein Objekt angeben, bei dem es sich um keine spezifische IP-Adresse handelt: <ul style="list-style-type: none"> ■ Fügen Sie im Fenster Objekte auswählen Objekte hinzu, die mit Ihrer Auswahl übereinstimmen, und klicken Sie auf Behalten, um sie der Regel hinzuzufügen. ■ Um eine Quelle aus der Regel auszuschließen, fügen Sie sie dieser Regel im Fenster Objekte auswählen hinzu und klicken Sie dann auf das Symbol „Ausschluss umschalten“, um diese Quelle aus dieser Regel auszuschließen. <p>Wenn „Ausschluss umschalten“ für die Quelle ausgewählt ist, wird die Regel auf den Datenverkehr angewendet, der aus allen Quellen außer der ausgeschlossenen Quelle stammt. Ist „Ausschluss umschalten“ nicht ausgewählt, so wird die Regel auf den Datenverkehr angewendet, der aus der im Fenster Objekte auswählen angegebenen Quelle stammt.</p>

7 Klicken Sie in die Zelle **Ziel** und führen Sie eine der folgenden Aktionen durch:

Aktion	Beschreibung
Auf das IP-Symbol klicken	Gilt für Regeln, die auf der Registerkarte Allgemein definiert sind. Geben Sie den Zielwert an, den Sie verwenden möchten. Gültige Werte sind eine IP-Adresse, CIDR, ein IP-Bereich oder das Schlüsselwort Beliebig . Die Distributed Firewall unterstützt nur das IPv4-Format.
Auf das Plussymbol (+) klicken	Über das Plussymbol (+) können Sie die Quelle als ein Objekt angeben, bei dem es sich um keine spezifische IP-Adresse handelt: <ul style="list-style-type: none"> ■ Fügen Sie im Fenster Objekte auswählen Objekte hinzu, die mit Ihrer Auswahl übereinstimmen, und klicken Sie auf Behalten, um sie der Regel hinzuzufügen. ■ Um eine Quelle aus der Regel auszuschließen, fügen Sie sie dieser Regel im Fenster „Objekte auswählen“ hinzu und klicken Sie dann auf das Symbol „Ausschluss umschalten“, um diese Quelle aus dieser Regel auszuschließen. <p>Wenn „Ausschluss umschalten“ für die Quelle ausgewählt ist, wird die Regel auf den Datenverkehr angewendet, der aus allen Quellen außer der ausgeschlossenen Quelle stammt. Ist „Ausschluss umschalten“ nicht ausgewählt, so wird die Regel auf den Datenverkehr angewendet, der aus der im Fenster Objekte auswählen angegebenen Quelle stammt.</p>

8 Klicken Sie in die Zelle **Dienst** der neuen Regel und führen Sie eine der folgenden Aktionen durch:

Aktion	Beschreibung
Auf das IP-Symbol klicken	So geben Sie den Dienst als Port-Protokoll-Kombination an: <ol style="list-style-type: none"> Wählen Sie das Dienstprotokoll aus. Geben Sie die Portnummern für die Quell- und Zielports ein oder Beliebige an und klicken Sie auf Behalten.
Auf das Plussymbol (+) klicken	Wählen Sie einen vordefinierten Dienst oder eine vordefinierte Dienstgruppe aus oder definieren Sie einen neuen Dienst oder eine neue Dienstgruppe: <ol style="list-style-type: none"> Wählen Sie ein oder mehrere Objekte aus und fügen Sie sie dem Filter hinzu. Klicken Sie auf Behalten.

9 Konfigurieren Sie in der Zelle **Aktion** der neuen Regel die Aktion für die Regel.

Option	Beschreibung
Zulassen	Lässt Datenverkehr von den angegebenen Quellen, Zielen und Diensten oder zu diesen zu.
Verweigern	Blockiert Datenverkehr von den angegebenen Quellen, Zielen und Diensten oder zu diesen.

10 Wählen Sie in der Zelle **Richtung** der neuen Regel aus, ob die Regel auf eingehenden Datenverkehr, ausgehenden Datenverkehr oder beides angewendet wird.

- 11 Falls es sich um eine Regel auf der Registerkarte **Allgemein** in der Zelle **Pakettyp** der neuen Regel handelt, wählen Sie als Pakettyp **Beliebig**, **IPV4** oder **IPV6** aus.
- 12 Markieren Sie die Zelle **Angewendet auf** und definieren Sie mithilfe des Plussymbols (+) den Objektbereich, auf den diese Regel anwendbar ist.

Wenn die Regel in den Zellen **Quelle** und **Ziel** virtuelle Maschinen enthält, müssen Sie die virtuellen Quell- und Zielmaschinen der Zelle **Angewendet auf** der Regel hinzufügen, damit die Regel ordnungsgemäß funktioniert.

Wichtig IP-Adressgruppen (IP Sets), MAC-Adressgruppen (MAC Sets) und Sicherheitsgruppen, die entweder IP Sets oder MAC Sets enthalten, sind keine gültigen Eingabeparameter.

- 13 Klicken Sie auf **Änderungen speichern**.

Bearbeiten einer Distributed Firewall-Regel

Verwenden Sie in einer vCloud Director-Umgebung zum Ändern einer vorhandenen Distributed Firewall-Regel eines virtuellen Organisations-Datencenters den Bildschirm **Distributed Firewall**.


Weitere Informationen zu den verfügbaren Einstellungen für die verschiedenen Zellen einer Regel finden Sie unter [Hinzufügen einer Distributed Firewall-Regel](#).

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie das VDC-Netzwerk für Sicherheitsdienste aus, für das Sie Firewallregeln ändern möchten, und klicken Sie auf **Dienste konfigurieren**.

Der Bildschirm „Sicherheitsdienste“ wird angezeigt.

- 3 Führen Sie eine der folgenden Aktionen aus, um Distributed Firewall-Regeln zu verwalten:

- Deaktivieren Sie eine Regel durch Klicken auf das grüne Häkchen in der Zelle **Nein**.
Das grüne Häkchen verwandelt sich in ein rotes Deaktiviert-Symbol. Wenn die Regel deaktiviert ist und Sie die Regel aktivieren möchten, klicken Sie auf das rote Deaktiviert-Symbol.
- Bearbeiten Sie einen Regelnamen, indem Sie auf die Zelle **Name** doppelklicken und den neuen Namen eingeben.
- Ändern Sie die Einstellungen für eine Regel, z. B. die Quell- oder Aktionseinstellungen, indem Sie die entsprechende Zelle auswählen und die angezeigten Steuerelemente verwenden.
- Löschen Sie eine Regel, indem Sie sie auswählen und oberhalb der Regeltabelle auf die Schaltfläche **Löschen** () klicken.

- Verschieben Sie eine Regel in der Regeltabelle nach oben oder unten, indem Sie die Regel auswählen und oberhalb der Regeltabelle auf eine der Schaltflächen mit dem Pfeil nach oben oder unten klicken.

4 Klicken Sie auf **Änderungen speichern**.

Verwalten des DHCP-Protokolls für Edge-Gateways

Sie konfigurieren die Edge-Gateways, um virtuellen Maschinen, die mit den zugeordneten VDC-Organisationsnetzwerken verbunden sind, DHCP-Dienste (Dynamic Host Configuration Protocol) bereitzustellen.

Wie in der [NSX-Dokumentation](#) beschrieben, gehören zu den Funktionen eines NSX-Edge-Gateways IP-Adresspools, die 1:1-Zuordnung statischer IP-Adressen und eine externe DNS-Server-Konfiguration. Die Bindung statischer IP-Adressen basiert auf der verwalteten Objekt- und Schnittstellen-ID der anfordernden virtuellen Client-Maschine.

Der DHCP-Dienst verfährt für ein NSX Edge-Gateway wie folgt:

- Überwacht die interne Schnittstelle des Edge-Gateways zum Zweck der DHCP-Erkennung.
- Verwendet die IP-Adresse der internen Schnittstelle des Edge-Gateways als standardmäßige Gateway-Adresse für alle Clients.
- Die Broadcast- und Subnetzmaskenwerte der internen Schnittstelle werden für das Containernetzwerk verwendet.

In den folgenden Situationen müssen Sie den DHCP-Dienst auf denjenigen virtuellen Client-Maschinen neu starten, die über von DHCP zugewiesene IP-Adressen verfügen:

- Sie haben einen DHCP-Pool, ein Standard-Gateway oder einen DNS-Server geändert bzw. gelöscht.
- Sie haben die interne IP-Adresse der Edge-Gateway-Instanz geändert.

Hinweis Wenn die DNS-Einstellungen eines für DHCP konfigurierten Edge-Gateways geändert werden, stellt das Edge-Gateway möglicherweise keine DHCP-Dienste mehr bereit. Wenn dieser Fall eintritt, verwenden Sie die Option **Status des DHCP-Diensts** auf dem Bildschirm „DHCP-Pools“, um DHCP auf dem Edge-Gateway zu deaktivieren und erneut zu aktivieren. Weitere Informationen finden Sie unter [Hinzufügen eines DHCP-IP-Pools](#).

Hinzufügen eines DHCP-IP-Pools

Sie können die für einen DHCP-Dienst eines erweiterten Edge-Gateways benötigten IP-Pools konfigurieren. DHCP automatisiert die Zuweisung von IP-Adressen zu virtuellen Maschinen, die mit VDC-Organisationsnetzwerken verbunden sind.

Wie in der *Administratordokumentation für NSX* beschrieben, benötigt der DHCP-Dienst einen Pool von IP-Adressen. Ein IP-Pool ist ein sequenzieller Bereich von IP-Adressen innerhalb des Netzwerks. Virtuelle Maschinen, die durch das Edge-Gateway geschützt werden und keine Adressbindung aufweisen, werden einer IP-Adresse aus diesem Pool zugewiesen. Bereiche eines IP-Pools können sich nicht mit anderen Bereichen überschneiden. Daher kann eine IP-Adresse nur zu einem IP-Pool gehören.

Hinweis Es muss mindestens ein DHCP-IP-Pool konfiguriert werden, damit der DHCP-Dienststatus aktiviert wird.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **DHCP > Pools**.
- 3 Falls der DHCP-Dienst derzeit nicht aktiviert ist, aktivieren Sie die Option **Status des DHCP-Diensts**.

Hinweis Nachdem Sie die Option **Status des DHCP-Diensts** aktiviert haben, fügen Sie mindestens einen DHCP-IP-Pool hinzu, bevor Sie die Änderungen speichern. Wenn auf dem Bildschirm keine DHCP-IP-Pools aufgelistet werden und Sie die Umschaltoption **Status des DHCP-Diensts** aktivieren sowie die Änderungen speichern, wird der Bildschirm mit deaktivierter Option angezeigt.

- 4 Klicken Sie unter „DHCP-Pools“ auf die Schaltfläche **Erstellen** () , geben Sie die Details für den DHCP-Pool ein und klicken Sie auf **Behalten**.

Option	Beschreibung
IP-Bereich	Geben Sie einen Bereich von IP-Adressen ein.
Domänenname	Domänenname des DNS-Servers.
DNS automatisch konfigurieren	Aktivieren Sie diese Umschaltoption, um die DNS-Dienstkonfiguration für die DNS-Bindung dieses IP-Pools zu verwenden. Wenn sie aktiviert ist, werden Primärer Namensserver und Sekundärer Namensserver auf Automatisch festgelegt.
Primärer Namensserver	Wenn Sie DNS automatisch konfigurieren nicht aktivieren, geben Sie die IP-Adresse des primären DNS-Servers ein. Diese IP-Adresse wird für die Auflösung von Hostnamen in IP-Adressen verwendet.
Sekundärer Namensserver	Wenn Sie DNS automatisch konfigurieren nicht aktivieren, geben Sie die IP-Adresse des sekundären DNS-Servers ein. Diese IP-Adresse wird für die Auflösung von Hostnamen in IP-Adressen verwendet.

Option	Beschreibung
Standard-Gateway	Geben Sie die Adresse des Standard-Gateways ein. Wenn Sie die IP-Adresse des Standard-Gateways nicht eingeben, wird die interne Schnittstelle der Edge-Gateway-Instanz als Standard-Gateway verwendet.
Subnetzmaske	Geben Sie die Subnetzmaske der Edge-Gateway-Schnittstelle ein.
Lease läuft nie ab	Aktivieren Sie diese Option, um die Bindung der aus diesem Pool zugewiesenen IP-Adressen an deren zugewiesene virtuelle Maschinen dauerhaft beizubehalten. Wenn Sie diese Option auswählen, wird die Lease-Zeit auf „Unendlich“ festgelegt.
Lease-Zeit (Sekunden)	Zeitdauer (in Sekunden), die die über DHCP zugewiesenen IP-Adressen für die Clients geleast werden. Die standardmäßige Lease-Zeit beträgt einen Tag (86.400 Sekunden). Hinweis Wenn Sie Lease läuft nie ab auswählen, können Sie keine Lease-Zeit angeben.

5 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

vCloud Director aktualisiert das Edge-Gateway, sodass DHCP-Dienste bereitgestellt werden.

Hinzufügen von DHCP-Bindungen

Wenn Sie über auf einer virtuellen Maschine ausgeführte Dienste verfügen, deren IP-Adresse nicht geändert werden soll, können Sie die MAC-Adresse der virtuellen Maschine an die IP-Adresse binden. Die IP-Adresse, die Sie binden, darf sich mit keinem DHCP-IP-Pool überschneiden.

Voraussetzungen

Sie verfügen über die MAC-Adressen für die virtuellen Maschinen, für die Sie Bindungen einrichten möchten.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.

2 Klicken Sie auf der Registerkarte **DHCP > Bindungen** auf die Schaltfläche **Erstellen**



() , geben Sie die Details für die Bindung an und klicken Sie auf **Behalten**.

Option	Beschreibung
MAC-Adresse	Geben Sie die MAC-Adresse der virtuellen Maschine ein, die an die IP-Adresse gebunden werden soll.
Hostname	Geben Sie den Hostnamen ein, den Sie für diese virtuelle Maschine festlegen möchten, wenn die virtuelle Maschine eine DHCP-Lease anfordert.
IP-Adresse	Geben Sie die IP-Adresse ein, die an die MAC-Adresse gebunden werden soll.
Subnetzmaske	Geben Sie die Subnetzmaske der Edge-Gateway-Schnittstelle ein.
Domänenname	Geben Sie den Domännennamen des DNS-Servers ein.
DNS automatisch konfigurieren	Aktivieren Sie diese Option, um die DNS-Dienstkonfiguration für diese DNS-Bindung zu verwenden. Wenn sie aktiviert ist, werden Primärer Namensserver und Sekundärer Namensserver auf Automatisch festgelegt.
Primärer Namensserver	Wenn Sie DNS automatisch konfigurieren nicht auswählen, geben Sie die IP-Adresse des primären DNS-Servers ein. Diese IP-Adresse wird für die Auflösung von Hostnamen in IP-Adressen verwendet.
Sekundärer Namensserver	Wenn Sie DNS automatisch konfigurieren nicht auswählen, geben Sie die IP-Adresse des sekundären DNS-Servers ein. Diese IP-Adresse wird für die Auflösung von Hostnamen in IP-Adressen verwendet.
Standard-Gateway	Geben Sie die Adresse des Standard-Gateways ein. Wenn Sie die IP-Adresse des Standard-Gateways nicht eingeben, wird die interne Schnittstelle der Edge-Gateway-Instanz als Standard-Gateway verwendet.
Lease läuft nie ab	Aktivieren Sie diese Option, damit die IP-Adresse dauerhaft an diese MAC-Adresse gebunden wird. Wenn Sie diese Option auswählen, wird die Lease-Zeit auf „Unendlich“ festgelegt.
Lease-Zeit (Sekunden)	Zeitdauer (in Sekunden), die die über DHCP zugewiesenen IP-Adressen für die Clients geleast werden. Die standardmäßige Lease-Zeit beträgt einen Tag (86.400 Sekunden). Hinweis Wenn Sie Lease läuft nie ab auswählen, können Sie keine Lease-Zeit angeben.

3 Klicken Sie auf **Änderungen speichern**.

Konfigurieren von DHCP-Relay für Edge-Gateways

Die DHCP-Relay-Funktion, die von NSX in Ihrer vCloud Director-Umgebung bereitgestellt wird, ermöglicht Ihnen die Nutzung Ihrer vorhandenen DHCP-Infrastruktur von Ihrer vCloud Director-Umgebung aus, ohne die IP-Adressverwaltung in der vorhandenen DHCP-Infrastruktur zu

unterbrechen. DHCP-Nachrichten werden von virtuellen Maschinen an die designierten DHCP-Server in Ihrer physischen DHCP-Infrastruktur übertragen. Dadurch wird ermöglicht, dass von der NSX-Software gesteuerte IP-Adressen weiter mit den IP-Adressen in den restlichen DHCP-gesteuerten Umgebungen synchronisiert bleiben.

In der DHCP-Relay-Konfiguration eines Edge-Gateways können verschiedene DHCP-Server aufgelistet werden. Anforderungen werden an alle aufgelisteten Server gesendet. Während der Übertragung der DHCP-Anforderung von den VMs fügt das Edge-Gateway der Anforderung eine Gateway-IP-Adresse hinzu. Der externe DHCP-Server verwendet diese Gateway-Adresse, um einen Pool abzugleichen und eine IP-Adresse für die Anforderung zuzuteilen. Die Gateway-Adresse muss zu einem Subnetz der Schnittstelle des Edge-Gateways gehören.

Sie können einen anderen DHCP-Server für jedes Edge-Gateway angeben und mehrere DHCP-Server auf jedem Edge-Gateway konfigurieren, um mehrere IP-Domänen zu unterstützen.

Hinweis

- DHCP-Relay unterstützt keine überlappenden IP-Adressbereiche.
 - DHCP-Relay und der DHCP-Dienst können nicht gleichzeitig auf der gleichen vNIC ausgeführt werden. Wenn ein Relay-Agent auf einer vNIC konfiguriert ist, kann kein DHCP-Pool in den Subnetzen dieser vNIC konfiguriert werden. Weitere Einzelheiten finden Sie im *NSX-Administratorhandbuch*.
-

Angeben einer DHCP-Relay-Konfiguration für ein Edge-Gateway

Die NSX-Software in Ihrer vCloud Director-Umgebung stellt dem Edge-Gateway die Funktionalität zur Relay-gestützten Weiterleitung von DHCP-Meldungen an DHCP-Server bereit, die sich außerhalb Ihres vCloud Director-Organisations-VDC befinden. Sie können die DHCP-Relay-Funktion des Edge-Gateways konfigurieren.

Wie in der *Administratordokumentation für NSX* beschrieben, können die DHCP-Server mithilfe eines vorhandenen IP Sets, eines IP-Adressblocks, einer Domäne oder einer Kombination aus diesen angegeben werden. DHCP-Meldungen werden an alle angegebenen DHCP-Server weitergeleitet.

Sie müssen auch mindestens einen DHCP-Relay-Agent konfigurieren. Ein DHCP-Relay-Agent ist eine Schnittstelle auf dem Edge-Gateway, von der aus die DHCP-Anforderungen an die externen DHCP-Server weitergeleitet werden.


Voraussetzungen

Wenn Sie mithilfe eines IP-Satzes einen DHCP-Server angeben möchten, stellen Sie sicher, dass der IP-Satz als dem Edge-Gateway zur Verfügung stehendes Gruppierungsobjekt vorhanden ist. Weitere Informationen finden Sie unter [Erstellen eines IP Sets zur Verwendung in Firewallregeln und bei der DHCP-Relay-Konfiguration](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **DHCP > Relay**.
- 3 Geben Sie die DHCP-Server in den Feldern auf dem Bildschirm anhand von IP-Adressen, Domännennamen oder IP Sets an.

Über die Schaltfläche **Hinzufügen** () können Sie vorhandene IP Sets auswählen und die verfügbaren IP Sets durchsuchen.

- 4 Konfigurieren Sie einen DHCP-Relay-Agent und fügen Sie die Konfiguration anschließend der Tabelle auf dem Bildschirm hinzu. Klicken Sie dazu auf die Schaltfläche **Hinzufügen** () , wählen Sie eine vNIC und deren Gateway-IP-Adresse aus und klicken Sie dann auf **Behalten**.

Die Gateway-IP-Adresse entspricht standardmäßig der primären Adresse der ausgewählten vNIC. Sie können die Standardeinstellung beibehalten oder eine alternative Adresse auswählen, falls auf dieser vNIC eine verfügbar ist.

- 5 Klicken Sie auf **Änderungen speichern**.

Verwalten der Netzwerkadressübersetzung mithilfe des Mandantenportals

Mithilfe der NSX -Software in der vCloud Director-Umgebung können die Edge-Gateways einen NAT-Dienst (Netzwerkadressübersetzung, Network Address Translation) zur Verfügung stellen. Mit dieser Funktion kann die Anzahl öffentlicher IP-Adressen verringert werden, die eine Organisation verwenden muss. Dies hat wirtschaftliche Vorteile und dient der Sicherheit.

Der NAT-Dienst des Edge-Gateways bietet die Möglichkeit, einer virtuellen Maschine oder einer Gruppe von virtuellen Maschinen in einem privaten Netzwerk eine öffentliche Adresse zuzuweisen. Um Ihre Edge-Gateways so zu konfigurieren, dass Zugriff auf Dienste gewährt wird, die auf privat zugänglichen virtuellen Maschinen in Ihrem Organisations-VDC ausgeführt werden, müssen Sie NAT-Regeln auf den Edge-Gateways konfigurieren. In den meisten Fällen ordnen Sie einen NAT-Dienst einer Uplink-Schnittstelle auf einem Edge-Gateway in der vCloud Director-Umgebung zu, sodass die Adressen in einem Organisations-VDC nicht im externen Netzwerk offengelegt werden.

Die Konfiguration des NAT-Diensts gliedert sich in SNAT- (Source NAT, Quell-NAT) und DNAT-Regeln (Destination NAT, Ziel-NAT). Bei der Konfiguration einer SNAT- oder DNAT-Regel auf einem Edge-Gateway in der vCloud Director-Umgebung konfigurieren Sie die Regel immer aus der Perspektive des virtuellen Datacenters Ihrer Organisation. Speziell bedeutet dies, dass Sie die Regeln auf folgende Arten konfigurieren können:

- **SNAT:** Der Datenverkehr wird von einer virtuellen Maschine in einem internen Netzwerk in Ihrem Organisations-VDC (der Quelle) über das Internet zum externen Netzwerk (dem Ziel) geleitet. Eine SNAT-Regel übersetzt die IP-Quelladresse der ausgehenden Pakete eines VDC-Organisationsnetzwerks, die an ein externes Netzwerk oder ein anderes VDC-Organisationsnetzwerk gesendet werden.
- **DNAT:** Der Datenverkehr wird aus dem Internet (der Quelle) an eine virtuelle Maschine innerhalb Ihres Organisations-VDC (das Ziel) geleitet. Eine DNAT-Regel übersetzt die IP-Adresse und optional den Port von Paketen, die von einem VDC-Organisationsnetzwerk empfangen werden und aus einem externen Netzwerk oder einem anderen VDC-Organisationsnetzwerk stammen.

Sie können NAT-Regeln konfigurieren, um einen privaten IP-Adressbereich innerhalb des Organisations-VDC zu erstellen. Diese Konfiguration bietet die Möglichkeit, einen privaten IP-Adressbereich aus einem Organisations-VDC in ein anderes zu portieren. Indem Sie NAT-Regeln konfigurieren, können Sie dieselben privaten IP-Adressen für Ihre virtuellen Maschinen in einem Organisations-VDC verwenden, die bereits in einem anderen Organisations-VDC verwendet wurden.

Die NAT-Regelfunktion in Ihrer vCloud Director-Umgebung unterstützt Folgendes:

- Erstellen von Subnetzen innerhalb des privaten IP-Adressbereichs
- Erstellen mehrerer privater IP-Adressbereiche für ein Edge-Gateway
- Konfigurieren mehrerer NAT-Regeln in mehreren Edge-Gateway-Schnittstellen

Wichtig Sie müssen sowohl Firewall- als auch NAT-Regeln auf einem Edge-Gateway konfigurieren, damit die virtuellen Maschinen in einem Edge-Gateway-Netzwerk zugänglich sind. Standardmäßig werden Edge-Gateways mit Firewallregeln bereitgestellt, die so konfiguriert sind, dass sämtlicher Netzwerkdatenverkehr zu und von den virtuellen Maschinen in den Edge-Gateway-Netzwerken abgelehnt wird. Darüber hinaus ist NAT standardmäßig auf den Edge-Gateways deaktiviert, sodass Edge-Gateways die IP-Adressen des ein- und ausgehenden Datenverkehrs nicht übersetzen können, es sei denn, Sie konfigurieren NAT auf den Edge-Gateways. Der Versuch, eine virtuelle Maschine in einem Netzwerk mittels Ping zu erreichen, nachdem eine NAT-Regel konfiguriert wurde, schlägt fehl, es sei denn, Sie fügen eine Firewallregel hinzu, um den entsprechenden Datenverkehr zuzulassen.

Hinzufügen einer SNAT- oder DNAT-Regel

Sie können eine Quell-NAT- bzw. SNAT-Regel erstellen, um die Quell-IP-Adresse von einer öffentlichen in eine private IP-Adresse zu ändern oder umgekehrt. Sie können eine Ziel-NAT- bzw.

DNAT-Regel erstellen, um die Ziel-IP-Adresse von einer öffentlichen in eine private IP-Adresse zu ändern oder umgekehrt.

Beim Erstellen von NAT-Regeln können Sie die ursprünglichen und übersetzten IP-Adressen mit den folgenden Formaten angeben:

- IP-Adresse – Beispiel: 192.0.2.0
- IP-Adressbereich – Beispiel: 192.0.2.0-192.0.2.24
- IP-Adresse/-Subnetzmaske – Beispiel: 192.0.2.0/24
- any

Bei der Konfiguration einer SNAT- oder DNAT-Regel auf einem Edge-Gateway in der vCloud Director-Umgebung konfigurieren Sie die Regel immer aus der Perspektive des virtuellen Datencenters Ihrer Organisation. Eine SNAT-Regel übersetzt die IP-Quelladresse von Paketen, die von einem VDC-Organisationsnetzwerk an ein externes Netzwerk oder an ein anderes VDC-Organisationsnetzwerk gesendet werden. Eine DNAT-Regel übersetzt die IP-Adresse und optional den Port von Paketen, die von einem VDC-Organisationsnetzwerk empfangen werden und aus einem externen Netzwerk oder einem anderen VDC-Organisationsnetzwerk stammen.

Voraussetzungen

Die öffentliche IP-Adresse muss bereits der Edge-Gateway-Schnittstelle, für die Sie die Regel hinzufügen möchten, hinzugefügt worden sein. Für DNAT-Regeln muss der Edge-Gateway-Schnittstelle die ursprüngliche (öffentliche) IP-Adresse hinzugefügt worden sein, für SNAT-Regeln die übersetzte (öffentliche) IP-Adresse.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf **NAT**, um den Bildschirm „NAT-Regeln“ anzuzeigen.
- 3 Klicken Sie je nach dem Typ der zu erstellenden NAT-Regel auf **DNAT-Regel** oder **SNAT-Regel**.

4 Konfigurieren Sie eine NAT-Zielregel (von außen nach innen).

Option	Beschreibung
Angewendet auf	Wählen Sie die Schnittstelle aus, auf die die Regel angewendet werden soll.
Ursprüngliche(r) IP/Bereich	Geben Sie die erforderliche IP-Adresse ein. Bei dieser Adresse muss es sich um die öffentliche IP-Adresse des Edge-Gateways handeln, für das Sie die DNAT-Regel konfigurieren. Im untersuchten Paket würde diese IP-Adresse oder dieser Bereich die Adressen umfassen, die als IP-Zieladresse des Pakets angezeigt werden. Bei diesen Paket-Zieladressen handelt es sich um die Adressen, die von dieser DNAT-Regel übersetzt werden.
Protokoll	Wählen Sie das Protokoll aus, auf das die Regel angewendet wird. Wenn die Regel für alle Protokolle gelten soll, wählen Sie Alle aus.
Ursprünglicher Port	(Optional) Wählen Sie den Port oder Portbereich aus, über den der eingehende Datenverkehr auf dem Edge-Gateway eine Verbindung zum internen Netzwerk herstellt, in dem die virtuellen Maschinen verbunden sind. Diese Auswahl ist nicht verfügbar, wenn Protokoll auf ICMP oder Alle festgelegt ist.
ICMP-Typ	Wenn Sie ICMP (ein Fehlerberichts- und Diagnose-Dienstprogramm für die geräteübergreifende Kommunikation von Fehlerinformationen) als Protokoll auswählen, wählen Sie im Dropdown-Menü die Option ICMP-Typ aus. ICMP-Meldungen werden anhand des Feldtyps identifiziert. Der ICMP-Typ ist standardmäßig auf „Alle“ festgelegt.
Übersetzte(r) IP/Bereich	Geben Sie die IP-Adresse oder einen Bereich von IP-Adressen ein, in die Zieladressen in eingehenden Paketen übersetzt werden. Bei diesen Adressen handelt es sich um die IP-Adressen der virtuellen Maschine(n), für die Sie DNAT konfigurieren, sodass sie Datenverkehr aus dem externen Netzwerk empfangen können.
Übersetzter Port	(Optional) Wählen Sie den Port oder Portbereich aus, zu dem eingehender Datenverkehr auf den virtuellen Maschinen im internen Netzwerk eine Verbindung herstellt. Dies sind die Ports, in die die DNAT-Regel die Übersetzung für die auf den virtuellen Maschinen eingehenden Pakete vornimmt.
Beschreibung	(Optional) Geben Sie eine Beschreibung ein, anhand derer die Funktionsweise dieser Regel identifiziert werden kann.
Aktiviert	Aktivieren Sie diese Option, um diese Regel zu aktivieren.
Protokollierung aktivieren	Aktivieren Sie diese Option, damit die Adressübersetzung dieser Regel protokolliert wird.

5 Konfigurieren Sie eine NAT-Quellregel (von innen nach außen).

Option	Beschreibung
Angewendet auf	Wählen Sie die Schnittstelle aus, auf die die Regel angewendet werden soll.
Ursprüngliche(r) Quell-IP/ Quellbereich	Geben Sie die ursprüngliche IP-Adresse oder einen Bereich von IP-Adressen an, die auf diese Regel angewendet werden sollen. Bei diesen Adressen handelt es sich um die IP-Adressen der virtuellen Maschinen, für die Sie die SNAT-Regel konfigurieren, damit diese Datenverkehr an das externe Netzwerk senden können.
Übersetzte(r) Quell-IP/Quellbereich	Geben Sie die erforderliche IP-Adresse ein. Bei dieser Adresse handelt es sich immer um die öffentliche IP-Adresse des Gateways, für das Sie die SNAT-Regel konfigurieren. Gibt die IP-Adresse an, in die Quelladressen (die virtuellen Maschinen) in ausgehenden Paketen übersetzt werden, wenn sie Datenverkehr an das externe Netzwerk senden.
Beschreibung	(Optional) Geben Sie eine Beschreibung ein, anhand derer die Funktionsweise dieser Regel identifiziert werden kann.
Aktiviert	Aktivieren Sie diese Option, um diese Regel zu aktivieren.
Protokollierung aktivieren	Aktivieren Sie diese Option, damit die Adressübersetzung dieser Regel protokolliert wird.

6 Klicken Sie auf **Behalten**, um die Regel der Tabelle auf dem Bildschirm hinzuzufügen.

7 Wiederholen Sie die Schritte, um weitere Regeln zu konfigurieren.

8 Klicken Sie auf **Änderungen speichern**, um die Regeln im System zu speichern.

Nächste Schritte

Fügen Sie die entsprechenden Edge-Gateway-Firewallregeln für die SNAT- oder DNAT-Regeln hinzu, die Sie soeben konfiguriert haben. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Konfiguration für erweitertes Routing

Sie können die statischen und dynamischen Routing-Funktionen konfigurieren, die von der NSX-Software für Ihre Edge-Gateways bereitgestellt werden.

Zur Aktivierung des dynamischen Routings konfigurieren Sie mit dem BGP- (Border Gateway Protocol) oder dem OSPF-Protokoll (Open Shortest Path First) ein erweitertes Edge-Gateway.

Detaillierte Informationen zu den von NSX bereitgestellten Routing-Funktionen finden Sie in der *Administratordokumentation für NSX* unter *Routing*.

Sie können für jedes erweiterte Edge-Gateway statisches und dynamisches Routing angeben. Die dynamische Routing-Funktion stellt die erforderlichen Weiterleitungsinformationen zwischen Layer-2-Broadcast-Domänen zur Verfügung. Auf diese Weise können Sie die Anzahl der Layer-2-Broadcast-Domänen verringern und die Netzwerkeffizienz und -skalierung verbessern. NSX erweitert diese Funktion auf die Speicherorte der Arbeitslasten für horizontales Routing. Diese Funktion ermöglicht mehr direkte Kommunikation zwischen virtuellen Maschinen, ohne dass hierbei der für die Erweiterung von Hops erforderliche Kosten- oder Zeitaufwand entsteht.

Angeben von Standard-Routing-Konfigurationen für das Edge-Gateway

Sie können die Standardeinstellungen für statisches und dynamisches Routing für ein Edge-Gateway angeben.

Hinweis Um alle konfigurierten Routing-Einstellungen zu entfernen, verwenden Sie die Schaltfläche **Globale Konfiguration löschen** unten im Bildschirm **Routing-Konfiguration**. Diese Aktion löscht alle auf den Unterbildschirmen aktuell angegebenen Routing-Einstellungen: Standard-Routing-Einstellungen, statische Routen, OSPF, BGP und Route Redistribution.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Routing > Routing-Konfiguration**.
- 3 Um das Equal Cost Multipath (ECMP)-Routing für dieses Edge-Gateway zu aktivieren, aktivieren Sie die Option **ECMP**.

Wie in der Dokumentation für *NSX-Administratoren* beschrieben, ist ECMP eine Routing-Strategie, mit der eine Next-Hop-Paketweiterleitung an ein einzelnes Ziel über mehrere bestmögliche Pfade stattfinden kann. NSX bestimmt diese bestmöglichen Pfade entweder statisch unter Verwendung von konfigurierten statischen Routen oder als Ergebnis von Metrikberechnungen durch dynamische Routing-Protokolle wie OSPF oder BGP. Sie können mehrere Pfade für statische Routen auswählen, indem Sie mehrere Next-Hop-Werte auf dem Bildschirm „Statische Routen“ angeben.

Weitere Informationen zu ECMP und NSX finden Sie in den Routing-Themen im *Fehlerbehebungshandbuch zu NSX*.

4 Geben Sie die Einstellungen für das Standard-Routing-Gateway an.

- a Verwenden Sie die Dropdown-Liste **Angewendet auf**, um eine Schnittstelle auszuwählen, von der aus der Next-Hop in Richtung des Zielnetzwerks erreicht werden kann.

Um Details zu der ausgewählten Schnittstelle anzuzeigen, klicken Sie auf das blaue Info-Symbol.

- b Geben Sie die Gateway-IP-Adresse ein.
- c Geben Sie den MTU-Wert ein.
- d (Optional) Geben Sie eine optionale Beschreibung ein.
- e Klicken Sie auf **Änderungen speichern**.

5 Geben Sie die dynamischen Standard-Routing-Einstellungen an.

Hinweis Wenn in Ihrer Umgebung IPsec-VPN konfiguriert ist, sollten Sie kein dynamisches Routing verwenden.

- a Wählen Sie eine Router-ID aus.

Sie können eine Router-ID in der Liste auswählen oder das Plussymbol (+) verwenden, um eine neue ID einzugeben. Diese Router-ID ist die erste Uplink-IP-Adresse des Edge-Gateways, die Routen zum Kernel für dynamisches Routing überträgt.

- b Konfigurieren Sie die Protokollierung, indem Sie die Option **Protokollierung aktivieren** aktivieren und die Protokollierungsebene auswählen.
- c Klicken Sie auf **OK**.

6 Klicken Sie auf **Änderungen speichern**.

Nächste Schritte

Fügen Sie statische Routen hinzu. Weitere Informationen finden Sie unter [Hinzufügen einer statischen Route](#).

Konfigurieren Sie die Route Redistribution. Weitere Informationen finden Sie unter [Konfigurieren der Route Redistribution](#).

Konfigurieren Sie dynamisches Routing. Lesen Sie hierzu auch folgende Themen:

- [Konfigurieren des BGP-Protokolls](#)
- [Konfigurieren des OSPF-Protokolls](#)

Hinzufügen einer statischen Route


Sie können eine statische Route für ein Zielsubnetz oder einen Zielhost hinzufügen.

Wenn ECMP in der standardmäßigen Routing-Konfiguration aktiviert ist, können Sie mehrere nächste Hops in den statischen Routen angeben. Die Schritte zur Aktivierung von ECMP sind unter [Angaben von Standard-Routing-Konfigurationen für das Edge-Gateway](#) beschrieben.

Voraussetzungen

Wie in der NSX-Dokumentation beschrieben, muss die IP-Adresse des nächsten Hops der statischen Route in einem Subnetz vorhanden sein, das einer der Edge-Gateway-Schnittstellen zugeordnet ist. Andernfalls schlägt die Konfiguration dieser statischen Route fehl.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Routing > Statische Routen**.
- 3 Klicken Sie auf die Schaltfläche **Erstellen** ().
- 4 Konfigurieren Sie die folgenden Optionen für die statische Route:

Option	Beschreibung
Netzwerk	Geben Sie das Netzwerk in CIDR-Notation ein.
Nächster Hop	Geben Sie die IP-Adresse des nächsten Hops ein. Die IP-Adresse des nächsten Hops muss in einem Subnetz vorhanden sein, das einer der Edge-Gateway-Schnittstellen zugeordnet ist. Wenn ECMP aktiviert ist, können Sie mehrere nächste Hops eingeben.
MTU	Bearbeiten Sie den maximalen Übertragungswert für Datenpakete. Der MTU-Wert darf nicht höher als der für die ausgewählte Edge-Gateway-Schnittstelle festgelegte MTU-Wert sein. Sie können den für die Edge-Gateway-Schnittstelle festgelegten MTU-Wert standardmäßig im Bildschirm „Routing-Konfiguration“ anzeigen.
Schnittstelle	Wählen Sie optional die Edge-Gateway-Schnittstelle aus, der Sie eine statische Route hinzufügen möchten. Standardmäßig ist die Schnittstelle ausgewählt, die der Adresse des nächsten Hops entspricht.
Beschreibung	Geben Sie optional eine Beschreibung für die statische Route ein.

- 5 Klicken Sie auf **Änderungen speichern**.

Nächste Schritte

Konfigurieren Sie eine NAT-Regel für die statische Route. Weitere Informationen finden Sie unter [Hinzufügen einer SNAT- oder DNAT-Regel](#).

Fügen Sie eine Firewallregel hinzu, damit Datenverkehr die statische Route durchlaufen darf. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Konfigurieren des OSPF-Protokolls

Sie können das OSPF-Routing-Protokoll (Open Shortest Path First) für die dynamischen Routing-Funktionen eines Edge-Gateways konfigurieren. Eine häufige Anwendung von OSPF

auf einem Edge-Gateway in einer vCloud Director-Umgebung besteht im Austausch von Routing-Informationen zwischen Edge-Gateways in vCloud Director.

Das NSX-Edge-Gateway unterstützt OSPF, ein internes Gateway-Protokoll, das IP-Pakete nur innerhalb einer einzelnen Routing-Domäne weiterleitet. Wie in der *Administratordokumentation für NSX* beschrieben, ermöglicht das Konfigurieren von OSPF auf einem NSX-Edge-Gateway es dem Edge-Gateway, Routen zu erlernen und anzukündigen. Das Edge-Gateway verwendet OSPF, um Informationen zum Verbindungszustand von verfügbaren Edge-Gateways zu erfassen und eine Topologiezuordnung des Netzwerks zu erstellen. Die Topologie bestimmt die Routing-Tabelle, die dem Internet Layer präsentiert wird, der Routing-Entscheidungen auf der Grundlage der in den IP-Paketen gefundenen IP-Adresse des Ziels trifft.

Daher bieten OSPF-Routing-Richtlinien einen dynamischen Vorgang des Datenverkehrs-Lastausgleichs zwischen Routen gleicher Kosten. Ein OSPF-Netzwerk ist in Routing-Bereiche aufgeteilt, um den Datenverkehr zu optimieren und die Größe der Routing-Tabellen zu begrenzen. Ein Bereich ist eine logische Sammlung von OSPF-Netzwerken, Routern und Links, die über dieselbe Bereichsidentifikation verfügen. Bereiche werden nach einer Bereichs-ID identifiziert.

Voraussetzungen

Eine Router-ID muss konfiguriert werden. [Angaben von Standard-Routing-Konfigurationen für das Edge-Gateway](#).

Verfahren


- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Routing > OSPF**.
- 3 Wenn OSPF derzeit nicht aktiviert ist, verwenden Sie die Option **OSPF aktiviert**, um es zu aktivieren.
- 4 Konfigurieren Sie die OSPF-Einstellungen entsprechend den Anforderungen Ihrer Organisation.

Option	Beschreibung
Graceful Restart aktivieren	Gibt an, dass Paketweiterleitung ununterbrochen beibehalten wird, wenn OSPF-Dienste neu gestartet werden.
Default Originate aktivieren	Ermöglicht es dem Edge-Gateway, sich selbst als Standard-Gateway für seine OSPF-Peers anzukündigen.

- 5 (Optional) Sie können auf **Änderungen speichern** klicken oder mit dem Konfigurieren von Bereichsdefinitionen und Schnittstellenzuordnungen fortfahren.

6 Fügen Sie eine OSPF-Area-Definition hinzu, indem Sie auf die Schaltfläche **Hinzufügen**



() klicken, Details für die Zuordnung im Dialogfeld angeben und auf **Behalten** klicken.


Hinweis Standardmäßig konfiguriert das System einen Bereich „Not-So-Stubby Area“ (NSSA) mit der Bereichs-ID 51, und dieser Bereich wird automatisch in der Tabelle der Bereichsdefinitionen auf dem OSPF-Bildschirm angezeigt. Sie können den NSSA-Bereich ändern oder löschen.

Option	Beschreibung
Bereichs-ID	Geben Sie eine Bereichs-ID in Form einer IP-Adresse oder Dezimalzahl ein.
Bereichstyp	<p>Wählen Sie Normal oder NSSA aus.</p> <p>NSSAs verhindern das Überfluten mit Hinweisen zum AS-externen Verbindungszustand (LSAs) in NSSAs. Sie verlassen sich auf das Standardrouting zu externen Zielen. Daher müssen NSSAs am Rand einer OSPF-Routing-Domäne platziert werden. NSSA kann externe Routen in die OSPF-Routing-Domäne importieren und somit Datenverkehrsdienste für kleine Routing-Domänen bereitstellen, die nicht zur OSPF-Routing-Domäne gehören.</p>
Bereichsauthentifizierung	<p>Wählen Sie den Typ der Authentifizierung für OSPF aus, die auf Bereichsebene durchgeführt werden soll.</p> <p>Für alle Edge-Gateways innerhalb des Bereichs müssen dieselbe Authentifizierung und das entsprechende Kennwort konfiguriert sein. Damit die MD5-Authentifizierung funktioniert, müssen der Empfänger und der Sender über denselben MD5-Schlüssel verfügen.</p> <p>Zur Auswahl stehen:</p> <ul style="list-style-type: none"> ■ Keine <p>Es ist keine Authentifizierung erforderlich.</p> ■ Kennwort <p>Mit dieser Option wird das Kennwort, das Sie im Feld Bereichsauthentifizierungswert angeben, in das übertragene Paket aufgenommen.</p> ■ MD5 <p>Mit dieser Option verwendet die Authentifizierung MD5 (Message Digest Type 5)-Verschlüsselung. Ein MD5-Prüfsummenwert wird in das übertragene Paket eingeschlossen. Geben Sie den MD5-Schlüssel in das Feld Bereichsauthentifizierungswert ein.</p>

7 Klicken Sie auf **Änderungen speichern**, sodass die neu konfigurierten Bereichsdefinitionen zur Auswahl verfügbar sind, wenn Sie Schnittstellenzuordnungen hinzufügen.

8 Fügen Sie eine Schnittstellenzuordnung hinzu, indem Sie auf die Schaltfläche **Hinzufügen**



() klicken, Details für die Zuordnung im Dialogfeld angeben und auf **Behalten** klicken.

Diese Zuordnungen ordnen den Bereichen die Schnittstellen des Edge-Gateways zu.

- a Wählen Sie im Dialogfeld die Schnittstelle aus, die Sie einer Bereichsdefinition zuordnen möchten.

Die Schnittstelle gibt das externe Netzwerk an, mit dem beide Edge-Gateways verbunden sind.

- b Wählen Sie die Bereichs-ID für den Bereich aus, um die ausgewählte Schnittstelle zuzuordnen.
- c (Optional) Ändern Sie die Standardwerte der OSPF-Einstellungen, um sie an diese Schnittstellenzuordnung anzupassen.

Wenn eine neue Zuordnung konfiguriert wird, werden die Standardwerte für diese Einstellungen angezeigt. In den meisten Fällen wird empfohlen, die Standardeinstellungen beizubehalten. Wenn Sie die Einstellungen ändern, stellen Sie sicher, dass die OSPF-Peers dieselben Einstellungen verwenden.

Option	Beschreibung
Hello-Intervall	Intervall (in Sekunden) zwischen Hello-Paketen, die auf der Schnittstelle gesendet werden.
Dead-Intervall	Intervall (in Sekunden), während dessen mindestens ein Hello-Paket von einem Nachbarn empfangen werden muss, bevor der Nachbar als ausgefallen gilt.
Priorität	Priorität der Schnittstelle. Die Schnittstelle mit der höchsten Priorität ist der designierte Edge-Gateway-Router.
Kosten	Overhead, der zum Senden von Paketen über die Schnittstelle erforderlich ist. Die Kosten einer Schnittstelle sind umgekehrt proportional zur Bandbreite dieser Schnittstelle. Je größer die Bandbreite, desto geringer sind die Kosten.

- d Klicken Sie auf **Behalten**.

9 Klicken Sie im OSPF-Bildschirm auf **Änderungen speichern**.

Nächste Schritte

Konfigurieren Sie OSPF auf den anderen Edge-Gateways, mit denen Sie Routing-Informationen austauschen möchten.

Fügen Sie eine Firewallregel hinzu, die Datenverkehr zwischen den mit OSPF konfigurierten Edge-Gateways zulässt. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Stellen Sie sicher, dass Route Redistribution und Firewall-Konfiguration das Ankündigen der richtigen Routen zulassen. Weitere Informationen finden Sie unter [Konfigurieren der Route Redistribution](#).

Konfigurieren des BGP-Protokolls

Sie können das BGP-Protokoll (Border Gateway Protocol) für die dynamischen Routing-Funktionen eines Edge-Gateways konfigurieren.

Wie im *NSX-Administratorhandbuch* beschrieben, trifft BGP wichtige Routing-Entscheidungen mithilfe einer Tabelle mit IP-Netzwerken oder -Präfixen, die die Erreichbarkeit des Netzwerks unter verschiedenen autonomen Systemen festlegen. Auf dem Gebiet der Netzwerke bezieht sich der Begriff „BGP-Speaker“ auf ein Netzwerkgerät, das BGP ausführt. Zwei BGP-Speaker stellen eine Verbindung her, bevor Routing-Informationen ausgetauscht werden. Der Begriff „BGP-Nachbar“ bezieht sich auf einen BGP-Speaker, der eine solche Verbindung hergestellt hat. Nachdem die Verbindung hergestellt wurde, tauschen die Geräte Routen aus und synchronisieren ihre Tabellen. Jedes Gerät sendet Keep-Alive-Nachrichten, um diese Beziehung aufrecht zu erhalten.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Routing > BGP**.
- 3 Wenn BGP derzeit nicht aktiviert ist, verwenden Sie die Option **BGP aktivieren**, um es zu aktivieren.


4 Konfigurieren Sie die BGP-Einstellungen entsprechend den Anforderungen Ihrer Organisation.

Option	Beschreibung
Graceful Restart aktivieren	Gibt an, dass die Paketweiterleitung ununterbrochen beibehalten wird, wenn BGP-Dienste neu gestartet werden.
Default Originate aktivieren	Ermöglicht es dem Edge-Gateway, sich selbst als Standard-Gateway für seine BGP-Nachbarn anzukündigen.
Lokales AS	<p>Diese Angabe ist erforderlich. Geben Sie die ID-Nummer des autonomen Systems (AS) an, die für die lokale AS-Funktion des Protokolls verwendet werden soll. Der von den Ihnen angegebene Wert muss eine global eindeutige Zahl zwischen 1 und 65534 sein.</p> <p>Das lokale AS ist eine Funktion von BGP. Das System weist die lokale AS-Nummer dem Edge-Gateway zu, das Sie konfigurieren. Das Edge-Gateway kündigt diese ID an, wenn das Edge-Gateway als Peer seiner BGP-Nachbarn in anderen autonomen Systemen fungiert. Der Pfad der autonomen Systeme, die eine Route durchlaufen würde, wird als eine Metrik im dynamischen Routing-Algorithmus verwendet, wenn der beste Pfad zum Ziel ausgewählt wird.</p>

5 Sie können entweder auf **Änderungen speichern** klicken oder weitere Einstellungen für die BGP-Routing-Nachbarn konfigurieren.

6 Fügen Sie eine BGP-Nachbarkonfiguration hinzu, indem Sie auf die Schaltfläche **Hinzufügen**



() klicken, Details für den Nachbarn im Dialogfeld angeben und auf **Behalten** klicken.

Option	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse eines BGP-Nachbarn für dieses Edge-Gateway ein.
Remote-AS	Geben Sie eine global eindeutige Nummer zwischen 1 und 65534 für das autonome System ein, zu dem dieser BGP-Nachbar gehört. Diese Remote-AS-Nummer wird im Eintrag des BGP-Nachbarn in der Tabelle für BGP-Nachbarn des Systems verwendet.
Gewichtung	Die Standardgewichtung für die Nachbarverbindung. Sie kann entsprechend den Bedürfnissen Ihrer Organisation angepasst werden.
Keep Alive-Zeit	Die Häufigkeit, mit der die Software Keep-Alive-Nachrichten an den Peer sendet. Die Standardhäufigkeit beträgt 60 Sekunden. Nehmen Sie die Anpassungen entsprechend den Anforderungen Ihrer Organisation vor.

Option	Beschreibung
Hold Down-Zeit	<p>Das Intervall, für das die Software einen Peer als ausgefallen einstuft, nachdem keine Keepalive-Nachricht erhalten wurde. Dieses Intervall muss dreimal so lang wie das Keepalive-Intervall sein. Das Standardintervall beträgt 180 Sekunden. Nehmen Sie die Anpassungen entsprechend den Anforderungen Ihrer Organisation vor.</p> <p>Sobald Peering zwischen zwei BGP-Nachbarn erreicht ist, startet das Edge-Gateway einen Hold Down-Timer. Jede Keepalive-Nachricht, die es von einem Nachbarn empfängt, setzt den Hold Down-Timer auf 0 zurück. Wenn das Edge-Gateway drei aufeinander folgende Keepalive-Nachrichten nicht empfängt und somit der Hold Down-Timer das Dreifache des Keepalive-Intervalls erreicht, betrachtet das Edge-Gateway den Nachbarn als ausgefallen und löscht die Routen aus diesem Nachbarn.</p>
Kennwort	<p>Wenn dieser BGP-Nachbar Authentifizierung erfordert, geben Sie das Authentifizierungskennwort ein.</p> <p>Jedes Segment, das über die Verbindung zwischen Nachbarn gesendet wird, wird überprüft. MD5-Authentifizierung muss mit demselben Kennwort auf beiden BGP-Nachbarn konfiguriert sein, andernfalls kann die Verbindung zwischen ihnen nicht hergestellt werden.</p>
BGP-Filter	<p>Verwenden Sie diese Tabelle, um Routenfilterung anhand einer Präfixliste von diesem BGP-Nachbarn anzugeben.</p> <p>Vorsicht Eine Regel des Typs <code>Alle blockieren</code> wird am Ende der Filter erzwungen.</p> <p>Fügen Sie einen Filter zur Tabelle hinzu, indem Sie auf das Plussymbol (+) klicken und die Optionen konfigurieren. Klicken Sie auf Behalten, um jeden Filter zu speichern.</p> <ul style="list-style-type: none"> ■ Wählen Sie die Richtung aus, um anzugeben, ob Sie den Datenverkehr zu oder von einem Nachbarn filtern. ■ Wählen Sie die Aktion, um anzugeben, ob Sie Datenverkehr zulassen oder verweigern. ■ Geben Sie das Netzwerk an, das Sie zu oder von einem Nachbarn filtern möchten. Geben Sie <code>ANY</code> oder ein Netzwerk im CIDR-Format ein. ■ Geben Sie das IP-Präfix-GE und IP-Präfix-LE ein, um die Schlüsselwörter <code>le</code> und <code>ge</code> in der Liste der IP-Präfixe zu verwenden.

7 Klicken Sie auf **Änderungen speichern**, um die Konfigurationen im System zu speichern.

Nächste Schritte

Konfigurieren Sie BGP auf den anderen Edge-Gateways, mit denen Sie Routing-Informationen austauschen möchten.



Fügen Sie eine Firewallregel hinzu, die Datenverkehr zu und von den mit BGP konfigurierten Edge-Gateways zulässt. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Konfigurieren der Route Redistribution

Standardmäßig gibt der Router nur Routen für andere Router frei, auf denen dasselbe Protokoll ausgeführt wird. Wenn Sie eine Umgebung mit mehreren Protokollen erstellt haben, müssen Sie

die Route Redistribution mit protokollübergreifender Routenfreigabe konfigurieren. Sie können die Route Redistribution für ein Edge-Gateway konfigurieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Routing > Route Redistribution**.
- 3 Verwenden Sie die Protokolloptionen, um die Protokolle zu aktivieren, für die Sie Route Redistribution aktivieren möchten.
- 4 Fügen Sie IP-Präfixe zur Tabelle auf dem Bildschirm hinzu.
 - a Klicken Sie auf die Schaltfläche **Hinzufügen** ().
 - b Geben Sie einen Namen und die IP-Adresse des Netzwerks im CIDR-Format ein.
 - c Klicken Sie auf **Behalten**.
- 5 Geben Sie Neuverteilungskriterien für jedes IP-Präfix an, indem Sie auf die Schaltfläche **Hinzufügen** () klicken, die Kriterien im Dialogfeld angeben und auf **Behalten** klicken.

Einträge in der Tabelle werden nacheinander verarbeitet. Mithilfe der Aufwärts- und Abwärtspfeile können Sie die Reihenfolge anpassen.

Option	Beschreibung
Präfixname	Wählen Sie ein bestimmtes IP-Präfix aus, um diese Kriterien darauf anzuwenden, oder wählen Sie Alle aus, um die Kriterien auf alle Netzwerkrouen anzuwenden.
Learner-Protokoll	Wählen Sie das Protokoll, das Routen von anderen Protokollen unter diesen Neuverteilungskriterien erlernen soll.
Lernen zulassen von	Wählen Sie die Typen von Netzwerken aus, von denen Routen für das in der Liste Learner-Protokoll ausgewählte Protokoll gelernt werden können.
Aktion	Wählen Sie, ob Neuverteilung vom ausgewählten Netzwerktyp zugelassen werden soll oder nicht.

- 6 Klicken Sie auf **Änderungen speichern**.

Lastausgleich

Der Lastausgleichsdienst verteilt eingehende Dienstanforderungen an mehrere Server und sorgt dabei dafür, dass die Lastverteilung für den Benutzer erkennbar ist. Der Lastausgleich

ermöglicht eine optimale Ressourcennutzung, maximalen Durchsatz und minimale Antwortzeiten und verhindert gleichzeitig eine Überlastung.

Lastausgleich

Der NSX-Lastausgleichsdienst unterstützt zwei Lastausgleichsmodule. Der Ebene-4-Lastausgleich ist paketbasiert und bietet Fast-Path-Verarbeitung. Der Ebene-7-Lastausgleich ist Socket-basiert und unterstützt erweiterte Strategien zur Verwaltung des Datenverkehrs und die DDOS-Minimierung für Back-End-Dienste.

Der Lastausgleich für ein Edge-Gateway wird in der externen Schnittstelle konfiguriert, da das Edge-Gateway den Lastausgleich für den eingehenden Datenverkehr vom externen Netzwerk durchführt. Wenn Sie virtuelle Server für den Lastausgleich konfigurieren, geben Sie eine der verfügbaren IP-Adressen an, über die Sie in Ihrem Organisations-VDC verfügen. Weitere Informationen dazu finden Sie im *vCloud Director-Benutzerhandbuch*.

Strategien und Konzepte für den Lastausgleich

Eine paketbasierte Lastausgleichsstrategie wird auf der TCP- und der UDP-Ebene implementiert. Paketbasierter Lastausgleich hält die Verbindung weder an noch puffert er die gesamte Anforderung. Stattdessen sendet er das geänderte Paket direkt an den ausgewählten Server. TCP- und UDP-Sitzungen werden im Lastausgleichsdienst beibehalten, sodass Pakete für eine einzelne Sitzung an denselben Server geleitet werden. Sie können „Beschleunigung aktiviert“ sowohl in der globalen Konfiguration als auch in der entsprechenden Konfiguration des virtuellen Servers auswählen, um den paketbasierten Lastausgleich zu aktivieren.

Eine Socket-basierte Lastausgleichsstrategie wird zusätzlich zu der Socket-Schnittstelle implementiert. Es werden zwei Verbindungen für eine einzelne Anforderung eingerichtet, nämlich eine clientseitige und eine serverseitige Verbindung. Die serverseitige Verbindung wird nach der Serverauswahl eingerichtet. Bei der HTTP-Socket-basierten Implementierung wird die gesamte Anforderung vor dem Senden an den ausgewählten Server mit optionaler L7-Verarbeitung empfangen. Bei der HTTPS-Socket-Implementierung werden die Authentifizierungsinformationen entweder über die clientseitige Verbindung oder über die serverseitige Verbindung ausgetauscht. Der Socket-basierte Lastausgleich ist der Standardmodus für virtuelle TCP-, HTTP- und HTTPS-Server.

Die grundlegenden Konzepte des NSX-Lastausgleichs sind virtueller Server, Serverpool, Serverpoolmitglied und Dienstüberwachung.

Virtueller Server

Zusammenfassender Begriff für einen Anwendungsdienst, der durch eine eindeutige Kombination aus IP, Port, Protokoll und Anwendungsprofil wie TCP oder UDP dargestellt wird.

Serverpool

Gruppe von Back-End-Servern.

Serverpoolmitglied

Stellt den Back-End-Server als Mitglied in einem Pool dar.

Dienstüberwachung

Definiert, wie der Systemzustand eines Back-End-Servers untersucht wird.

Anwendungsprofil

Stellt die TCP-, UDP-, Persistenz- und Zertifikatkonfiguration für eine bestimmte Anwendung dar.

Übersicht über die Einrichtung

Zunächst legen Sie globale Optionen für den Lastausgleichsdienst fest. Sie erstellen nun einen Serverpool, der aus Back-End-Server-Mitgliedern besteht, und ordnen dem Pool eine Dienstüberwachung zu, damit die Back-End-Server effizient verwaltet und gemeinsam genutzt werden können.

Anschließend erstellen Sie ein Anwendungsprofil, um das allgemeine Anwendungsverhalten in einem Lastausgleichsdienst – Client-SSL, Server-SSL, X-Forwarded-For oder Persistenz – zu definieren. Bei Wahl von Persistenz werden nachfolgende Anforderungen mit ähnlichen Merkmalen gesendet – beispielsweise dass Quell-IP oder Cookie an dasselbe Poolmitglied gesendet werden müssen, ohne dass der Lastausgleichsalgorithmus ausgeführt wird. Das Anwendungsprofil kann auf allen virtuellen Servern wiederverwendet werden.

Anschließend erstellen Sie eine optionale Anwendungsregel, um anwendungsspezifische Einstellungen für die Manipulation von Datenverkehr zu konfigurieren: beispielsweise das Abgleichen eines bestimmten URL- oder Hostnamens, sodass verschiedene Anforderungen von verschiedenen Pools verarbeitet werden können. Anschließend erstellen Sie eine Dienstüberwachung speziell für Ihre Anwendung oder verwenden ggf. eine bereits vorhandene Dienstüberwachung, falls diese Ihre Anforderungen erfüllt.

Optional können Sie eine Anwendungsregel zur Unterstützung von erweiterten Funktionen virtueller L7-Server erstellen. Einige Anwendungsfälle für Anwendungsregeln beinhalten das Wechseln von Inhalten, die Kopfzeilenmanipulation, Sicherheitsregeln und DOS-Schutz.

Abschließend erstellen Sie einen virtuellen Server, der Ihren Serverpool, das Anwendungsprofil und potenzielle Anwendungsregeln miteinander verbindet.

Wenn der virtuelle Server eine Anforderung erhält, berücksichtigt der Lastausgleichsalgorithmus die Poolmitgliedskonfiguration und den Laufzeitstatus. Der Algorithmus berechnet dann den entsprechenden Pool für die Verteilung des Datenverkehrs für ein oder mehrere Mitglieder. Zur Poolmitgliedskonfiguration gehören Einstellungen wie Gewichtung, maximale Verbindung und Bedingungsstatus. Der Laufzeitstatus beinhaltet die aktuellen Verbindungen, die Antwortzeit und Informationen über den Systemstatus. Die Berechnungsmethoden können Round-Robin, gewichtetes Round-Robin, schwächste Verbindung, Quell-IP-Hash, gewichtete schwächste Verbindungen, URL, URI oder HTTP-Header sein.

Jeder Pool wird von der zugehörigen Dienstüberwachung überwacht. Wenn der Lastausgleichsdienst ein Problem bei einem Poolmitglied erkennt, wird das Mitglied als „Nicht erreichbar“ markiert. Beim Auswählen eines Poolmitglieds aus dem Serverpool wird nur ein Server ausgewählt, der als „Erreichbar“ gekennzeichnet ist. Wenn der Serverpool nicht mit einer Dienstüberwachung konfiguriert ist, werden alle Poolmitglieder als „Erreichbar“ betrachtet.

Konfigurieren des Lastausgleichsdiensts

Zu den globalen Konfigurationsparametern des Lastausgleichsdiensts zählen die allgemeine Aktivierung, die Auswahl der Engine für Layer 4 oder Layer 7 und die Angabe der zu protokollierenden Ereignistypen.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Lastausgleichsdienst > Globale Konfiguration**.
- 3 Wählen Sie die Optionen, die Sie aktivieren möchten:

Option	Aktion
Status	<p>Aktivieren Sie den Lastausgleichsdienst durch Klicken auf das Symbol zum Umschalten.</p> <p>Aktivieren Sie Beschleunigung aktiviert, um den Lastausgleichsdienst so zu konfigurieren, dass die schnellere L4-Engine anstelle der L7-Engine verwendet wird. L4 TCP VIP wird vor der Edge-Gateway-Firewall verarbeitet, daher ist keine Regel zum Zulassen der Firewall erforderlich.</p> <hr/> <p>Hinweis L7-VIPs für HTTP und HTTPS werden nach der Firewall verarbeitet. Wenn Sie die Beschleunigung also nicht aktivieren, muss eine Firewallregel für das Edge-Gateway vorhanden sein, um Zugriff auf L7-VIP für diese Protokolle zuzulassen. Wenn Sie die Beschleunigung aktiviert haben und der Serverpool sich im nicht transparenten Modus befindet, wird eine SNAT-Regel hinzugefügt. Daher müssen Sie sicherstellen, dass die Firewall für das Edge-Gateway aktiviert ist.</p> <hr/>
Protokollierung aktivieren	Aktivieren Sie die Protokollierung, damit der Lastausgleichsdienst des Edge-Gateways Datenverkehrsprotokolle erfasst.
Protokollierungsebene	Wählen Sie den Schweregrad der Ereignisse aus, die in den Protokollen erfasst werden sollen.

- 4 Klicken Sie auf **Änderungen speichern**.
Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

Konfigurieren Sie Anwendungsprofile für den Lastausgleichsdienst. Weitere Informationen finden Sie unter [Erstellen eines Anwendungsprofils](#).


Erstellen eines Anwendungsprofils

Ein Anwendungsprofil definiert das Verhalten des Lastausgleichsdiensts für einen bestimmten Typ des Netzwerkdatenverkehrs. Nach der Profilkonfiguration können Sie es einem virtuellen Server zuordnen. Der virtuelle Server verarbeitet dann den Datenverkehr gemäß den im Profil angegebenen Werten. Durch die Verwendung von Profilen wird Ihre Kontrolle über die Verwaltung des Netzwerkdatenverkehrs verbessert, und die Aufgaben für die Verwaltung des Datenverkehrs werden einfacher und effizienter.

Wenn Sie ein Profil für HTTPS-Datenverkehr erstellen, sind die folgenden HTTPS-Datenverkehrsmuster zulässig:

- Client -> HTTPS -> LB (SSL beenden) -> HTTP -> Server
- Client -> HTTPS -> LB (SSL beenden) -> HTTPS -> Server
- Client -> HTTPS -> LB (SSL-Passthrough) -> HTTPS -> Server
- Client -> HTTP -> LB -> HTTP -> Server

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Lastausgleichsdienst > Anwendungsprofile**.
- 3 Klicken Sie auf die Schaltfläche **Erstellen** ().
- 4 Geben Sie einen Namen für das Profil ein.
- 5 Konfigurieren Sie das Anwendungsprofil.

Option	Beschreibung
Typ	Wählen Sie den Protokolltyp aus, der zum Senden von Anforderungen an den Server verwendet wird. Die Liste der erforderlichen Parameter hängt vom ausgewählten Protokoll ab. Parameter, die nicht für das von Ihnen ausgewählte Protokoll gelten, können nicht eingegeben werden. Alle anderen Parameter sind erforderlich.
SSL-Passthrough aktivieren	Klicken Sie, um die Weitergabe der SSL-Authentifizierung an den virtuellen Server zu aktivieren. Andernfalls wird die SSL-Authentifizierung an der Zieladresse ausgeführt.
HTTP-Umleitungs-URL	(HTTP und HTTPS) Geben Sie die URL ein, an die der Datenverkehr, der an der Zieladresse ankommt, umgeleitet werden soll.

Option	Beschreibung
Persistenz	<p>Geben Sie einen Persistenzmechanismus für das Profil an.</p> <p>Persistenz verfolgt und speichert Sitzungsdaten, wie z. B. das spezifische Poolmitglied, das eine Clientanforderung bearbeitet hat. Dadurch wird sichergestellt, dass die Clientanforderungen während des Lebenszyklus einer Sitzung oder während nachfolgender Sitzungen demselben Poolmitglied zugeordnet werden. Zu den Optionen gehören:</p> <ul style="list-style-type: none"> ■ Quell-IP <p>Quell-IP-Persistenz verfolgt Sitzungen basierend auf der IP-Quelladresse. Wenn ein Client eine Verbindung zu einem virtuellen Server anfordert, der die Persistenz der Quelladressen-Affinität unterstützt, überprüft der Lastausgleichsdienst, ob dieser Client zuvor eine Verbindung hergestellt hat, und wenn ja, gibt er den Client an dasselbe Poolmitglied zurück.</p> ■ MSRDP <p>(Nur TCP) MSRDP-Persistenz (Microsoft Remote Desktop Protocol) behält persistente Sitzungen zwischen Windows-Clients und -Servern bei, die den RDP-Dienst (Remote Desktop Protocol) von Microsoft ausführen. Das empfohlene Szenario für die Aktivierung der MSRDP-Persistenz ist die Erstellung eines Lastausgleichspools, der aus Mitgliedern besteht, die ein Windows Server-Gastbetriebssystem ausführen, wobei alle Mitglieder zu einem Windows-Cluster gehören und an einem Windows-Sitzungsverzeichnis teilnehmen.</p> ■ SSL-Sitzungs-ID <p>Persistenz der SSL-Sitzungs-ID ist verfügbar, wenn Sie SSL-Passthrough aktivieren. Persistenz der SSL-Sitzungs-ID stellt sicher, dass wiederholte Verbindungen vom selben Client an denselben Server gesendet werden. Persistenz der SSL-Sitzungs-ID ermöglicht die Wiederaufnahme der SSL-Sitzung, wodurch die Verarbeitungszeit sowohl für den Client als auch für den Server gespeichert wird.</p>
Cookiename	<p>(HTTP und HTTPS) Wenn Sie Cookie als Mechanismus für die Persistenz angegeben haben, geben Sie den Cookienamen ein. Die Cookiepersistenz verwendet ein Cookie, um die Sitzung eindeutig zu identifizieren, wenn ein Client zum ersten Mal auf die Site zugreift. Der Lastausgleichsdienst verweist auf dieses Cookie, wenn die Verbindung nachfolgender Anforderungen in der Sitzung hergestellt wird, sodass sie alle an den gleichen virtuellen Server weitergeleitet werden.</p>

Option	Beschreibung
Modus	<p>Wählen Sie den Modus aus, mit dem das Cookie eingefügt werden soll. Die folgenden Modi werden unterstützt:</p> <ul style="list-style-type: none"> ■ Einfügen <p>Das Edge-Gateway sendet ein Cookie. Wenn der Server ein oder mehrere Cookies sendet, empfängt der Client ein zusätzliches Cookie (Server-Cookies und Edge-Gateway-Cookie). Wenn der Server keine Cookies sendet, empfängt der Client nur das Edge-Gateway-Cookie.</p> ■ Präfix <p>Wählen Sie diese Option aus, wenn Ihr Client nur ein Cookie unterstützt.</p> <p>Hinweis Alle Browser akzeptieren mehrere Cookies. Möglicherweise verfügen Sie jedoch über eine proprietäre Anwendung mit einem proprietären Client, der nur ein Cookie unterstützt. Der Webserver sendet wie üblich sein Cookie. Das Edge-Gateway fügt seine Cookieinformationen in den Server-Cookiewert ein (als Präfix). Diese hinzugefügten Cookieinformationen werden entfernt, wenn das Edge-Gateway sie an den Server sendet.</p> ■ App-Sitzung Für diese Option sendet der Server kein Cookie. Stattdessen sendet er die Informationen zur Benutzersitzung als URL. Beispiel: <code>http://example.com/admin/UpdateUserServlet;jsessionid=0I24B9ASD7BSSD</code>, wobei <code>jsessionid</code> die Benutzersitzungsinformationen bezeichnet und für die Persistenz verwendet wird. Es ist nicht möglich, die Persistenztabelle der App-Sitzung zur Fehlerbehebung anzuzeigen.
Läuft ab in (Sekunden)	<p>Geben Sie eine Zeitdauer in Sekunden ein, für die die Persistenz wirksam bleibt. Dies muss eine positive Ganzzahl im Bereich von 1-86400 sein.</p> <p>Hinweis Beim L7-Lastausgleich mit TCP-Quell-IP-Persistenz kommt es zu einer Zeitüberschreitung des Persistenzeintrags, wenn in einem bestimmten Zeitraum keine neuen TCP-Verbindungen hergestellt werden, selbst wenn die bestehenden Verbindungen noch aktiv sind.</p>
HTTP-Header 'X-Forwarded-For' einfügen	(HTTP und HTTPS) Wählen Sie HTTP-Header 'X-Forwarded-For' einfügen für das Identifizieren der Ursprungs-IP-Adresse eines Clients aus, der eine Verbindung zu einem Webserver über den Lastausgleichsdienst herstellt.
Pool-seitiges SSL aktivieren	(Nur HTTPS) Wählen Sie Pool-seitiges SSL aktivieren aus, um das Zertifikat, die Zertifizierungsstellen oder die CRLs zu definieren, die zur Authentifizierung des Lastausgleichsdiensts über die Serverseite auf der Registerkarte „Pool-Zertifikate“ verwendet werden.

- 6 (Nur HTTPS) Konfigurieren Sie die Zertifikate, die mit dem Anwendungsprofil verwendet werden. Wenn die benötigten Zertifikate nicht vorhanden sind, können Sie diese über die Registerkarte **Zertifikate** erstellen.

Option	Beschreibung
Zertifikate für den virtuellen Server	Wählen Sie das Zertifikat, die Zertifizierungsstellen oder CRLs aus, die zum Entschlüsseln des HTTPS-Datenverkehrs verwendet werden.
Pool-Zertifikate	Definieren Sie das Zertifikat, die Zertifizierungsstellen oder CRLs, die zur Authentifizierung des Lastausgleichsdiensts über die Serverseite verwendet werden. Hinweis Wählen Sie Pool-seitiges SSL aktivieren aus, um diese Registerkarte zu aktivieren.
Schlüssel	Wählen Sie die Schlüsselalgorithmen (oder Verschlüsselungs-Suite) aus, die während des SSL/TLS-Handshakes ausgehandelt wurden.
Clientauthentifizierung	Geben Sie an, ob die Clientauthentifizierung ignoriert werden soll oder erforderlich ist. Hinweis Wenn Erforderlich festgelegt ist, muss der Client nach der Anforderung ein Zertifikat bereitstellen, oder der Handshake wird abgebrochen.

- 7 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.


Nächste Schritte

Fügen Sie eine Dienstüberwachung für den Lastausgleichsdienst hinzu, um Systemdiagnosen für verschiedene Arten von Netzwerkdatenverkehr zu definieren. Weitere Informationen finden Sie unter [Erstellen einer Dienstüberwachung](#).

Erstellen einer Dienstüberwachung

Sie können eine Dienstüberwachung erstellen, um Systemdiagnoseparameter für einen bestimmten Typ des Netzwerkdatenverkehrs zu definieren. Wenn Sie eine Dienstüberwachung einem Pool zuweisen, werden die Poolmitglieder gemäß den Dienstüberwachungsparametern überwacht.

Verfahren

- Öffnen Sie „Edge-Gateway-Dienste“.
 - Navigieren Sie zu **Netzwerk > Edges**.
 - Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- Navigieren Sie zu **Lastausgleichsdienst > Dienstüberwachung**.
- Klicken Sie auf die Schaltfläche **Erstellen** ().

- 4 Geben Sie einen Namen für die Dienstüberwachung ein.
- 5 (Optional) Konfigurieren Sie die folgenden Optionen für die Dienstüberwachung:

Option	Beschreibung
Intervall	Geben Sie das Intervall ein, in dem ein Server unter Verwendung der angegebenen Methode zu überwachen ist.
Zeitüberschreitung	Geben Sie die maximale Zeit in Sekunden ein, in der eine Antwort vom Server empfangen werden muss.
Max. Wiederholungen	Geben Sie an, wie oft die angegebene Methode für die Überwachung hintereinander fehlschlagen muss, bevor der Server als ausgefallen erklärt wird.
Typ	Wählen Sie aus, wie die Systemdiagnoseanforderung an den Server gesendet werden soll: HTTP, HTTPS, TCP, ICMP oder UDP. Je nach ausgewähltem Typ werden die übrigen Optionen im Dialogfeld Neue Dienstüberwachung aktiviert oder deaktiviert.
Erwartet	(HTTP und HTTPS) Geben Sie die Zeichenfolge, deren Übereinstimmung die Überwachung erwartet, in die Statuszeile der HTTP- oder HTTPS-Antwort ein (z. B. HTTP/1.1).
Methode	(HTTP und HTTPS) Wählen Sie die Methode aus, die zum Erkennen des Serverstatus zu verwenden ist.
URL	(HTTP und HTTPS) Geben Sie die URL ein, die in der Serverstatusanforderung zu verwenden ist. Hinweis Wenn Sie die POST-Methode auswählen, müssen Sie einen Wert für Senden angeben.
Senden	(HTTP, HTTPS und UDP) Geben Sie die zu sendenden Daten ein.
Empfangen	(HTTP, HTTPS und UDP) Geben Sie die Zeichenfolge ein, die im Antwortinhalt abgeglichen werden soll. Hinweis Wenn Erwartet nicht übereinstimmt, versucht die Überwachung nicht, den Inhalt von Empfangen abzugleichen.
Erweiterung	(ALLE) Geben Sie erweiterte Überwachungsparameter als Schlüssel=Wert-Paare ein. Beispielsweise bedeutet „warning=10“, dass der Status eines Servers als Warnung festgelegt wird, wenn er nicht innerhalb von 10 Sekunden antwortet. Alle Erweiterungselemente müssen mit einem Wagenrücklaufzeichen getrennt werden. Beispiel: <pre><extension>delay=2 critical=3 escape</extension></pre>

- 6 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Beispiel: Erweiterungen unterstützt für jedes Protokoll

Tabelle 6-1. Erweiterungen für HTTP/HTTPS-Protokolle

Überwachungserweiterung	Beschreibung
no-body	Wartet nicht auf ein Dokumenthauptteil und beendet Lesevorgang nach dem HTTP/HTTPS-Header. Hinweis HTTP GET oder HTTP POST wird weiterhin gesendet, und keine HEAD-Methode.
max-age= <i>SECONDS</i>	Warnt, wenn ein Dokument älter als SEKUNDEN ist. Die Anzahl kann in der Form „10m“ für Minuten, „10h“ für Stunden oder „10d“ für Tage angegeben werden.
content-type= <i>STRING</i>	Gibt einen Header-Medientyp „Content-Type“ in POST-Aufrufen an.
linespan	Lässt zu, dass regex Zeilenvorschübe überbrückt (muss vor „-r“ oder „-R“ stehen).
regex= <i>STRING</i> oder ereg= <i>STRING</i>	Durchsucht die Seite nach regex-ZEICHENFOLGE.
eregi= <i>STRING</i>	Durchsucht die Seite nach regex-ZEICHENFOLGE, bei der nicht zwischen Groß- und Kleinschreibung unterschieden wird.
invert-regex	Gibt CRITICAL zurück, wenn gefunden, und OK, wenn nicht gefunden.
proxy-authorization= <i>AUTH_PAIR</i>	Gibt Benutzernamen:Kennwort auf Proxyservern mit Standardauthentifizierung an.
useragent= <i>STRING</i>	Sendet die Zeichenfolge im HTTP-Header als User Agent.
header= <i>STRING</i>	Sendet alle anderen Tags in den HTTP-Header. Mehrmalige Verwendung für zusätzliche Header.
onredirect=ok warning critical follow sticky stickyport	Gibt an, wie umgeleitete Seiten verarbeitet werden. <i>sticky</i> ist wie <i>follow</i> , aber ist an die angegebene IP-Adresse gebunden. <i>stickyport</i> stellt sicher, dass sich der Port nicht ändert.
pagesize= <i>INTEGER:INTEGER</i>	Gibt die erforderlichen minimalen und maximalen Seitengrößen in Bytes an.
warning=DOUBLE	Gibt die Antwortzeit in Sekunden an, nach der ein Warnstatus gemeldet wird.
critical=DOUBLE	Gibt die Antwortzeit in Sekunden an, nach der ein kritischer Status gemeldet wird.

Tabelle 6-2. Erweiterungen nur für HTTPS-Protokoll

Überwachungserweiterung	Beschreibung
sni	Aktiviert die Unterstützung für die SSL/TLS-Hostnamenerweiterung (SNI).
certificate= INTEGER	Gibt an, wie viele Tage ein Zertifikat mindestens gültig sein muss. Der Port ist standardmäßig auf 443 gesetzt. Wenn diese Option verwendet wird, wird die URL nicht überprüft.
authorization=AUTH_PAIR	Gibt Benutzernamen:Kennwort auf Sites mit Standardauthentifizierung an.

Tabelle 6-3. Erweiterungen für TCP-Protokoll

Überwachungserweiterung	Beschreibung
escape	Ermöglicht die Verwendung von \n, \r, \t oder \ in einer send- oder quit-Zeichenfolge. Muss einer send- oder quit-Option vorangestellt werden. Standardmäßig wird nichts an „send“ angefügt, und \r\n wird ans Ende von „quit“ angefügt.
alle	Gibt an, dass alle erwarteten Zeichenfolgen in einer Serverantwort auftreten müssen. Standardmäßig wird <i>any</i> verwendet.
quit= <i>STRING</i>	Sendet eine Zeichenfolge an den Server, um die Verbindung ordnungsgemäß zu schließen.
refuse=ok warn crit	Akzeptiert TCP-Zurückweisungen mit dem Status <i>ok</i> , <i>warn</i> oder <i>crit</i> . Verwendet standardmäßig den Status <i>crit</i> .
mismatch=ok warn crit	Akzeptiert erwartete Zeichenfolgenkonflikte mit dem Status <i>ok</i> , <i>warn</i> oder <i>crit</i> . Verwendet standardmäßig den Status <i>warn</i> .
jail	Blendet die Ausgabe im TCP-Socket aus.
maxbytes= <i>INTEGER</i>	Schließt die Verbindung, wenn mehr als die angegebene Anzahl an Byte empfangen werden.
delay= <i>INTEGER</i>	Wartet die angegebene Anzahl von Sekunden zwischen dem Senden der Zeichenfolge und dem Abrufen einer Antwort.
certificate= <i>INTEGER</i> [, <i>INTEGER</i>]	Gibt an, wie viele Tage ein Zertifikat mindestens gültig sein muss. Der erste Wert ist #days für „warning“, und der zweite Wert ist „critical“ (wenn nicht angegeben, -0).
ssl	Verwendet SSL für die Verbindung.
warning= <i>DOUBLE</i>	Gibt die Antwortzeit in Sekunden an, nach der ein Warnstatus gemeldet wird.
critical= <i>DOUBLE</i>	Gibt die Antwortzeit in Sekunden an, nach der ein kritischer Status gemeldet wird.


Nächste Schritte

Fügen Sie Serverpools für Ihren Lastausgleichsdienst hinzu. Weitere Informationen finden Sie unter [Hinzufügen eines Serverpools für den Lastausgleich](#).

Hinzufügen eines Serverpools für den Lastausgleich

Sie können einen Serverpool hinzufügen, um Back-End-Server flexibel und effizient zu verwalten und freizugeben. Ein Pool dient zur Verwaltung von Lastausgleichs-Verteilungsmethoden und ist mit einer Dienstüberwachung für Integritätsprüfungsparameter verbunden.


Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Lastausgleichsdienst > Pools**.
- 3 Klicken Sie auf die Schaltfläche **Erstellen** ().
- 4 Geben Sie einen Namen und optional eine Beschreibung für den Lastausgleichspool ein.
- 5 Wählen Sie im Dropdown-Menü **Algorithmus** eine Ausgleichsmethode für den Dienst aus:

Option	Beschreibung
ROUND_ROBIN	Alle Server werden der Reihe nach entsprechend der zugewiesenen Gewichtung verwendet. Dies ist der ausgewogenste und reibungsloseste Algorithmus, wenn die Verarbeitungszeit des Servers gleichmäßig verteilt bleibt.
IP_HASH	Wählt einen Server auf Grundlage eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets aus.
LEASTCONN	Verteilt Clientanforderungen entsprechend der Anzahl der bereits geöffneten Serververbindungen auf mehrere Server. Neue Verbindungen werden an den Server mit den wenigsten geöffneten Verbindungen gesendet.
URI	Der linke Teil des URI (vor dem Fragezeichen) wird gehasht und durch die Gesamtgewichtung der ausgeführten Server geteilt. Das Ergebnis bestimmt, welcher Server die Anforderung erhält. Durch diese Option wird sichergestellt, dass ein URI immer an denselben Server weitergeleitet wird, solange der Server nicht heruntergefahren wird.

Option	Beschreibung
HTTPHEADER	Der Name des HTTP-Headers wird bei jeder HTTP-Anforderung gesucht. Beim in Klammern angegebenen Header-Namen wird – ähnlich wie bei der ACL-Funktion „hdr()“ – nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn der Header nicht vorhanden ist oder keinen Wert enthält, wird der Round-Robin-Algorithmus angewendet. Der HTTP HEADER-Algorithmusparameter verfügt über eine Option <code>headerName=<name></code> . Sie können z. B. host als HTTP HEADER-Algorithmusparameter verwenden.
URL	Der im Argument angegebene URL-Parameter wird in der Abfragezeichenfolge jeder HTTP GET-Anforderung gesucht. Wenn hinter dem Parameter ein Gleichheitszeichen (=) und ein Wert stehen, wird der Wert gehasht und durch die Gesamtgewichtung der ausgeführten Server geteilt. Das Ergebnis bestimmt, welcher Server die Anforderung erhält. Dieses Verfahren wird verwendet, um Benutzerbezeichner in Anforderungen zu verfolgen und sicherzustellen, dass immer dieselbe Benutzer-ID an denselben Server gesendet wird, solange kein Server hoch- oder heruntergefahren wird. Wenn kein Wert oder Parameter gefunden wird, wird ein Round-Robin-Algorithmus angewendet. Der URL-Algorithmusparameter verfügt über eine Option <code>urlParam=<url></code> .

6 Fügen Sie dem Pool Mitglieder hinzu.

- a Klicken Sie auf die Schaltfläche **Hinzufügen** ().
- b Geben Sie den Namen für das Poolmitglied ein.
- c Geben Sie die IP-Adresse des Poolmitglieds ein.
- d Geben Sie den Port ein, an dem das Mitglied den Datenverkehr vom Lastausgleichsdienst empfangen soll.
- e Geben Sie den Überwachungsport ein, an dem das Mitglied Integritätsüberwachungsanforderungen erhalten soll.
- f Geben Sie im Textfeld **Gewichtung** den Anteil des Datenverkehrs ein, der von diesem Mitglied verarbeitet werden soll. Hierbei muss es sich um eine Ganzzahl im Bereich von 1–256 handeln.
- g (Optional) Geben Sie im Textfeld **Höchstanzahl an Verbindungen** die maximale Anzahl gleichzeitiger Verbindungen ein, die das Mitglied verarbeiten kann.

Wenn die Anzahl der eingehenden Anforderungen den Maximalwert übersteigt, werden Anforderungen in die Warteschlange gestellt, und der Lastausgleichsdienst wartet, bis eine Verbindung freigegeben wird.
- h (Optional) Geben Sie im Textfeld **Mindestanzahl an Verbindungen** die minimale Anzahl gleichzeitiger Verbindungen ein, die ein Mitglied immer akzeptieren muss.
- i Klicken Sie auf **Behalten**, um dem Pool das neue Mitglied hinzuzufügen.

Der Vorgang kann eine Minute dauern.

- 7 (Optional) Wählen Sie **Transparent** aus, damit die Client-IP-Adressen für die Back-End-Server sichtbar sind.

Wenn **Transparent** (Standardeinstellung) nicht ausgewählt ist, wird die IP-Adresse der Quelle des Datenverkehrs den Back-End-Servern als interne IP-Adresse des Lastausgleichsdiensts angezeigt.

Ist **Transparent** ausgewählt, so ist die Quell-IP-Adresse die tatsächliche IP-Adresse des Clients. Das Edge-Gateway muss dann als Standard-Gateway festgelegt werden, um sicherzustellen, dass Rückpakete über das Edge-Gateway geleitet werden.

- 8 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Nächste Schritte

Fügen Sie virtuelle Server für den Lastausgleichsdienst hinzu. Ein virtueller Server hat eine öffentliche IP-Adresse und bedient alle eingehenden Clientanforderungen. Weitere Informationen finden Sie unter [Hinzufügen eines virtuellen Servers](#).

Hinzufügen einer Anwendungsregel

Sie können eine Anwendungsregel schreiben, mit der der IP-Anwendungsdatenverkehr direkt gesteuert und verwaltet werden kann.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Lastausgleichsdienst > Anwendungsregeln**.

- 3 Klicken Sie auf die Schaltfläche **Hinzufügen** ().

- 4 Geben Sie den Namen für die Anwendungsregel ein.

- 5 Geben Sie das Skript für die Anwendungsregel ein.

Informationen über die Syntax der Anwendungsregel finden Sie unter <http://cbonte.github.io/haproxy-dconv/configuration-1.5.html>.

- 6 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Nächste Schritte


Ordnen Sie die neue Anwendungsregel einem virtuellen Server für den Lastausgleichsdienst hinzu. Weitere Informationen finden Sie unter [Hinzufügen eines virtuellen Servers](#).

Hinzufügen eines virtuellen Servers

Fügen Sie eine interne Edge-Gateway-Schnittstelle oder eine Edge-Gateway-Uplink-Schnittstelle als virtuellen Server hinzu. Ein virtueller Server hat eine öffentliche IP-Adresse und bedient alle eingehenden Clientanforderungen.

Der Lastausgleichsdienst schließt die TCP-Verbindung des Servers standardmäßig nach jeder Clientanforderung.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **Lastausgleichsdienst > Virtuelle Server**.
- 3 Klicken Sie auf die Schaltfläche **Hinzufügen** ().
- 4 Konfigurieren Sie auf der Registerkarte **Allgemein** die folgenden Optionen für den virtuellen Server:

Option	Beschreibung
Virtuellen Server aktivieren	Klicken Sie auf diese Option, um den virtuellen Server zu aktivieren.
Beschleunigung aktivieren	Klicken Sie auf diese Option, um die Beschleunigung zu aktivieren.
Anwendungsprofil	Wählen Sie ein Anwendungsprofil aus, das dem virtuellen Server zugeordnet werden soll.
Name	Geben Sie einen Namen für den virtuellen Server ein.
Beschreibung	Geben Sie eine optionale Beschreibung für den virtuellen Server ein.
IP-Adresse	Geben Sie die vom Lastausgleichsdienst überwachte IP-Adresse ein oder suchen Sie nach der Adresse.
Protokoll	Wählen Sie das vom virtuellen Server akzeptierte Protokoll aus. Sie müssen dasselbe Protokoll auswählen, das vom ausgewählten Anwendungsprofil verwendet wird.
Port	Geben Sie die vom Lastausgleichsdienst überwachte Portnummer ein.
Standardpool	Wählen Sie den Serverpool aus, der vom Lastausgleichsdienst verwendet wird.
Verbindungsgrenzwert	(Optional) Geben Sie die maximale Anzahl an gleichzeitigen Verbindungen ein, die der virtuelle Server verarbeiten kann.
Grenzwert für Verbindungsrate (CPS)	(Optional) Geben Sie die maximale Anzahl an eingehenden neuen Verbindungsanforderungen pro Sekunde ein.

- 5 (Optional) Wenn Sie dem virtuellen Server Anwendungsregeln zuordnen möchten, klicken Sie auf die Registerkarte **Erweitert** und führen Sie folgende Schritte aus:

- a Klicken Sie auf die Schaltfläche **Hinzufügen** ()

Die für den Lastausgleichsdienst erstellten Anwendungsregeln werden angezeigt. Fügen Sie ggf. Anwendungsregeln für den Lastausgleichsdienst hinzu. Weitere Informationen finden Sie unter [Hinzufügen einer Anwendungsregel](#).

- 6 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Nächste Schritte

Erstellen Sie eine Edge-Gateway-Firewallregel, um Datenverkehr zum neuen virtuellen Server (Ziel-IP-Adresse) zuzulassen. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#)

Sicherer Zugriff mit virtuellen privaten Netzwerken

Sie können die VPN-Funktionen konfigurieren, die von der NSX-Software für Ihre Edge-Gateways bereitgestellt werden. Sie können VPN-Verbindungen zu Ihrem Organisations-VDC über einen SSL VPN-Plus-Tunnel, einen IPsec-VPN-Tunnel oder einen L2 VPN-Tunnel konfigurieren.

Wie im *NSX Administratorhandbuch* beschrieben, unterstützt das NSX Edge-Gateway die folgenden VPN-Dienste:

- SSL VPN-Plus, mit dem Remotebenutzer auf private Unternehmensanwendungen zugreifen können.
- IPsec-VPN, das Site-to-Site-Konnektivität zwischen einem NSX Edge-Gateway und Remote-Sites bietet, die auch über NSX oder Hardwarerouter von Drittanbietern oder VPN-Gateways verfügen.
- L2 VPN, das eine Erweiterung Ihres Organisations-VDC zulässt, indem die virtuellen Maschinen Netzwerkkonnektivität unter Verwendung derselben IP-Adresse über geografische Grenzen hinweg beibehalten können.

In einer vCloud Director-Umgebung können Sie die folgenden VPN-Tunnel erstellen:

- Zwischen VDC-Organisationsnetzwerken in derselben Organisation
- Zwischen VDC-Organisationsnetzwerken in verschiedenen Organisationen
- Zwischen einem VDC-Organisationsnetzwerk und einem externen Netzwerk

Hinweis vCloud Director unterstützt nicht mehrere VPN-Tunnel zwischen den gleichen zwei Edge-Gateways. Wenn ein Tunnel zwischen zwei Edge-Gateways besteht und Sie dem Tunnel ein weiteres Subnetz hinzufügen möchten, löschen Sie den VPN-Tunnel und erstellen Sie einen neuen Tunnel, in dem das neue Subnetz enthalten ist.

Nachdem Sie die VPN-Tunnel für ein Edge-Gateway konfiguriert haben, können Sie einen VPN-Client aus einem Remotespeicherort verwenden, um eine Verbindung zu dem Organisations-VDC herzustellen, das von diesem Edge-Gateway unterstützt wird.

Konfigurieren von SSL VPN-Plus

Die SSL VPN-Plus-Dienste für ein Edge-Gateway in einer vCloud Director-Umgebung ermöglichen Remotebenutzern die sichere Verbindung mit den privaten Netzwerken und Anwendungen in den Organisations-VDCs, die von diesem Edge-Gateway unterstützt werden. Sie können verschiedene SSL VPN-Plus-Dienste auf dem Edge-Gateway konfigurieren.

In Ihrer vCloud Director-Umgebung unterstützt die SSL VPN-Plus-Funktion des Edge-Gateways den Netzwerkzugriffsmodus. Remote-Benutzer müssen einen SSL-Client installieren, um sichere Verbindungen und Zugriff auf die Netzwerke und Anwendungen hinter dem Edge-Gateway herzustellen. Im Rahmen der SSL VPN-Plus-Konfiguration des Edge-Gateways fügen Sie die Installationspakete für das Betriebssystem hinzu und konfigurieren bestimmte Parameter. Weitere Informationen finden Sie unter [Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients](#).

Das Konfigurieren von SSL VPN-Plus auf einem Edge-Gateway ist ein mehrstufiger Prozess.

Voraussetzungen

Vergewissern Sie sich, dass alle für SSL VPN-Plus erforderlichen SSL-Zertifikate zum Bildschirm **Zertifikate** hinzugefügt wurden. Weitere Informationen finden Sie unter [SSL-Zertifikatsverwaltung](#).

Hinweis Auf einem Edge-Gateway ist Port 443 der Standardport für HTTPS. Für die SSL VPN-Funktionalität muss der HTTPS-Port des Edge-Gateways für externe Netzwerke zugänglich sein. Der SSL VPN-Client benötigt die IP-Adresse und den Port des Edge-Gateways, die im Bildschirm „Servereinstellungen“ auf der Registerkarte **SSL VPN-Plus** konfiguriert werden, um über das Clientsystem erreichbar zu sein. Weitere Informationen finden Sie unter [Konfigurieren der SSL-VPN-Servereinstellungen](#).

Verfahren

1 Navigieren zum Bildschirm „SSL-VPN Plus“

Sie können zum Bildschirm „SSL-VPN Plus“ navigieren, um mit der Konfiguration des SSL-VPN Plus-Diensts für ein Edge-Gateway zu beginnen.

2 Konfigurieren der SSL-VPN-Servereinstellungen

Mit diesen Servereinstellungen wird der SSL VPN-Server konfiguriert, wie z. B. die IP-Adresse und der Port, der vom Dienst überwacht wird, die Schlüsselliste des Diensts und das Dienstzertifikat. Beim Herstellen einer Verbindung mit dem Edge-Gateway geben die Remotebenutzer dieselbe IP-Adresse und den Port an, die/den Sie in diesen Servereinstellungen festlegen.

3 Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Den Remotebenutzern werden virtuelle IP-Adressen aus den statischen IP-Pools zugewiesen, die Sie über den Bildschirm **IP-Pools** auf der Registerkarte **SSL VPN-Plus** konfigurieren.

4 Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm „Private Netzwerke“ auf der Registerkarte **SSL VPN-Plus**, um die privaten Netzwerke zu konfigurieren. Die privaten Netzwerke sind diejenigen, auf die die VPN-Clients Zugriff haben sollen, wenn die Remotebenutzer eine Verbindung über ihre VPN-Clients und den SSL-VPN-Tunnel herstellen. Die aktivierten privaten Netzwerke werden in der Routing-Tabelle des VPN-Clients installiert.

5 Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm **Authentifizierung** auf der Registerkarte **SSL VPN-Plus**, um einen lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways einzurichten und optional die Authentifizierung von Clientzertifikaten zu aktivieren. Dieser Authentifizierungsserver wird zur Authentifizierung der Benutzer, die eine Verbindung herstellen, verwendet. Alle Benutzer, die im lokalen Authentifizierungsserver konfiguriert sind, werden authentifiziert.

6 Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver

Verwenden Sie den Bildschirm **Benutzer** auf der Registerkarte **SSL VPN-Plus**, um dem lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways Konten für Remotebenutzer hinzuzufügen.

7 Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients

Verwenden Sie den Bildschirm „Installationspakete“ auf der Registerkarte **SSL VPN-Plus**, um benannte Installationspakete des SSL VPN-Plus-Clients für die Remotebenutzer zu erstellen.

8 Bearbeiten der SSL VPN-Plus-Client-Konfiguration

Verwenden Sie den Bildschirm **Client-Konfiguration** auf der Registerkarte **SSL VPN-Plus**, um die Reaktion des SSL VPN-Client-Tunnels anzupassen, wenn sich der Remotebenutzer bei SSL VPN anmeldet.

9 Anpassen der allgemeinen SSL VPN-Plus-Einstellungen für ein Edge-Gateway

Das System legt standardmäßig einige SSL VPN-Plus-Einstellungen für ein Edge-Gateway in Ihrer vCloud Director-Umgebung fest. Auf dem Bildschirm **Allgemeine Einstellungen** auf der Registerkarte **SSL VPN-Plus** im vCloud Director-Mandantenportal können Sie diese Einstellungen anpassen.

Navigieren zum Bildschirm „SSL-VPN Plus“

Sie können zum Bildschirm „SSL-VPN Plus“ navigieren, um mit der Konfiguration des SSL-VPN Plus-Diensts für ein Edge-Gateway zu beginnen.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **SSL VPN-Plus**.

Nächste Schritte

Konfigurieren Sie die SSL VPN-Plus-StandardEinstellungen im Bildschirm **Allgemein**. Weitere Informationen finden Sie unter [Anpassen der allgemeinen SSL VPN-Plus-Einstellungen für ein Edge-Gateway](#).

Konfigurieren der SSL-VPN-Servereinstellungen

Mit diesen Servereinstellungen wird der SSL VPN-Server konfiguriert, wie z. B. die IP-Adresse und der Port, der vom Dienst überwacht wird, die Schlüsselliste des Diensts und das Dienstzertifikat. Beim Herstellen einer Verbindung mit dem Edge-Gateway geben die Remotebenutzer dieselbe IP-Adresse und den Port an, die/den Sie in diesen Servereinstellungen festlegen.

Wenn Ihr Edge-Gateway mit mehreren Overlay-IP-Adressnetzwerken für die externe Schnittstelle konfiguriert ist, kann sich die IP-Adresse, die Sie für den SSL VPN-Server auswählen, von der für die standardmäßige externe Schnittstelle des Edge-Gateways unterscheiden.

Beim Konfigurieren der SSL-VPN-Servereinstellungen müssen Sie den Verschlüsselungsalgorithmus auswählen, der für den SSL-VPN-Tunnel verwendet werden soll. Sie können eine oder mehrere Verschlüsselungen auswählen. Gehen Sie bei der Auswahl der Verschlüsselungen sorgfältig vor und berücksichtigen Sie die Vor- und Nachteile der verschiedenen Verschlüsselungen.

Standardmäßig verwendet das System das selbstsignierte Standardzertifikat, das das System für jedes Edge-Gateway als Standard-Serveridentitätszertifikat für den SSL-VPN-Tunnel generiert. Statt dieses Standardzertifikats können Sie auch ein digitales Zertifikat verwenden, das Sie dem System im Bildschirm **Zertifikate** hinzugefügt haben.

Voraussetzungen

- Vergewissern Sie sich, dass die unter [Konfigurieren von SSL VPN-Plus](#) beschriebenen Voraussetzungen erfüllt sind.
- Wenn Sie ein anderes Dienstzertifikat als das Standardzertifikat verwenden möchten, importieren Sie das erforderliche Zertifikat in das System. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).
- Navigieren zum Bildschirm „SSL-VPN Plus“.

Verfahren

- 1 Klicken Sie im Bildschirm **SSL VPN-Plus** auf **Servereinstellungen**.

- 2 Klicken Sie auf **Aktiviert**.
- 3 Wählen Sie im Dropdown-Menü eine IP-Adresse aus.
- 4 (Optional) Geben Sie eine TCP-Portnummer ein.

Die TCP-Portnummer wird vom SSL-Clientinstallationspaket verwendet. Standardmäßig verwendet das System Port 443. Dies ist der Standardport für HTTPS/SSL-Datenverkehr. Es ist zwar eine Portnummer erforderlich, Sie können aber einen beliebigen TCP-Port für die Kommunikation festlegen.

Hinweis Der SSL VPN-Client benötigt die an dieser Stelle konfigurierte IP-Adresse und den Port, um über die Clientsysteme der Remotebenutzer erreichbar zu sein. Stellen Sie bei einer Änderung der Standardeinstellung für die Portnummer sicher, dass die Kombination aus IP-Adresse und Port über die Systeme der vorgesehenen Benutzer erreichbar ist.

- 5 Wählen Sie in der Schlüsselliste eine Verschlüsselungsmethode aus.
- 6 Konfigurieren Sie die Syslog-Protokollierungsrichtlinie des Diensts.

Die Protokollierung ist standardmäßig aktiviert. Sie können den Grad der Nachrichten, die protokolliert werden sollen, ändern oder die Protokollierung deaktivieren.
- 7 (Optional) Wenn Sie anstelle des vom System generierten selbstsignierten Standardzertifikats ein Dienstzertifikat verwenden möchten, klicken Sie auf **Server-Zertifikat ändern**, wählen Sie ein Zertifikat aus und klicken Sie auf **OK**.
- 8 Klicken Sie auf **Änderungen speichern**.

Nächste Schritte

Hinweis Die von Ihnen festgelegte Edge-Gateway-IP-Adresse und die TCP-Portnummer müssen für die Remotebenutzer erreichbar sein. Fügen Sie eine Edge-Gateway-Firewallregel hinzu, die Zugriff auf die in diesem Verfahren konfigurierte SSL VPN-Plus-IP-Adresse und den Port gestattet. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Fügen Sie einen IP-Pool hinzu, sodass Remotebenutzern IP-Adressen zugewiesen werden, wenn sie eine Verbindung über SSL VPN-Plus herstellen. Weitere Informationen finden Sie unter [Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway](#).

Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Den Remotebenutzern werden virtuelle IP-Adressen aus den statischen IP-Pools zugewiesen, die Sie über den Bildschirm **IP-Pools** auf der Registerkarte **SSL VPN-Plus** konfigurieren.


Jeder in diesem Bildschirm hinzugefügte IP-Pool führt zu einem IP-Adress-Subnetz, das auf dem Edge-Gateway konfiguriert ist. Die in diesen IP-Pools verwendeten IP-Adressbereiche müssen sich von allen anderen auf dem Edge-Gateway konfigurierten Netzwerken unterscheiden.

Hinweis SSL VPN-Plus weist den Remotebenutzern basierend auf der Reihenfolge, in der die IP-Pools in der Tabelle auf dem Bildschirm angezeigt werden, IP-Adressen aus den IP-Pools zu. Nachdem Sie die IP-Pools zur Tabelle auf dem Bildschirm hinzugefügt haben, können Sie ihre Positionen in der Tabelle mit den Pfeiltasten nach oben und unten anpassen.

Voraussetzungen

- Navigieren zum Bildschirm „SSL-VPN Plus“.
- Konfigurieren der SSL-VPN-Servereinstellungen.

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **IP-Pools**.
- 2 Klicken Sie auf die Schaltfläche **Erstellen** ()
- 3 Konfigurieren Sie die Einstellungen des IP-Pools.

Option	Aktion
IP-Bereich	Geben Sie einen IP-Adressbereich für diesen IP-Pool ein, wie z. B. 127.0.0.1–127.0.0.9 . Diese IP-Adressen werden VPN-Clients zugewiesen, wenn sie sich authentifizieren und eine Verbindung mit dem SSL-VPN-Tunnel herstellen.
Netzmaske	Geben Sie die Netzmaske des IP-Pools ein, wie z. B. 255.255.255.0 .
Gateway	Geben Sie die IP-Adresse ein, die das Edge-Gateway erstellen soll, und weisen Sie sie als Gateway-Adresse für diesen IP-Pool zu. Beim Erstellen des IP-Pools wird ein virtueller Adapter auf der Edge-Gateway-VM erstellt und diese IP-Adresse auf dieser virtuellen Schnittstelle konfiguriert. Diese IP-Adresse kann eine beliebige IP-Adresse innerhalb des Subnetzes sein, die nicht auch im Bereich des Feldes IP-Bereich liegt.
Beschreibung	(Optional) Geben Sie eine Beschreibung für diesen IP-Pool ein.
Status	Wählen Sie aus, ob dieser IP-Pool aktiviert oder deaktiviert werden soll.
Primäres DNS	(Optional) Geben Sie den Namen des primären DNS-Servers ein, der für die Namensauflösung für diese virtuellen IP-Adressen verwendet wird.
Sekundäres DNS	(Optional) Geben Sie den Namen des zu verwendenden sekundären DNS-Servers ein.
DNS-Suffix	(Optional) Geben Sie das DNS-Suffix für die Domäne, in der die Clientsysteme gehostet werden, für eine domänenbasierte Hostnamensauflösung ein.
WINS-Server	(Optional) Geben Sie die Adresse des WINS-Servers entsprechend den Anforderungen Ihrer Organisation ein.

- 4 Klicken Sie auf **Behalten**.

Ergebnisse

Die IP-Pool-Konfiguration wird zur Tabelle auf dem Bildschirm hinzugefügt.

Nächste Schritte

Fügen Sie private Netzwerke hinzu, auf die die Remotebenutzer bei der Verbindungsherstellung mit SSL VPN-Plus zugreifen können. Weitere Informationen finden Sie unter [Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway](#).

Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm „Private Netzwerke“ auf der Registerkarte **SSL VPN-Plus**, um die privaten Netzwerke zu konfigurieren. Die privaten Netzwerke sind diejenigen, auf die die VPN-Clients Zugriff haben sollen, wenn die Remotebenutzer eine Verbindung über ihre VPN-Clients und den SSL-VPN-Tunnel herstellen. Die aktivierten privaten Netzwerke werden in der Routing-Tabelle des VPN-Clients installiert.


Die privaten Netzwerke sind eine Liste aller erreichbaren IP-Netzwerke hinter dem Edge-Gateway, das Datenverkehr für einen VPN-Client verschlüsseln soll, oder das von der Verschlüsselung ausgeschlossen werden soll. Jedes private Netzwerk, das Zugriff über einen SSL-VPN-Tunnel erfordert, muss als separater Eintrag hinzugefügt werden. Unter Verwendung von Techniken zur Routenzusammenfassung können Sie die Anzahl der Einträge einschränken.

- SSL VPN-Plus ermöglicht Remotebenutzern den Zugriff auf private Netzwerke, basierend auf der Reihenfolge von oben nach unten, in der die IP-Pools in der Tabelle auf dem Bildschirm angezeigt werden. Nachdem Sie die privaten Netzwerke zur Tabelle auf dem Bildschirm hinzugefügt haben, können Sie ihre Positionen in der Tabelle mit den Pfeiltasten nach oben und unten anpassen.
- Wenn Sie für ein privates Netzwerk „TCP-Optimierung aktivieren“ auswählen, funktionieren möglicherweise einige Anwendungen wie z. B. FTP im aktiven Modus nicht innerhalb dieses Subnetzes. Zum Hinzufügen eines FTP-Servers im aktiven Modus müssen Sie ein weiteres privates Netzwerk für diesen FTP-Server hinzufügen und die Option „TCP-Optimierung“ für dieses private Netzwerk deaktivieren. Außerdem muss das private Netzwerk für diesen FTP-Server aktiviert sein und in der Tabelle auf dem Bildschirm über dem TCP-optimierten privaten Netzwerk angezeigt werden.

Voraussetzungen

- [Navigieren zum Bildschirm „SSL-VPN Plus“](#).
- [Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Private Netzwerke**.
- 2 Klicken Sie auf die Schaltfläche **Hinzufügen** ()

3 Konfigurieren Sie die Einstellungen des privaten Netzwerks.

Option	Aktion
Netzwerk	Geben Sie die IP-Adresse des privaten Netzwerks im CIDR-Format ein, wie z. B. 192169.1.0/24 .
Beschreibung	(Optional) Geben Sie eine Beschreibung für das Netzwerk ein.
Datenverkehr senden	<p>Geben Sie an, wie der VPN-Client den Datenverkehr des privaten Netzwerks und des Internets senden soll.</p> <ul style="list-style-type: none"> ■ Über Tunnel <p>Der VPN-Client sendet den Datenverkehr des privaten Netzwerks und des Internets über das Edge-Gateway, auf dem SSL VPN-Plus aktiviert ist.</p> ■ Bypass für Tunnel <p>Der VPN-Client umgeht das Edge-Gateway und sendet den Datenverkehr direkt an den privaten Server.</p>
TCP-Optimierung aktivieren	<p>(Optional) Zur bestmöglichen Optimierung der Internetgeschwindigkeit müssen Sie, wenn Sie für das Senden des Datenverkehrs Über Tunnel auswählen, auch die Option TCP-Optimierung aktivieren auswählen.</p> <p>Durch die Auswahl dieser Option wird die Leistung von TCP-Paketen innerhalb des VPN-Tunnels verbessert, nicht jedoch die Leistung des UDP-Datenverkehrs.</p> <p>Bei einem konventionellen SSL-VPN-Tunnel mit Vollzugriff werden TCP/IP-Daten in einem zweiten TCP/IP-Stack zwecks Verschlüsselung über das Internet übertragen. Diese konventionelle Methode kapselt die Daten der Anwendungsschicht in zwei getrennte TCP-Streams. Wenn Paketverluste auftreten, was selbst unter optimalen Internetbedingungen passieren kann, kommt es zu einer Leistungsbeeinträchtigung mit der Bezeichnung „TCP-over-TCP Meltdown“. Bei Vorliegen von „TCP-over-TCP Meltdown“ korrigieren zwei TCP-Instrumente dasselbe einzelne Paket von IP-Daten, was den Netzwerkdurchsatz beeinträchtigt und Verbindungszeitüberschreitungen verursacht. Durch die Auswahl von TCP-Optimierung aktivieren wird verhindert, dass dieses TCP-over-TCP-Problem auftritt.</p> <p>Hinweis Wenn Sie die TCP-Optimierung aktivieren, gilt Folgendes:</p> <ul style="list-style-type: none"> ■ Sie müssen die Portnummern eingeben, für die der Internetdatenverkehr optimiert werden soll. ■ Der SSL VPN-Server öffnet die TCP-Verbindung im Namen des VPN-Clients. Wenn der SSL-VPN-Server die TCP-Verbindung öffnet, wird die erste automatisch generierte Edge-Firewallregel angewendet, mit der alle über das Edge-Gateway geöffneten Verbindungen übergeben werden können. Nicht optimierter Datenverkehr wird durch die regulären Edge-Firewallregeln ausgewertet. Mit der standardmäßig generierten TCP-Regel werden beliebige Verbindungen zugelassen.

Option	Aktion
Ports	<p>Wenn Sie Über Tunnel auswählen, geben Sie einen Bereich von Portnummern ein, die für den Remotebenutzer für den Zugriff auf interne Server geöffnet sein sollen, wie z. B. 20–21 für FTP-Datenverkehr und 80–81 für HTTP-Datenverkehr.</p> <p>Um Benutzern uneingeschränkten Zugriff zu gewähren, lassen Sie das Feld leer.</p>
Status	Aktivieren oder deaktivieren Sie das private Netzwerk.

4 Klicken Sie auf **Behalten**.

5 Klicken Sie auf **Änderungen speichern**, um die Konfiguration im System zu speichern.

Nächste Schritte

Fügen Sie einen Authentifizierungsserver hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem Edge-Gateway](#).

Wichtig Fügen Sie die entsprechenden Firewallregeln hinzu, um den Netzwerkverkehr zu den privaten Netzwerken, die Sie in diesem Bildschirm hinzugefügt haben, zuzulassen. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm **Authentifizierung** auf der Registerkarte **SSL VPN-Plus**, um einen lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways einzurichten und optional die Authentifizierung von Clientzertifikaten zu aktivieren. Dieser Authentifizierungsserver wird zur Authentifizierung der Benutzer, die eine Verbindung herstellen, verwendet. Alle Benutzer, die im lokalen Authentifizierungsserver konfiguriert sind, werden authentifiziert.

Es kann nur ein lokaler SSL-VPN-Plus-Authentifizierungsserver auf dem Edge-Gateway konfiguriert werden. Wenn Sie auf **+ Lokal** klicken und weitere Authentifizierungsserver angeben, wird beim Versuch, die Konfiguration zu speichern, eine Fehlermeldung angezeigt.

Die maximale Zeit für die Authentifizierung über SSL-VPN beträgt drei (3) Minuten. Dieser Maximalwert wird durch die Nichtauthentifizierungs-Zeitüberschreitung festgelegt, die standardmäßig 3 Minuten beträgt und nicht konfigurierbar ist. Wenn mehrere Authentifizierungsserver in der Autorisierungskette vorhanden sind und die Benutzerauthentifizierung länger als 3 Minuten dauert, wird der Benutzer infolgedessen nicht authentifiziert.

Voraussetzungen

- [Navigieren zum Bildschirm „SSL-VPN Plus“](#).
- [Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway](#).

- Wenn Sie die Clientzertifikatauthentifizierung aktivieren möchten, stellen Sie sicher, dass ein CA-Zertifikat zum Edge-Gateway hinzugefügt wurde. Weitere Informationen finden Sie unter [Hinzufügen eines CA-Zertifikats zum Edge-Gateway für die Überprüfung der Vertrauenswürdigkeit von SSL-Zertifikaten](#).

Verfahren

- 1 Klicken Sie auf die Registerkarte **SSL VPN-Plus** und anschließend auf **Authentifizierung**.
- 2 Klicken Sie auf **Lokal**.

3 Konfigurieren Sie die Einstellungen des Authentifizierungsservers.

a (Optional) Aktivieren und konfigurieren Sie die Kennwortrichtlinie.

Option	Beschreibung
Kennwortrichtlinie aktivieren	Aktivieren Sie die Durchsetzung der Einstellungen für die Kennwortrichtlinie, die Sie hier konfigurieren.
Kennwortlänge	Geben Sie die zulässige minimale und maximale Zeichenanzahl für die Kennwortlänge ein.
Mindestanzahl Buchstaben	(Optional) Geben Sie die Mindestanzahl von Buchstabe ein, die für das Kennwort erforderlich sind.
Mindestanzahl Ziffern	(Optional) Geben Sie die Mindestanzahl von numerischen Zeichen ein, die für das Kennwort erforderlich sind.
Mindestanzahl Sonderzeichen	(Optional) Geben Sie die Mindestanzahl der Sonderzeichen ein, beispielsweise kaufmännisches Und-Zeichen (&), Hashtag (#), Prozentzeichen (%) usw., die für das Kennwort erforderlich sind.
Kennwort darf keine Benutzer-ID enthalten	(Optional) Aktivieren Sie diese Option, um durchzusetzen, dass das Kennwort nicht die Benutzer-ID enthalten darf.
Kennwort läuft ab in	(Optional) Geben Sie die maximale Gültigkeitsdauer in Tagen für ein Kennwort ein, bevor der Benutzer es ändern muss.
Ablaufbenachrichtigung in	(Optional) Geben Sie die Anzahl der Tage vor dem Wert Kennwort läuft ab in ein, bei dem der Benutzer benachrichtigt wird, dass das Kennwort in Kürze abläuft.

b (Optional) Aktivieren und konfigurieren Sie die Kontosperrungsrichtlinie.

Option	Beschreibung
Kontosperrungsrichtlinie aktivieren	Aktivieren Sie die Durchsetzung der Einstellungen für die Kontosperrungsrichtlinie, die Sie hier konfigurieren.
Wiederholungsanzahl	Geben Sie die Anzahl der Zugriffsversuche ein, die ein Benutzer auf sein Konto hat.
Wiederholungsdauer	Geben Sie das Zeitintervall in Minuten ein, nach dessen Ablauf das Konto des Benutzers bei fehlgeschlagenen Anmeldeversuchen gesperrt wird. Wenn Sie beispielsweise für Wiederholungsanzahl den Wert 5 und für Wiederholungsdauer 1 Minute festlegen, wird das Konto des Benutzers nach 5 fehlgeschlagenen Anmeldeversuchen innerhalb einer Minute gesperrt.
Sperrdauer	Geben Sie den Zeitraum ein, für den das Benutzerkonto gesperrt bleibt. Nach Ablauf dieses Zeitraums wird die Kontosperrung automatisch aufgehoben.

c Aktivieren Sie im Abschnitt „Status“ diesen Authentifizierungsserver.

- d (Optional) Konfigurieren Sie die sekundäre Authentifizierung.

Optionen	Beschreibung
Diesen Server für die sekundäre Authentifizierung verwenden	(Optional) Geben Sie an, ob der Server als zweite Authentifizierungsebene verwendet werden soll.
Sitzung bei Fehlschlag der Authentifizierung beenden	(Optional) Geben Sie an, ob die VPN-Sitzung beendet werden soll, wenn die Authentifizierung fehlschlägt.

- e Klicken Sie auf **Behalten**.

- 4 (Optional) Um die Clientzertifikatauthentifizierung zu aktivieren, klicken Sie auf **Zertifikat ändern**, aktivieren Sie die Umschaltoption für die Aktivierung und wählen Sie das zu verwendende CA-Zertifikat aus. Klicken Sie anschließend auf **OK**.

Nächste Schritte

Fügen Sie dem lokalen Authentifizierungsserver lokale Benutzer hinzu, damit diese eine Verbindung mit SSL VPN-Plus herstellen können. Weitere Informationen finden Sie unter [Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver](#).

Erstellen Sie ein Installationspaket, das den SSL-Client enthält, damit Remotebenutzer ihn auf ihren lokalen Systemen installieren können. Weitere Informationen finden Sie unter [Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients](#).

Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver


Verwenden Sie den Bildschirm **Benutzer** auf der Registerkarte **SSL VPN-Plus**, um dem lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways Konten für Remotebenutzer hinzuzufügen.

Hinweis Wenn noch kein lokaler Authentifizierungsserver konfiguriert wurde, wird durch das Hinzufügen eines Benutzers im Bildschirm **Benutzer** automatisch ein lokaler Authentifizierungsserver mit Standardwerten hinzugefügt. Über die Schaltfläche „Bearbeiten“ im Bildschirm **Authentifizierung** können Sie die Standardwerte anzeigen und bearbeiten. Informationen zur Verwendung des Bildschirms **Authentifizierung** finden Sie unter [Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem Edge-Gateway](#).

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Benutzer**.
- 2 Klicken Sie auf die Schaltfläche **Erstellen** ()

3 Konfigurieren Sie die folgenden Optionen für den Benutzer:

Option	Beschreibung
Benutzer-ID	Geben Sie die Benutzer-ID ein.
Kennwort	Geben Sie ein Kennwort für den Benutzer ein.
Kennwort erneut eingeben	Geben Sie das Kennwort erneut ein.
Vorname	(Optional) Geben Sie den Vornamen des Benutzers ein.
Nachname	(Optional) Geben Sie den Nachnamen des Benutzers ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für den Benutzer ein.
Aktiviert	Geben Sie an, ob der Benutzer aktiviert oder deaktiviert ist.
Kennwort läuft nie ab	(Optional) Geben Sie an, ob für diesen Benutzer dasselbe Kennwort beibehalten werden soll.
Kennwortänderung erlauben	(Optional) Geben Sie an, ob der Benutzer das Kennwort ändern kann.
Kennwort bei der nächsten Anmeldung ändern	(Optional) Geben Sie an, ob dieser Benutzer das Kennwort bei der nächsten Anmeldung ändern muss.

4 Klicken Sie auf **Behalten**.

5 Wiederholen Sie die Schritte, um weitere Benutzer hinzuzufügen.

Nächste Schritte

Fügen Sie dem lokalen Authentifizierungsserver lokale Benutzer hinzu, damit diese eine Verbindung mit SSL VPN-Plus herstellen können. Weitere Informationen finden Sie unter [Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver](#).

Erstellen Sie ein Installationspaket mit dem SSL-Client, damit Remotebenutzer diesen auf ihren lokalen Systemen installieren können. Weitere Informationen finden Sie unter [Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients](#).

Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients

Verwenden Sie den Bildschirm „Installationspakete“ auf der Registerkarte **SSL VPN-Plus**, um benannte Installationspakete des SSL VPN-Plus-Clients für die Remotebenutzer zu erstellen.


Sie können dem Edge-Gateway ein Installationspaket des SSL VPN-Plus-Clients hinzufügen. Neue Benutzer werden zum Herunterladen und Installieren dieses Pakets aufgefordert, wenn sie sich anmelden, um die VPN-Verbindung zum ersten Mal zu nutzen. Diese Clientinstallationspakete können nach dem Hinzufügen vom FQDN der öffentlichen Schnittstelle des Edge-Gateways heruntergeladen werden.


Sie können Installationspakete erstellen, die unter Windows-, Linux- und Mac-Betriebssysteme ausgeführt werden. Wenn Sie unterschiedliche Installationsparameter pro SSL VPN-Client benötigen, erstellen Sie ein Installationspaket für jede Konfiguration.

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“](#)

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im Mandantenportal auf **Installationspakete**.
- 2 Klicken Sie auf die Schaltfläche **Hinzufügen** ().
- 3 Konfigurieren Sie die Einstellungen für das Installationspaket.

Option	Beschreibung
Profilname	Geben Sie einen Profilnamen für dieses Installationspaket ein. Dieser Name wird dem Remotebenutzer angezeigt, um diese SSL-VPN-Verbindung zum Edge-Gateway zu identifizieren.
Gateway	Geben Sie die IP-Adresse oder den FQDN der öffentlichen Schnittstelle des Edge-Gateways ein. Die IP-Adresse oder der FQDN, die bzw. den Sie eingeben, ist an den SSL-VPN-Client gebunden. Wenn der Client auf dem lokalen System des Remotebenutzers installiert ist, wird diese IP-Adresse bzw. dieser FQDN auf diesem SSL VPN-Client angezeigt. Um zusätzliche Edge-Gateway-Uplink-Schnittstellen an diesen SSL-VPN-Client zu binden, klicken Sie auf die Schaltfläche Hinzufügen () , um Zeilen hinzuzufügen und ihre Schnittstellen-IP-Adressen oder FQDNs und Ports einzugeben.
Port	(Optional) Um den Portwert des angezeigten Standardwerts zu ändern, doppelklicken Sie auf den Wert und geben Sie einen neuen Wert ein.
Windows Linux Mac	Wählen Sie die Betriebssysteme aus, für die Sie die Installationspakete erstellen möchten.
Beschreibung	(Optional) Geben Sie eine Beschreibung für den Benutzer ein.
Aktiviert	Geben Sie an, ob dieses Paket aktiviert oder deaktiviert ist.

- 4 Wählen Sie die Installationsparameter für Windows aus.

Option	Beschreibung
Client bei der Anmeldung starten	Startet den SSL-VPN-Client, wenn sich der Remotebenutzer beim lokalen System anmeldet.
Kennwortspeicherung erlauben	Lässt zu, dass der Client das Kennwort des Benutzers speichert.
Unbeaufsichtigten Installationsmodus aktivieren	Blendet die Installationsbefehle der Remotebenutzer aus.
SSL-Client-Netzwerkadapter ausblenden	Blendet den VMware SSL VPN-Plus-Adapter aus, der zusammen mit dem Installationspaket des SSL-VPN-Clients auf dem Computer des Remotebenutzers installiert wird.
Taskleistensymbol für Client ausblenden	Mit dieser Option können Sie das SSL VPN-Taskleistensymbol, das angibt, ob die VPN-Verbindung aktiv ist oder nicht, ausblenden.
Desktopsymbol erstellen	Erstellt auf dem Desktop des Benutzers ein Symbol zum Aufrufen des SSL-Clients.

Option	Beschreibung
Unbeaufsichtigten Betriebsmodus aktivieren	Blendet das Fenster mit der Information, dass die Installation abgeschlossen ist, aus.
Validierung des Serversicherheitszertifikats	Der SSL VPN-Client prüft das SSL VPN-Serverzertifikat, bevor die sichere Verbindung hergestellt wird.

5 Klicken Sie auf **Behalten**.

Nächste Schritte

Bearbeiten Sie die Clientkonfiguration. Weitere Informationen finden Sie unter [Bearbeiten der SSL VPN-Plus-Client-Konfiguration](#).

Bearbeiten der SSL VPN-Plus-Client-Konfiguration

Verwenden Sie den Bildschirm **Client-Konfiguration** auf der Registerkarte **SSL VPN-Plus**, um die Reaktion des SSL VPN-Client-Tunnels anzupassen, wenn sich der Remotebenutzer bei SSL VPN anmeldet.

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“](#)

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Client-Konfiguration**.
- 2 Wählen Sie den **Tunneling-Modus** aus.
 - Im Split-Tunnel-Modus fließt nur der VPN-Datenverkehr über das Edge-Gateway.
 - Im Full-Tunnel-Modus wird das Edge-Gateway zum Standard-Gateway des Remotebenutzers und der gesamte Datenverkehr (z. B. VPN, lokal und Internet) wird über dieses Gateway geleitet.
- 3 Geben Sie bei Verwendung des Full-Tunnel-Modus die IP-Adresse für das Standard-Gateway ein, das von den Clients der Remotebenutzer verwendet wird. Wählen Sie optional aus, ob der Datenverkehr im lokalen Subnetz von der Leitung über den VPN-Tunnel ausgeschlossen werden soll.
- 4 (Optional) Deaktivieren Sie die automatische erneute Verbindungsherstellung.

Automatische erneute Verbindungsherstellung aktivieren ist standardmäßig aktiviert. Wenn die automatische erneute Verbindungsherstellung aktiviert ist, verbindet der SSL VPN-Client Benutzer, deren Verbindung getrennt wurde, automatisch erneut.
- 5 (Optional) Aktivieren Sie optional auch die Möglichkeit für den Client, Remotebenutzer zu benachrichtigen, wenn ein Client-Upgrade verfügbar ist.

Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option aktivieren, können Remotebenutzer wahlweise das Upgrade installieren.
- 6 Klicken Sie auf **Änderungen speichern**.

Anpassen der allgemeinen SSL VPN-Plus-Einstellungen für ein Edge-Gateway

Das System legt standardmäßig einige SSL VPN-Plus-Einstellungen für ein Edge-Gateway in Ihrer vCloud Director-Umgebung fest. Auf dem Bildschirm **Allgemeine Einstellungen** auf der Registerkarte **SSL VPN-Plus** im vCloud Director-Mandantenportal können Sie diese Einstellungen anpassen.

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“.](#)

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Allgemeine Einstellungen**.
- 2 Bearbeiten Sie die allgemeinen Einstellungen entsprechend den Anforderungen Ihrer Organisation.

Option	Beschreibung
Mehrere Anmeldungen mit demselben Benutzernamen verhindern	Aktivieren Sie diese Einstellung, um einen Remotebenutzer auf eine aktive Anmeldungssitzung unter demselben Benutzernamen zu beschränken.
Komprimierung	Aktivieren Sie diese Einstellung, um die TCP-basierte intelligente Datenkomprimierung zu aktivieren und die Datenübertragungsgeschwindigkeit zu erhöhen.
Protokollierung aktivieren	Aktivieren Sie diese Einstellung, um ein Protokoll des Datenverkehrs bereitzustellen, der über das SSL VPN-Gateway geleitet wird. Die Protokollierung ist standardmäßig aktiviert.
Virtuelle Tastatur erzwingen	Aktivieren Sie diese Einstellung, um festzulegen, dass Remotebenutzer nur für die Eingabe von Anmeldeinformationen eine virtuelle Tastatur (Bildschirmtastatur) verwenden müssen.
Tasten der virtuellen Tastatur zufällig anordnen	Aktivieren Sie diese Einstellung, damit für die virtuelle Tastatur ein zufallsgeneriertes Tastenlayout verwendet wird.
Sitzungszeitüberschreitung bei Leerlauf	Geben Sie die Zeitüberschreitung der Sitzung bei Leerlauf in Minuten ein. Wenn während des angegebenen Zeitraums in der Sitzung eines Benutzers keine Aktivität stattfindet, wird die Sitzung des Benutzers getrennt. Der Standardwert des Systems ist 10 Minuten.
Benutzerbenachrichtigung	Geben Sie die Nachricht ein, die Remotebenutzern nach der Anmeldung angezeigt werden soll.
Öffentlichen URL-Zugriff aktivieren	Aktivieren Sie diese Einstellung, damit Remotebenutzer auf Sites zugreifen können, die nicht explizit von Ihnen für den Zugriff durch Remotebenutzer konfiguriert wurden.
Erzwungene Zeitüberschreitung aktivieren	Aktivieren Sie diese Einstellung, damit das System die Verbindung zu Remotebenutzern trennt, nachdem der Zeitraum verstrichen ist, den Sie im Feld Erzwungene Zeitüberschreitung angegeben haben.
Erzwungene Zeitüberschreitung	Geben Sie das Zeitlimit in Minuten ein. Dieses Feld wird angezeigt, wenn die Umschaltoption Erzwungene Zeitüberschreitung aktivieren aktiviert ist.

3 Klicken Sie auf **Änderungen speichern**.

Konfigurieren von IPsec-VPN

Die Edge-Gateways in einer vCloud Director-Umgebung unterstützen Site-to-Site Internet Protocol Security (IPsec), um sichere VPN-Tunnel zwischen VDC-Organisationsnetzwerken oder zwischen einem VDC-Organisationsnetzwerk und einer externen IP-Adresse einzurichten. Sie können den IPSec-VPN-Dienst auf einem Edge-Gateway konfigurieren.

Die Einrichtung einer IPsec-VPN-Verbindung von einem Remotenetzwerk zum Organisations-VDC ist das häufigste Szenario. Die NSX-Software stellt die IPsec-VPN-Funktionen eines Edge-Gateways bereit, u. a. Unterstützung für Zertifikatsauthentifizierung, vorinstallierter Schlüsselmodus und IP-Unicast-Datenverkehr zwischen dem Edge-Gateway und VPN-Remote-Routern. Sie können auch mehrere Subnetze für die Verbindung über IPsec-Tunnel mit dem internen Netzwerk hinter einem Edge-Gateway konfigurieren. Wenn Sie mehrere Subnetze für die Verbindung über IPsec-Tunnel mit dem internen Netzwerk konfigurieren, dürfen diese Subnetze und das interne Netzwerk hinter dem Edge-Gateway keine überlappenden Adressbereiche aufweisen.

Hinweis Wenn der lokale und der Remote-Peer eines IPsec-Tunnels überlappende IP-Adressen haben, ist die Datenverkehrsweiterleitung über den Tunnel möglicherweise inkonsistent, abhängig davon, ob lokal verbundene Routen und autoPlumbed-Routen vorhanden sind.

Die folgenden IPsec-VPN-Algorithmen werden unterstützt:

- AES (AES128-CBC)
- AES256 (AES265-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie-Hellman-Gruppe 2)
- DH-5 (Diffie-Hellman-Gruppe 5)
- DH-14 (Diffie-Hellman-Gruppe 14)

Hinweis Dynamische Routing-Protokolle werden mit IPsec-VPN nicht unterstützt. Wenn Sie einen IPsec-VPN-Tunnel zwischen einem Edge-Gateway der VDC-Organisation und einem physisches Gateway-VPN an einer Remote-Site konfigurieren, können Sie für diese Verbindung kein dynamisches Routing konfigurieren. Die IP-Adresse dieser Remote-Site kann nicht durch dynamisches Routing auf dem Edge-Gateway-Uplink gelernt werden.

Wie im Thema *Überblick über IPsec-VPN* im *NSX-Administratorhandbuch* beschrieben, wird die maximale Anzahl unterstützter Tunnel auf einem Edge-Gateway von seiner konfigurierten Größe bestimmt: „Kompakt“, „Groß“, „Vollständig“, „Vollständig-4“. Sie können die Größe des Edge-Gateways anzeigen, indem Sie sich bei der vCloud Director-Webkonsole anmelden, zum Edge-Gateway navigieren und die Aktion **Eigenschaften** verwenden, um die Edge-Gateway-Konfiguration anzuzeigen. Unter *vCloud Director-Administratorhandbuch* finden Sie weitere Informationen zur Verwendung der vCloud Director-Webkonsole.

Das Konfigurieren von IPsec-VPN auf einem Edge-Gateway ist ein mehrstufiger Prozess.

Hinweis Wenn eine Firewall zwischen den Tunnel-Endpoints vorhanden ist, müssen Sie nach dem Konfigurieren des IPsec-VPN-Diensts die Firewallregeln aktualisieren, um die folgenden IP-Protokolle und UDP-Ports zuzulassen:

- IP Protocol ID 50 (ESP)
 - IP Protocol ID 51 (AH)
 - UDP-Port 500 (IKE)
 - UDP-Port 4500
-

Verfahren

1 Navigieren zum Bildschirm „IPsec-VPN“

Im Bildschirm **IPsec-VPN** können Sie den IPsec-VPN-Dienst für ein Edge-Gateway konfigurieren.

2 Konfigurieren von IPsec-VPN-Site-Verbindungen für das Edge-Gateway

Verwenden Sie den Bildschirm **IPsec-VPN-Sites** im vCloud Director-Mandantenportal, um die Einstellungen zu konfigurieren, die zum Erstellen einer IPsec-VPN-Verbindung zwischen dem Organisations-VDC und einer anderen Site mithilfe der IPsec-VPN-Funktionen des Edge-Gateways benötigt werden.

3 Aktivieren des IPsec-VPN-Diensts auf einem Edge-Gateway

Wenn mindestens eine IPsec-VPN-Verbindung konfiguriert ist, können Sie den IPsec-VPN-Dienst auf dem Edge-Gateway aktivieren.

4 Angeben der globalen IPsec-VPN-Einstellungen

Verwenden Sie den Bildschirm **Globale Konfiguration**, um Einstellungen für die IPsec-VPN-Authentifizierung auf einer Edge-Gateway-Ebene zu konfigurieren. Auf dieser Seite können Sie einen globalen vorinstallierten Schlüssel festlegen und die Zertifizierungsauthentifizierung aktivieren.

Navigieren zum Bildschirm „IPsec-VPN“

Im Bildschirm **IPsec-VPN** können Sie den IPsec-VPN-Dienst für ein Edge-Gateway konfigurieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **VPN > IPsec-VPN**.

Nächste Schritte

Verwenden Sie den Bildschirm **IPsec-VPN-Sites**, um eine IPsec-VPN-Verbindung zu konfigurieren. Mindestens eine Verbindung muss konfiguriert werden, bevor Sie den IPsec-VPN-Dienst auf dem Edge-Gateway aktivieren können. Weitere Informationen finden Sie unter [Konfigurieren von IPsec-VPN-Site-Verbindungen für das Edge-Gateway](#).

Konfigurieren von IPsec-VPN-Site-Verbindungen für das Edge-Gateway

Verwenden Sie den Bildschirm **IPsec-VPN-Sites** im vCloud Director-Mandantenportal, um die Einstellungen zu konfigurieren, die zum Erstellen einer IPsec-VPN-Verbindung zwischen dem Organisations-VDC und einer anderen Site mithilfe der IPsec-VPN-Funktionen des Edge-Gateways benötigt werden.

Wenn Sie eine IPsec-VPN-Verbindung zwischen Sites konfigurieren, konfigurieren Sie die Verbindung aus der Sicht Ihres derzeitigen Standorts. Zum Einrichten einer Verbindung müssen Sie die Konzepte im Zusammenhang mit der vCloud Director-Umgebung verstehen, sodass Sie die VPN-Verbindung ordnungsgemäß konfigurieren.


- Die lokalen und Peer-Subnetze geben die Netzwerke an, mit denen das VPN eine Verbindung herstellt. Wenn Sie diese Subnetze in den Konfigurationen für IPsec-VPN-Sites angeben, geben Sie einen Netzwerkbereich und keine bestimmte IP-Adresse ein. Verwenden Sie das CIDR-Format, z. B. **192.168.99.0/24**.
- Die Peer-ID ist ein Bezeichner, der das Remotegerät eindeutig identifiziert, das die VPN-Verbindung beendet. In der Regel ist dies die öffentliche IP-Adresse. Bei Peers mit Zertifikatsauthentifizierung muss diese ID als Distinguished Name im Peer-Zertifikat festgelegt sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. NSX empfiehlt die Verwendung des FQDN oder der öffentlichen IP-Adresse des Remotegeräts als Peer-ID. Wenn die IP-Adresse des Peers aus einem anderen VDC-Organisationsnetzwerk stammt, geben Sie die native IP-Adresse des Peers ein. Wenn NAT für den Peer konfiguriert wurde, geben Sie die private IP-Adresse des Peers ein.
- Der Peer-Endpoint gibt die öffentliche IP-Adresse des Remotegeräts an, zu dem Sie eine Verbindung herstellen. Der Peer-Endpoint kann eine andere Adresse als die Peer-ID haben, wenn das Gateway des Peers nicht direkt über das Internet erreicht werden kann, sondern über ein anderes Gerät verbunden wird. Wenn NAT für den Peer konfiguriert wurde, geben Sie die öffentliche IP-Adresse ein, die das Gerät für NAT verwendet.

- Mit der lokalen ID wird die öffentliche IP-Adresse des Edge-Gateways des Organisations-VDCs angegeben. Sie können eine IP-Adresse oder einen Hostnamen zusammen mit der Firewall des Edge-Gateways eingeben.
- Der lokale Endpoint gibt das Netzwerk im Organisation-VDC an, in dem das Edge-Gateway überträgt. In der Regel stellt das externe Netzwerk des Edge-Gateways den lokalen Endpunkt dar.

Voraussetzungen

- [Navigieren zum Bildschirm „IPsec-VPN“](#).
- [Konfigurieren von IPsec-VPN](#).
- Wenn Sie beabsichtigen, ein globales Zertifikat als Authentifizierungsmethode zu verwenden, stellen Sie sicher, dass die Zertifikatauthentifizierung im Bildschirm **Globale Konfiguration** aktiviert ist. Weitere Informationen finden Sie unter [Angaben der globalen IPsec-VPN-Einstellungen](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf der Registerkarte **IPsec-VPN** auf **IPsec-VPN-Sites**.
- 3 Klicken Sie auf die Schaltfläche **Hinzufügen** ()
- 4 Konfigurieren Sie die Einstellungen für die IPsec-VPN-Verbindung.

Option	Aktion
Aktiviert	Aktivieren Sie diese Verbindung zwischen den zwei VPN-Endpoints.
PFS (Perfect Forward Secrecy) aktivieren	<p>Aktivieren Sie diese Option, damit das System eindeutige öffentliche Schlüssel für alle IPsec-VPN-Sitzungen generiert, die Ihre Benutzer initiieren. Durch Aktivieren von PFS wird sichergestellt, dass das System keine Verknüpfung zwischen dem privaten Schlüssel des Edge-Gateways und allen Sitzungsschlüsseln erstellt.</p> <p>Die Beschädigung eines Sitzungsschlüssels betrifft nur die Daten, die in der von diesem bestimmten Schlüssel geschützten Sitzung ausgetauscht wurden. Auf andere Daten wirkt sie sich nicht aus. Ein beschädigter privater Schlüssel des Servers kann nicht zum Entschlüsseln von archivierten Sitzungen oder zukünftigen Sitzungen verwendet werden.</p> <p>Wenn PFS aktiviert ist, tritt bei IPsec-VPN-Verbindungen mit diesem Edge-Gateway ein leichter Verarbeitungs-Overhead auf.</p> <p>Wichtig Der eindeutige Sitzungsschlüssel darf nicht zum Ableiten von zusätzlichen Schlüsseln verwendet werden. Zudem müssen beide Seiten des IPsec-VPN-Tunnels PFS unterstützen, damit es funktioniert.</p>

Option	Aktion
Name	(Optional) Geben Sie einen Namen für die Verbindung ein.
Lokale ID	<p>Geben Sie die externe IP-Adresse der Edge-Gateway-Instanz ein, die die öffentliche IP-Adresse des Edge-Gateways ist.</p> <p>Die IP-Adresse wird für die Peer-ID in der IPsec-VPN-Konfiguration auf der Remote-Site verwendet.</p>
Lokaler Endpoint	<p>Geben Sie das Netzwerk ein, das der lokale Endpoint für diese Verbindung ist.</p> <p>Der lokale Endpoint gibt das Netzwerk im Organisation-VDC an, in dem das Edge-Gateway überträgt. In der Regel ist das externe Netzwerk der lokale Endpoint.</p> <p>Wenn Sie unter Verwendung eines vorinstallierten Schlüssels einen IP-zu-IP-Tunnel hinzufügen, können die lokale ID und die ID des lokalen Endpoints identisch sein.</p>
Lokale Subnetze	<p>Geben Sie die Netzwerke ein, die von den Sites gemeinsam genutzt werden sollen, und verwenden Sie zur Eingabe mehrerer Subnetze ein Komma als Trennzeichen.</p> <p>Geben Sie einen Netzwerkbereich (keine spezifische IP-Adresse) ein, indem Sie die IP-Adresse im CIDR-Format eingeben, z. B. 192.168.99.0/24.</p>
Peer-ID	<p>Geben Sie eine Peer-ID ein, um die Peer-Site eindeutig zu identifizieren.</p> <p>Die Peer-ID ist ein Bezeichner, der das Remotegerät eindeutig identifiziert, das die VPN-Verbindung beendet. In der Regel ist dies die öffentliche IP-Adresse.</p> <p>Bei Peers mit Zertifikatsauthentifizierung muss die ID der Distinguished Name im Peer-Zertifikat sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. Eine Best Practice für NSX besteht darin, die öffentliche IP-Adresse oder den FQDN des Remotegeräts als Peer-ID zu verwenden.</p> <p>Wenn die IP-Adresse des Peers aus einem anderen VDC-Organisationsnetzwerk stammt, geben Sie die native IP-Adresse des Peers ein. Wenn NAT für den Peer konfiguriert wurde, geben Sie die private IP-Adresse des Peers ein.</p>
Peer-Endpoint	<p>Geben Sie die IP-Adresse oder den FQDN der Peer-Site ein, also die öffentliche Adresse des Remotegeräts, mit dem Sie eine Verbindung herstellen.</p> <p>Hinweis Wenn NAT für den Peer konfiguriert wurde, geben Sie die öffentliche IP-Adresse ein, die das Gerät für NAT verwendet.</p>
Peer-Subnetze	<p>Geben Sie das Remotenetzwerk ein, mit dem das VPN eine Verbindung herstellt, und verwenden Sie zur Eingabe mehrerer Subnetze ein Komma als Trennzeichen.</p> <p>Geben Sie einen Netzwerkbereich (keine spezifische IP-Adresse) ein, indem Sie die IP-Adresse im CIDR-Format eingeben, z. B. 192.168.99.0/24.</p>
Verschlüsselungsalgorithmus	<p>Wählen Sie den Typ des Verschlüsselungsalgorithmus im Dropdown-Menü aus.</p> <p>Hinweis Der Verschlüsselungstyp, den Sie auswählen, muss mit dem Verschlüsselungstyp übereinstimmen, der auf dem VPN-Gerät der Remote-Site konfiguriert ist.</p>

Option	Aktion
Authentifizierung	<p>Wählen Sie eine Authentifizierung aus. Zu den Optionen gehören:</p> <ul style="list-style-type: none"> ■ PSK „Vorinstallierter Schlüssel“ (Pre-Shared Key, PSK) gibt an, dass der vom Edge-Gateway und der Peer-Site gemeinsam verwendete geheime Schlüssel für die Authentifizierung verwendet wird. ■ Zertifikat Die Authentifizierung mittels Zertifikat gibt an, dass das auf globaler Ebene definierte Zertifikat für die Authentifizierung verwendet wird. Diese Option ist nicht verfügbar, es sei denn, Sie haben auf der Registerkarte IPsec-VPN im Bildschirm Globale Konfiguration das globale Zertifikat konfiguriert.
Gemeinsam verwendeten Schlüssel ändern	(Optional) Wenn Sie die Einstellungen einer vorhandenen Verbindung aktualisieren, können Sie diese Option aktivieren, um das Feld Vorinstallierter Schlüssel zur Verfügung zu stellen und den gemeinsam verwendeten Schlüssel zu aktualisieren.
Vorinstallierter Schlüssel	<p>Wenn Sie PSK als Authentifizierungstyp ausgewählt haben, geben Sie eine alphanumerische geheime Zeichenfolge ein. Diese Zeichenfolge darf maximal 128 Byte lang sein.</p> <p>Hinweis Der gemeinsam verwendete Schlüssel muss mit dem Schlüssel übereinstimmen, der auf dem VPN-Gerät der Remote-Site konfiguriert ist. Eine Best Practice besteht darin, einen gemeinsam verwendeten Schlüssel zu konfigurieren, wenn anonyme Sites eine Verbindung zum VPN-Dienst herstellen.</p>
Gemeinsam verwendeten Schlüssel anzeigen	(Optional) Aktivieren Sie diese Option, damit der gemeinsam verwendete Schlüssel auf dem Bildschirm angezeigt wird.
Diffie-Hellman-Gruppe	<p>Wählen Sie das kryptographische Schema aus, das es der Peer-Site und dem Edge-Gateway ermöglicht, über einen ungesicherten Kommunikationskanal einen gemeinsamen geheimen Schlüssel einzurichten.</p> <p>Hinweis Die Diffie-Hellman-Gruppe muss mit dem übereinstimmen, was auf dem VPN-Gerät der Remote-Site konfiguriert ist.</p>
Erweiterung	<p>(Optional) Geben Sie eine der folgenden Optionen ein:</p> <ul style="list-style-type: none"> ■ <code>securelocaltrafficbyip=IP-Adresse</code> zum Umleiten des lokalen Datenverkehrs des Edge-Gateways über den IPsec-VPN-Tunnel. Dies ist der Standardwert. ■ <code>passthroughSubnets=PeerSubnet/IPAddress</code>, um überlappende Subnetze zu unterstützen.

5 Klicken Sie auf **Behalten**.

6 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

Konfigurieren Sie die Verbindung für die Remote-Site. Sie müssen die IPsec-VPN-Verbindung auf beiden Seiten der Verbindung konfigurieren: dem Organisations-VDC und der Peer-Site.

Aktivieren Sie den IPsec-VPN-Dienst auf diesem Edge-Gateway. Wenn mindestens eine IPsec-VPN-Verbindung konfiguriert ist, können Sie den Dienst aktivieren. Weitere Informationen finden Sie unter [Aktivieren des IPsec-VPN-Diensts auf einem Edge-Gateway](#).

Aktivieren des IPsec-VPN-Diensts auf einem Edge-Gateway

Wenn mindestens eine IPsec-VPN-Verbindung konfiguriert ist, können Sie den IPsec-VPN-Dienst auf dem Edge-Gateway aktivieren.

Voraussetzungen

- [Navigieren zum Bildschirm „IPsec-VPN“](#).
- Stellen Sie sicher, dass mindestens eine IPsec-VPN-Verbindung für dieses Edge-Gateway konfiguriert ist. Weitere Informationen finden Sie in den unter [Konfigurieren von IPsec-VPN-Site-Verbindungen für das Edge-Gateway](#) beschriebenen Schritten.

Verfahren

- 1 Klicken Sie auf der Registerkarte „**IPsec-VPN**“ auf die Option **Aktivierungsstatus**.
- 2 Klicken Sie auf **IPSec-VPN-Dienststatus**, um den IPSec-VPN-Dienst zu aktivieren.
- 3 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

Der IPsec-VPN-Dienst des Edge-Gateways ist aktiv.

Angeben der globalen IPsec-VPN-Einstellungen

Verwenden Sie den Bildschirm **Globale Konfiguration**, um Einstellungen für die IPsec-VPN-Authentifizierung auf einer Edge-Gateway-Ebene zu konfigurieren. Auf dieser Seite können Sie einen globalen vorinstallierten Schlüssel festlegen und die Zertifizierungsauthentifizierung aktivieren.

Für Sites, deren Peer-Endpoint auf **Beliebig** festgelegt ist, wird ein globaler vorinstallierter Schlüssel verwendet.

Voraussetzungen

- Wenn Sie die Zertifikatsauthentifizierung aktivieren möchten, stellen Sie sicher, dass auf dem Bildschirm **Zertifikate** mindestens ein Dienstzertifikat sowie entsprechende von einer Zertifizierungsstelle signierte Zertifikate angezeigt werden. Selbstsignierte Zertifikate können nicht für IPSec-VPNs verwendet werden. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).
- [Navigieren zum Bildschirm „IPsec-VPN“](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf der Registerkarte **IPsec-VPN** auf die Option **Globale Konfiguration**.
- 3 (Optional) Legen Sie einen globalen vorinstallierten Schlüssel fest:
 - a Aktivieren Sie die Option **Gemeinsam verwendeten Schlüssel ändern**.
 - b Geben Sie einen vorinstallierten Schlüssel ein.

 Der globale vorinstallierte Schlüssel (Pre-Shared Key, PSK) wird von allen Sites geteilt, deren Peer-Endpoint auf `any` festgelegt ist. Wenn bereits ein globaler PSK festgelegt ist, wirkt sich das Ändern des PSK in einen leeren Wert mit anschließendem Speichern nicht auf die vorhandene Einstellung aus.
 - c (Optional) Aktivieren Sie optional **Gemeinsam verwendeten Schlüssel anzeigen**, um den vorinstallierten Schlüssel sichtbar zu machen.
 - d Klicken Sie auf **Änderungen speichern**.
- 4 Konfigurieren Sie die Zertifizierungsauthentifizierung:
 - a Aktivieren Sie die Option **Zertifikatsauthentifizierung aktivieren**.
 - b Wählen Sie die geeigneten Dienstzertifikate, die Zertifikate der Zertifizierungsstelle und die CRLs aus.
 - c Klicken Sie auf **Änderungen speichern**.

Nächste Schritte

Sie können optional Protokollierung für den IPsec-VPN-Dienst des Edge-Gateways aktivieren. Weitere Informationen finden Sie unter [Statistiken und Protokolle für ein Edge-Gateway](#).

L2 VPN konfigurieren

Die Edge-Gateways in einer vCloud Director-Umgebung unterstützen L2 VPN. L2 VPN lässt eine Erweiterung Ihres Organisations-VDC zu, indem die virtuellen Maschinen Netzwerkkonnektivität unter Verwendung derselben IP-Adresse über geografische Grenzen hinweg beibehalten können. Sie können den L2 VPN-Dienst auf einem Edge-Gateway konfigurieren.

Die NSX-Software stellt die L2 VPN-Funktionen eines Edge-Gateways bereit. Mit L2 VPN kann ein Tunnel zwischen zwei Sites konfiguriert werden. Virtuelle Maschinen verbleiben im selben Subnetz, obwohl sie zwischen diesen Sites verschoben werden. Daher können Sie das Organisations-VDC erweitern, indem Sie sein Netzwerk mit L2 VPN ausdehnen. Ein Edge-Gateway auf einer Site kann alle Dienste für virtuelle Maschinen auf der anderen Site bereitstellen.

Um den L2 VPN-Tunnel zu erstellen, konfigurieren Sie einen L2 VPN-Server und einen L2 VPN-Client. Wie im *Administratorhandbuch für NSX* beschrieben, ist der L2 VPN-Server das Ziel-Edge-Gateway und der L2 VPN-Client das Quell-Edge-Gateway. Nach dem Konfigurieren der L2 VPN-Einstellungen auf jedem Edge-Gateway müssen Sie den L2 VPN-Dienst sowohl auf dem Server als auch auf dem Client aktivieren.

Hinweis Auf den Edge-Gateways muss ein geroutetes VDC-Organisationsnetzwerk vorhanden sein, das als Teilschnittstelle erstellt wurde. Unter *vCloud Director-Administratorhandbuch* finden Sie die Schritte für die Erstellung eines externen gerouteten VDC-Organisationsnetzwerks.

Navigieren zum Bildschirm „L2 VPN“

Zum Konfigurieren des L2 VPN-Diensts für ein Edge-Gateway müssen Sie zum Bildschirm **L2 VPN** navigieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Navigieren Sie zu **VPN > L2 VPN**.

Nächste Schritte

Konfigurieren Sie den L2 VPN-Server. Weitere Informationen finden Sie unter [Konfigurieren des Edge-Gateways als L2 VPN-Server](#).

Konfigurieren des Edge-Gateways als L2 VPN-Server

Der L2 VPN-Server ist der Ziel-NSX Edge, mit dem der L2 VPN-Client eine Verbindung herstellen wird.

Wie im *Administratorhandbuch für NSX* beschrieben, können Sie mehrere Peer-Sites mit diesem L2 VPN-Server verbinden.

Hinweis Änderungen an den Site-Konfigurationseinstellungen führen dazu, dass das Edge-Gateway alle vorhandenen Verbindungen trennt und erneut herstellt.

Voraussetzungen


- Stellen Sie sicher, dass das Edge-Gateway über ein geroutetes VDC-Organisationsnetzwerk verfügt, das als Teilschnittstelle auf dem Edge-Gateway konfiguriert ist. Unter *vCloud Director-Administratorhandbuch* finden Sie die Schritte für die Erstellung eines externen gerouteten VDC-Organisationsnetzwerks.
- [Navigieren zum Bildschirm „L2 VPN“](#).

- Wenn Sie ein Dienstzertifikat an die L2 VPN-Verbindung binden möchten, vergewissern Sie sich, dass das Serverzertifikat bereits auf das Edge-Gateway hochgeladen wurde. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).
- Sie müssen die Listener-IP des Servers, den Listener-Port, den Verschlüsselungsalgorithmus und mindestens eine Peer-Site konfiguriert haben, bevor Sie den L2 VPN-Dienst aktivieren können.

Verfahren

- 1 Wählen Sie auf der Registerkarte **L2 VPN** die Option **Server** für den L2 VPN-Modus aus.
- 2 Konfigurieren Sie auf der Registerkarte **Server – Global** die globalen Konfigurationsdetails des L2 VPN-Servers.

Option	Aktion
Listener-IP	Wählen Sie die primäre oder sekundäre IP-Adresse einer externen Schnittstelle des Edge-Gateways aus.
Listener-Port	Bearbeiten Sie den angezeigten Wert entsprechend den Anforderungen Ihrer Organisation. Der Standardport für den L2 VPN-Dienst ist 443.
Verschlüsselungsalgorithmus	Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation zwischen dem Server und dem Client aus.
Details des Dienstzertifikats	Klicken Sie auf Serverzertifikat ändern , um das Zertifikat auszuwählen, das an den L2 VPN-Server gebunden werden soll. Aktivieren Sie im Fenster Serverzertifikat ändern die Option Serverzertifikat überprüfen , wählen Sie in der Liste ein Serverzertifikat aus und klicken Sie auf OK .

- 3 Zur Konfiguration der Peer-Sites klicken Sie auf die Registerkarte **Server-Sites**.
- 4 Klicken Sie auf die Schaltfläche **Hinzufügen** ().
- 5 Konfigurieren Sie die Einstellungen für eine L2 VPN-Peer-Site.

Option	Aktion
Aktiviert	Aktivieren Sie diese Peer-Site.
Name	Geben Sie einen eindeutigen Namen für die Peer-Site ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung ein.
Benutzer-ID	Geben Sie den Benutzernamen und das Kennwort ein, mit denen die Peer-Site authentifiziert werden soll.
Kennwort	Die Benutzeranmeldedaten auf der Peer-Site müssen mit den Anmeldedaten auf der Clientseite identisch sein.
Kennwort bestätigen	

Option	Aktion
Ausgeweitete Schnittstellen	Wählen Sie mindestens eine Teilschnittstelle aus, die mit dem Client ausgeweitet werden soll. Die zur Auswahl stehenden Teilschnittstellen sind die VDC-Organisationsnetzwerke, die als Teilschnittstellen auf dem Edge-Gateway konfiguriert sind.
Adresse des Egress-Optimierungs-Gateways	(Optional) Wenn das Standard-Gateway für virtuelle Maschinen auf beiden Sites das gleiche ist, geben Sie die Gateway-IP-Adressen der Teilschnittstellen ein, für die der Datenverkehr lokal weitergeleitet oder über den L2 VPN-Tunnel blockiert werden soll.

6 Klicken Sie auf **Behalten**.

7 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

Aktivieren Sie den L2 VPN-Dienst auf diesem Edge-Gateway. Weitere Informationen finden Sie unter [Aktivieren des L2 VPN-Diensts auf einem Edge-Gateway](#).

Konfigurieren des Edge-Gateways als L2 VPN-Client

Der L2 VPN-Client ist das quellseitige NSX Edge-Gateway, das die Kommunikation mit dem zielseitigen NSX Edge-Gateway, dem L2 VPN-Server, initiiert.

Voraussetzungen

- [Navigieren zum Bildschirm „L2 VPN“](#).
- Wenn dieser L2 VPN-Client eine Verbindung mit einem L2 VPN-Server herstellt, der ein Serverzertifikat verwendet, müssen Sie überprüfen, ob das entsprechende CA-Zertifikat auf das Edge-Gateway hochgeladen wurde, um die Validierung des Serverzertifikats für diesen L2 VPN-Client zu ermöglichen. Weitere Informationen finden Sie unter [Hinzufügen eines CA-Zertifikats zum Edge-Gateway für die Überprüfung der Vertrauenswürdigkeit von SSL-Zertifikaten](#).

Verfahren

- 1 Wählen Sie auf der Registerkarte **L2 VPN** die Option **Client** für den L2 VPN-Modus aus.
- 2 Konfigurieren Sie auf der Registerkarte **Client – Global** die globalen Konfigurationsdetails des L2 VPN-Clients.

Option	Beschreibung
Serveradresse	Geben Sie die IP-Adresse des L2 VPN-Servers ein, mit dem dieser Client verbunden werden soll.
Server-Port	Geben Sie den Port des L2 VPN-Servers ein, mit dem der Client eine Verbindung herstellen soll. Der Standardport ist 443.

Option	Beschreibung
Verschlüsselungsalgorithmus	Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation mit dem Server aus.
Ausgeweitete Schnittstellen	Wählen Sie die Teilschnittstellen aus, die auf den Server ausgeweitet werden sollen. Die zur Auswahl stehenden Teilschnittstellen sind die VDC-Organisationsnetzwerke, die als Teilschnittstellen auf dem Edge-Gateway konfiguriert sind.
Adresse des Egress-Optimierungs-Gateways	(Optional) Wenn das Standard-Gateway für virtuelle Maschinen bei den beiden Sites identisch ist, geben Sie die Gateway-IP-Adressen der Teilschnittstellen oder die IP-Adressen ein, an die der Datenverkehr nicht über den Tunnel fließen soll.
Benutzerdetails	Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung beim Server ein.

3 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

4 (Optional) Um erweiterte Optionen zu konfigurieren, klicken Sie auf die Registerkarte **Client – Erweitert**.

5 Wenn dieses L2 VPN-Client-Edge-Gateway keinen direkten Zugriff auf das Internet hat und das L2 VPN-Server-Edge-Gateway über einen Proxyserver erreichen muss, geben Sie die Proxyeinstellungen an.

Option	Beschreibung
Sicheren Proxy aktivieren	Wählen Sie diese Option aus, um den sicheren Proxy zu aktivieren.
Adresse	Geben Sie die IP-Adresse des Proxyservers ein.
Port	Geben Sie den Port des Proxyservers ein.
Benutzername Kennwort	Geben Sie Anmeldeinformationen für die Authentifizierung des Proxyservers ein.

6 Um die Validierung der Serverzertifizierung zu aktivieren, klicken Sie auf **Zertifikat der Zertifizierungsstelle ändern** und wählen Sie das entsprechende CA-Zertifikat aus.

7 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

Aktivieren Sie den L2 VPN-Dienst auf diesem Edge-Gateway. Weitere Informationen finden Sie unter [Aktivieren des L2 VPN-Diensts auf einem Edge-Gateway](#).

Aktivieren des L2 VPN-Diensts auf einem Edge-Gateway

Wenn die erforderlichen L2 VPN-Einstellungen konfiguriert sind, können Sie den L2 VPN-Dienst auf dem Edge-Gateway aktivieren.

Hinweis Wenn HA bereits auf diesem Edge-Gateway konfiguriert ist, müssen Sie sicherstellen, dass für das Edge-Gateway mehr als eine interne Schnittstelle konfiguriert ist. Wenn nur eine einzige Schnittstelle vorhanden ist und diese bereits durch die HA-Funktion verwendet wurde, schlägt die L2 VPN-Konfiguration für dieselbe interne Schnittstelle fehl.

Voraussetzungen

- Wenn dieses Edge-Gateway ein L2 VPN-Server ist, d. h. das Ziel-NSX-Edge, müssen Sie sicherstellen, dass die erforderlichen L2 VPN-Servereinstellungen und mindestens eine L2 VPN-Peer-Site konfiguriert sind. Weitere Informationen finden Sie in den unter [Konfigurieren des Edge-Gateways als L2 VPN-Server](#) beschriebenen Schritten.
- Wenn dieses Edge-Gateway ein L2 VPN-Client ist, d. h. das Quell-NSX-Edge, müssen Sie sicherstellen, dass die L2 VPN-Clienteneinstellungen konfiguriert sind. Weitere Informationen finden Sie in den unter [Konfigurieren des Edge-Gateways als L2 VPN-Client](#) beschriebenen Schritten.
- [Navigieren zum Bildschirm „L2 VPN“](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **L2 VPN** auf die Umschaltfläche **Aktivieren**.
- 2 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

Der L2 VPN-Dienst des Edge-Gateways wird aktiv.

Nächste Schritte

Erstellen Sie NAT- oder Firewallregeln auf der mit dem Internet verbundenen Seite der Firewall, um die Verbindung des L2 VPN-Servers mit dem L2 VPN-Client zu aktivieren.

Entfernen der L2 VPN-Dienstkonfiguration von einem Edge-Gateway

Sie können die vorhandene L2 VPN-Dienstkonfiguration des Edge-Gateways entfernen. Durch diese Aktion wird auch der L2 VPN-Dienst auf dem Edge-Gateway deaktiviert.

Voraussetzungen

[Navigieren zum Bildschirm „L2 VPN“](#)

Verfahren

- 1 Führen Sie einen Bildlauf zum unteren Rand des Bildschirms „L2 VPN“ aus und klicken Sie auf **Konfiguration löschen**.

2 Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Ergebnisse

Der L2 VPN-Dienst wird deaktiviert, und die Konfigurationsdetails werden vom Edge-Gateway entfernt.

SSL-Zertifikatsverwaltung

Die NSX-Software in der vCloud Director-Umgebung bietet die Möglichkeit, Secure Sockets Layer (SSL)-Zertifikate mit den für Ihre Edge-Gateways konfigurierten Tunneln SSL VPN-Plus und IPsec-VPN zu verwenden.

Die Edge-Gateways in Ihrer vCloud Director-Umgebung unterstützen selbstsignierte Zertifikate, von einer Zertifizierungsstelle (CA) signierte Zertifikate und Zertifikate, die von einer Zertifizierungsstelle generiert und signiert wurden. Sie können CSRs (Certificate Signing Requests, Zertifikatsignieranforderungen) generieren, die Zertifikate importieren, die importierten Zertifikate verwalten und CRLs (Certificate Revocation Lists, Zertifikatswiderrufslisten) erstellen.

Informationen zur Verwendung von Zertifikaten mit Ihrem Organisations-VDC

Sie können Zertifikate für die folgenden Netzwerkbereiche in Ihrem vCloud Director-Organisations-VDC verwalten.

- IPsec-VPN-Tunnel zwischen einem VDC-Organisationsnetzwerk und einem Remotenetzwerk.
- SSL VPN-Plus-Verbindungen zwischen Remotebenutzern, privaten Netzwerken und Webressourcen in Ihrem Organisations-VDC.
- Ein L2 VPN-Tunnel zwischen zwei NSX-Edge-Gateways.
- Die virtuellen Server und die Poolserver, die für den Lastausgleich in Ihrem Organisations-VDC konfiguriert sind

Verwendung von Clientzertifikaten

Sie können ein Clientzertifikat unter Verwendung eines CAI-Befehls oder eines REST-Aufrufs erstellen. Anschließend können Sie dieses Zertifikat an Ihre Remotebenutzer verteilen, die das Zertifikat dann im Webbrowser installieren können.

Der Hauptvorteil des Implementierens von Clientzertifikaten besteht darin, dass für jeden Remotebenutzer ein Client-Referenzzertifikat gespeichert und anhand des vom Remotebenutzer bereitgestellten Clientzertifikats überprüft werden kann. Um zu verhindern, dass ein bestimmter Benutzer zukünftig eine Verbindung herstellt, können Sie das Referenzzertifikat aus der Liste der Clientzertifikate des Sicherheitsservers löschen. Durch das Löschen des Zertifikats kann der Benutzer keine Verbindungen herstellen.

Generieren einer Zertifikatsignieranforderung für ein Edge-Gateway

Bevor Sie ein signiertes Zertifikat bei einer Zertifizierungsstelle anfordern oder ein selbstsigniertes Zertifikat erstellen können, müssen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für Ihr Edge-Gateway generieren.

Eine CSR ist eine codierte Datei, die Sie benötigen, um auf einem NSX Edge Gateway, das ein SSL-Zertifikat benötigt, ein Zertifikat zu generieren. Durch eine CSR wird die Art und Weise, wie Unternehmen ihre öffentlichen Schlüssel zusammen mit den Informationen senden, die ihre Unternehmens- und Domännennamen identifizieren, standardisiert.

Sie generieren eine CSR mit einer übereinstimmenden Datei mit dem privaten Schlüssel, die auf dem Edge-Gateway verbleiben muss. Die CSR enthält den passenden öffentlichen Schlüssel sowie weitere Informationen, wie z. B. Namen, Standort und Domännennamen Ihrer Organisation.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Zertifikate**.
- 3 Klicken Sie auf der Registerkarte **Zertifikate** auf **CSR**.
- 4 Konfigurieren Sie die folgenden Optionen für die CSR:

Option	Beschreibung
Allgemeiner Name	Geben Sie den vollqualifizierten Domännennamen (FQDN) für die Organisation ein, für die Sie das Zertifikat verwenden möchten (z. B. <code>www.example.com</code>). Schließen Sie das Präfix <code>http://</code> oder <code>https://</code> nicht in den allgemeinen Namen ein.
Organisationseinheit	Verwenden Sie dieses Feld, um zwischen Abteilungen innerhalb Ihrer vCloud Director-Organisation zu unterscheiden, denen dieses Zertifikat zugeordnet ist. Zum Beispiel Konstruktion oder Vertrieb.
Name der Organisation	Geben Sie den Namen ein, unter dem Ihr Unternehmen gesetzlich eingetragen ist. Die aufgeführte Organisation muss der gesetzliche Registrant des Domännennamens in der Zertifikatsanforderung sein.
Ort	Geben Sie die Stadt oder den Ort an, in der bzw. dem Ihr Unternehmen gesetzlich eingetragen ist.
Bundesland oder Kanton	Geben Sie den vollständigen Namen (keine Abkürzungen) des Bundeslandes, des Kantons, der Region oder des Gebiets ein, in dem bzw. der Ihr Unternehmen gesetzlich eingetragen ist.
Ländercode	Geben Sie den Namen des Landes ein, in dem Ihr Unternehmen gesetzlich eingetragen ist.

Option	Beschreibung
Algorithmus für privaten Schlüssel	Geben Sie den Schlüsseltyp für das Zertifikat ein (entweder RSA oder DSA). In der Regel wird RSA verwendet. Der Schlüsseltyp definiert den Verschlüsselungsalgorithmus für die Kommunikation zwischen den Hosts. Hinweis SSL VPN-Plus unterstützt nur RSA-Zertifikate.
Schlüsselgröße	Geben Sie die Schlüsselgröße in Bits ein. Die Mindestgröße beträgt 2048 Bits.
Beschreibung	(Optional) Geben Sie eine Beschreibung für das Zertifikat ein.

5 Klicken Sie auf **Behalten**.

Das System generiert die CSR und fügt einen neuen Eintrag mit dem Typ CSR in der Liste auf dem Bildschirm hinzu.

Ergebnisse

Wenn Sie in der Liste auf dem Bildschirm einen Eintrag mit dem Typ „CSR“ auswählen, werden die CSR-Details im Bildschirm angezeigt. Sie können die angezeigten PEM-formatierten Daten der CSR kopieren und an eine Zertifizierungsstelle (CA) übermitteln, um ein von einer Zertifizierungsstelle signiertes Zertifikat zu erhalten.

Nächste Schritte

Verwenden Sie die CSR, um mit einer der folgenden beiden Optionen ein Dienstzertifikat zu erstellen:

- Übertragen Sie die CSR an eine Zertifizierungsstelle, um ein von einer Zertifizierungsstelle signiertes Zertifikat zu erhalten. Wenn die Zertifizierungsstelle Ihnen das signierte Zertifikat sendet, importieren Sie das signierte Zertifikat in das System. Weitere Informationen finden Sie unter [Importieren des von der Zertifizierungsstelle signierten Zertifikats, das der für ein Edge-Gateway generierten CSR entspricht](#).
- Verwenden Sie die CSR, um ein selbstsigniertes Zertifikat erstellen. Weitere Informationen finden Sie unter [Konfigurieren eines selbstsignierten Dienstzertifikats](#).

Importieren des von der Zertifizierungsstelle signierten Zertifikats, das der für ein Edge-Gateway generierten CSR entspricht

Nachdem Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) generiert und das von der Zertifizierungsstelle signierte Zertifikat basierend auf dieser CSR bezogen haben, können Sie das von der Zertifizierungsstelle signierte Zertifikat importieren, damit es vom Edge-Gateway verwendet werden kann.

Voraussetzungen

Stellen Sie sicher, dass Sie das von der Zertifizierungsstelle signierte Zertifikat erhalten haben, das der CSR entspricht. Wenn der private Schlüssel in dem von der Zertifizierungsstelle signierten Zertifikat nicht dem für die ausgewählte CSR entspricht, schlägt der Importvorgang fehl.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Zertifikate**.
- 3 Wählen Sie die CSR in der Tabelle auf dem Bildschirm aus, für die Sie das von der Zertifizierungsstelle signierte Zertifikat importieren.
- 4 Importieren Sie das signierte Zertifikat.
 - a Klicken Sie auf **Signiertes für CSR generiertes Zertifikat**.
 - b Geben Sie die PEM-Daten des von der Zertifizierungsstelle signierten Zertifikats an.
 - Wenn sich die Daten in einer PEM-Datei auf einem System befinden, zu dem Sie navigieren können, klicken Sie auf die Schaltfläche **Hochladen**, um zu der Datei zu navigieren, und wählen Sie diese aus.
 - Falls Sie die PEM-Daten kopieren und einfügen können, fügen Sie sie in das Feld **Signiertes Zertifikat (PEM-Format)** ein.

Fügen Sie die Zeilen **-----BEGIN CERTIFICATE-----** und **-----END CERTIFICATE-----** hinzu.
 - c (Optional) Geben Sie eine Beschreibung ein.
 - d Klicken Sie auf **Behalten**.

Hinweis Wenn der private Schlüssel im von der Zertifizierungsstelle signierten Zertifikat nicht dem für die CSR, die Sie im Bildschirm „Zertifikate“ ausgewählt haben, entspricht, schlägt der Importvorgang fehl.

Ergebnisse

Das von der Zertifizierungsstelle signierte Zertifikat vom Typ „Dienstzertifikat“ wird in der Liste auf dem Bildschirm angezeigt.

Nächste Schritte

Fügen Sie das von der Zertifizierungsstelle signierte Zertifikat nach Bedarf dem SSL VPN-Plus- oder IPsec VPN-Tunnel hinzu. Weitere Informationen erhalten Sie unter [Konfigurieren der SSL-VPN-Servereinstellungen](#) und [Angaben der globalen IPsec-VPN-Einstellungen](#).

Konfigurieren eines selbstsignierten Dienstzertifikats

Sie können selbstsignierte Dienstzertifikate mit Ihren Edge-Gateways konfigurieren, um diese in den zugehörigen VPN-bezogenen Funktionen zu verwenden. Sie können selbstsignierte Zertifikate erstellen, installieren und verwalten.

Falls das Dienstzertifikat im Bildschirm „Zertifikate“ verfügbar ist, können Sie dieses Dienstzertifikat angeben, wenn Sie die VPN-bezogenen Einstellungen des Edge-Gateways konfigurieren. Das VPN zeigt das angegebene Dienstzertifikat für die Clients an, die auf das VPN zugreifen.

Voraussetzungen

Vergewissern Sie sich, dass auf dem Bildschirm **Zertifikate** für das Edge-Gateway mindestens eine CSR verfügbar ist. Weitere Informationen finden Sie unter [Generieren einer Zertifikatsignieranforderung für ein Edge-Gateway](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Zertifikate**.
- 3 Wählen Sie in der Liste die CSR aus, die Sie für dieses selbstsignierte Zertifikat verwenden möchten, und klicken Sie auf **Selbstsignierte CSR**.
- 4 Geben Sie die Anzahl der Tage ein, die das selbstsignierte Zertifikat gültig ist.
- 5 Klicken Sie auf **Behalten**.

Das System generiert das selbstsignierte Zertifikat und fügt einen neuen Eintrag mit dem Typ „Dienstzertifikat“ in der Liste auf dem Bildschirm hinzu.

Ergebnisse

Das selbstsignierte Zertifikat ist auf dem Edge-Gateway verfügbar. Wenn Sie in der Liste auf dem Bildschirm einen Eintrag mit dem Typ „Dienstzertifikat“ auswählen, werden die Details im Bildschirm angezeigt.

Hinzufügen eines CA-Zertifikats zum Edge-Gateway für die Überprüfung der Vertrauenswürdigkeit von SSL-Zertifikaten

Das Hinzufügen eines CA-Zertifikats zu einem Edge-Gateway ermöglicht die Überprüfung der Vertrauenswürdigkeit von SSL-Zertifikaten, die dem Edge-Gateway zur Authentifizierung vorgelegt werden, in der Regel die Clientzertifikate, die in VPN-Verbindungen zum Edge-Gateway verwendet werden.

In der Regel fügen Sie das Stammzertifikat Ihres Unternehmens oder Ihrer Organisation als CA-Zertifikat hinzu. Ein typischer Anwendungsfall ist SSL-VPN, bei dem Sie VPN-Clients unter Verwendung von Zertifikaten authentifizieren möchten. Clientzertifikate können an die VPN-Clients verteilt werden, und wenn die Verbindung der VPN-Clients hergestellt wird, werden dazugehörige Clientzertifikate anhand des CA-Zertifikats validiert.

Hinweis Beim Hinzufügen eines CA-Zertifikats konfigurieren Sie in der Regel eine relevante Zertifikatswiderrufsliste (Certificate Revocation List, CRL). Die CRL schützt vor Clients, die widerrufen Zertifikate vorlegen. Weitere Informationen finden Sie unter [Hinzufügen einer Zertifikatswiderrufsliste zu einem Edge-Gateway](#).

Voraussetzungen

Vergewissern Sie sich, dass die Daten der CA-Zertifikate im PEM-Format vorliegen. Auf der Benutzeroberfläche können Sie entweder die PEM-Daten des CA-Zertifikats einfügen oder zu einer Datei navigieren, die die Daten enthält und in Ihrem Netzwerk über das lokale System verfügbar ist.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Zertifikate**.
- 3 Klicken Sie auf **CA-Zertifikat**.
- 4 Geben Sie die Daten des CA-Zertifikats an.
 - Wenn sich die Daten in einer PEM-Datei auf einem System befinden, zu dem Sie navigieren können, klicken Sie auf die Schaltfläche **Hochladen**, um zu der Datei zu navigieren, und wählen Sie diese aus.
 - Falls Sie die PEM-Daten kopieren und einfügen können, fügen Sie sie in das Feld **CA-Zertifikat (PEM-Format)** ein.
 Fügen Sie die Zeilen `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----` hinzu.
- 5 (Optional) Geben Sie eine Beschreibung ein.
- 6 Klicken Sie auf **Behalten**.

Ergebnisse

Das CA-Zertifikat vom Typ „CA-Zertifikat“ wird in der Liste auf dem Bildschirm angezeigt. Dieses CA-Zertifikat kann nun von Ihnen angegeben werden, wenn Sie die VPN-bezogenen Einstellungen des Edge-Gateways konfigurieren.

Hinzufügen einer Zertifikatswiderrufsliste zu einem Edge-Gateway

Eine Zertifikatswiderrufsliste (Certificate Revocation List, CRL) ist eine Liste digitaler Zertifikate, die laut der ausstellenden Zertifizierungsstelle (CA) widerrufen wurden. Damit können Systeme aktualisiert werden, sodass Benutzern, die diese widerrufenen Zertifikate vorlegen, nicht vertraut wird. Sie können dem Edge-Gateway CRLs hinzufügen.

Wie im *Administratorhandbuch für NSX* beschrieben, enthält die CRL die folgenden Elemente:

- Die widerrufenen Zertifikate und den Grund des jeweiligen Widerrufs
- Das jeweilige Ausstellungsdatum des Zertifikats
- Der jeweilige Aussteller des Zertifikats
- Ein vorgeschlagenes Datum für die nächste Freigabe

Wenn ein potenzieller Benutzer versucht, auf einen Server zuzugreifen, wird anhand des CRL-Eintrags für den bestimmten Benutzer der Zugriff zugelassen oder verweigert.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Zertifikate**.
- 3 Klicken Sie auf **CRL**.
- 4 Geben Sie die CRL-Daten an.
 - Wenn sich die Daten in einer PEM-Datei auf einem System befinden, zu dem Sie navigieren können, klicken Sie auf die Schaltfläche **Hochladen**, um zu der Datei zu navigieren, und wählen Sie diese aus.
 - Wenn Sie die PEM-Daten kopieren und einfügen können, fügen Sie sie in das Feld **CRL (PEM-Format)** ein.
 Fügen Sie die Zeilen **-----BEGIN X509 CRL-----** und **-----END X509 CRL-----** hinzu.
- 5 (Optional) Geben Sie eine Beschreibung ein.
- 6 Klicken Sie auf **Behalten**.

Ergebnisse

Die CRL wird in der Liste auf dem Bildschirm angezeigt.

Hinzufügen eines Dienstzertifikats zum Edge-Gateway

Durch Hinzufügen von Dienstzertifikaten zu einem Edge-Gateway können diese Zertifikate in den VPN-bezogenen Einstellungen des Edge-Gateways verwendet werden. Sie können ein Dienstzertifikat dem Bildschirm **Zertifikate** hinzufügen.

Voraussetzungen

Vergewissern Sie sich, dass das Dienstzertifikat und der dazugehörige private Schlüssel im PEM-Format vorliegen. In der Benutzeroberfläche können Sie entweder die PEM-Daten einfügen oder zu einer Datei navigieren, die die Daten enthält und in Ihrem Netzwerk vom lokalen System aus verfügbar ist.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Zertifikate**.
- 3 Klicken Sie auf **Dienstzertifikat**.
- 4 Geben Sie die PEM-formatierten Daten des Dienstzertifikats ein.
 - Wenn sich die Daten in einer PEM-Datei auf einem System befinden, zu dem Sie navigieren können, klicken Sie auf die Schaltfläche **Hochladen**, um zu der Datei zu navigieren, und wählen Sie diese aus.
 - Falls Sie die PEM-Daten kopieren und einfügen können, fügen Sie sie in das Feld **Dienstzertifikat (PEM-Format)** ein.

Fügen Sie die Zeilen **-----BEGIN CERTIFICATE-----** und **-----END CERTIFICATE-----** hinzu.
- 5 Geben Sie die PEM-formatierten Daten des privaten Schlüssels des Zertifikats ein.
 - Wenn sich die Daten in einer PEM-Datei auf einem System befinden, zu dem Sie navigieren können, klicken Sie auf die Schaltfläche **Hochladen**, um zu der Datei zu navigieren, und wählen Sie diese aus.
 - Falls Sie die PEM-Daten kopieren und einfügen können, fügen Sie sie in das Feld **Privater Schlüssel (PEM-Format)** ein.

Fügen Sie die Zeilen **-----BEGIN RSA PRIVATE KEY-----** und **-----END RSA PRIVATE KEY-----** hinzu.
- 6 Geben Sie die Passphrase des privaten Schlüssels ein und bestätigen Sie sie.
- 7 (Optional) Geben Sie eine Beschreibung ein.
- 8 Klicken Sie auf **Behalten**.

Ergebnisse

Das Zertifikat vom Typ „Dienstzertifikat“ wird in der Liste auf dem Bildschirm angezeigt. Dieses Dienstzertifikat kann nun von Ihnen ausgewählt werden, wenn Sie die VPN-bezogenen Einstellungen des Edge-Gateways konfigurieren.

Benutzerdefiniertes Gruppieren von Objekten

Die NSX-Software in der vCloud Director-Umgebung bietet die Möglichkeit, Sätze und Gruppen von bestimmten Entitäten zu definieren, die Sie dann beim Angeben weiterer netzwerkbezogener Konfigurationen verwenden können, z. B. in Firewallregeln.

Erstellen eines IP Sets zur Verwendung in Firewallregeln und bei der DHCP-Relay-Konfiguration

Bei einem IP Set handelt es sich um eine Gruppe von IP-Adressen, die Sie auf Organisations-VDC-Ebene erstellen können. Sie können ein IP Set als Quelle oder Ziel in einer Firewallregel oder in einer DHCP-Relay-Konfiguration verwenden.

Sie können ein IP Set auf der Seite **Gruppierungsobjekte** des vCloud Director-Mandantenportals festlegen. Die Seite **Gruppierungsobjekte** ist auf den Bildschirmen „Dienste“ und „Edge-Gateway“ verfügbar.

Verfahren

- 1 Öffnen Sie die Seite „Gruppierungsobjekte“.

Option	Aktion
Öffnen über Edge-Gateway-Dienste	<ol style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Edges. b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.
Öffnen über Sicherheitsdienste	<ol style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Sicherheit. b Wählen Sie den zu bearbeitenden Sicherheitsdienst aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.

- 2 Klicken Sie auf die Registerkarte **IP Sets**.

Die bereits definierten IP Sets werden auf dem Bildschirm angezeigt.

- 3 Um ein IP Set hinzuzufügen, klicken Sie auf die Schaltfläche **Erstellen** (

- 4 Geben Sie einen Namen und optional eine Beschreibung für das IP Set sowie die IP-Adressen ein, die in das Set aufgenommen werden sollen.

- 5 (Optional) Wenn Sie das IP Set über die Seite **Gruppierungsobjekte** auf dem Bildschirm „Dienste“ angeben, verwenden Sie die Option **Vererbung**, um Vererbung zu aktivieren. Auf diese Weise wird die Sichtbarkeit in zugrunde liegenden Bereichen zugelassen.

Vererbung ist standardmäßig aktiviert.

- 6 Um das IP Set zu speichern, klicken Sie auf **Behalten**.

Ergebnisse

Das neue IP Set ist für die Auswahl als Quelle oder Ziel in Firewallregeln oder bei DHCP-Relay-Konfigurationen verfügbar.

Erstellen eines MAC Sets für die Verwendung in Firewallregeln

Bei einem MAC Set handelt es sich um eine Gruppe von MAC-Adressen, die Sie auf Organisations-VDC-Ebene erstellen können. Sie können ein MAC Set als Quelle oder Ziel in einer Firewallregel verwenden.

Sie können ein MAC Set auf der Seite **Gruppierungsobjekte** des vCloud Director-Mandantenportals erstellen. Die Seite „Gruppierungsobjekte“ ist auf den Bildschirmen **Dienste** und **Edge-Gateway** verfügbar.


Verfahren

- 1 Öffnen Sie die Seite „Gruppierungsobjekte“.

Option	Aktion
Öffnen über Edge-Gateway-Dienste	<ol style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Edges. b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.
Öffnen über Sicherheitsdienste	<ol style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Sicherheit. b Wählen Sie den zu bearbeitenden Sicherheitsdienst aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.

- 2 Klicken Sie auf die Registerkarte **MAC Sets**.

Die bereits definierten MAC Sets werden auf dem Bildschirm angezeigt.

- 3 Um ein MAC Set hinzuzufügen, klicken Sie auf die Schaltfläche **Erstellen** (- 4 Geben Sie einen Namen für das Set, optional eine Beschreibung sowie die MAC-Adressen ein, die in das Set aufgenommen werden sollen.
- 5 (Optional) Wenn Sie das MAC Set über die Seite **Gruppierungsobjekte** auf dem Bildschirm **Dienste** angeben, verwenden Sie die Option **Vererbung**, um Vererbung zu aktivieren. Auf diese Weise wird die Sichtbarkeit in zugrunde liegenden Bereichen zugelassen.

Vererbung ist standardmäßig aktiviert.

- 6 Um das MAC Set zu speichern, klicken Sie auf **Behalten**.

Ergebnisse

Das neue MAC Set ist für die Auswahl als Quelle oder Ziel in Firewallregeln verfügbar.

Anzeigen der für Firewallregeln verfügbaren Dienste

Sie können die Liste der Dienste anzeigen, die zur Verwendung in Firewallregeln bereitstehen. In diesem Kontext stellt ein Dienst eine Kombination aus Protokoll und Port dar.

Sie können die verfügbaren Dienste über die Seite „Gruppierungsobjekte“ des vCloud Director-Mandantenportals anzeigen. Die Seite „Gruppierungsobjekte“ ist auf den Bildschirmen „Dienste“ und „Edge-Gateway“ verfügbar.

Sie können keine neuen Dienste mithilfe der Mandantenportals hinzufügen. Die Dienste, die von Ihnen verwendet werden können, werden von Ihrem vCloud Director-Systemadministrator verwaltet.

Verfahren

- 1 Öffnen Sie die Seite „Gruppierungsobjekte“.

Option	Aktion
Öffnen über Edge-Gateway-Dienste	<ul style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Edges. b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.
Öffnen über Sicherheitsdienste	<ul style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Sicherheit. b Wählen Sie den zu bearbeitenden Sicherheitsdienst aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.

- 2 Klicken Sie auf die Registerkarte **Dienste**.

Ergebnisse

Die verfügbaren Dienste werden auf dem Bildschirm angezeigt.

Anzeigen der für Firewallregeln verfügbaren Dienstgruppen

Sie können die Liste der Dienstgruppen anzeigen, die zur Verwendung in Firewallregeln bereitstehen. In diesem Kontext stellt ein Dienst eine Kombination aus Protokoll und Port dar, und eine Dienstgruppe ist eine Gruppe von Diensten oder anderen Dienstgruppen.

Sie können die verfügbaren Dienstgruppen über die Seite „Gruppierungsobjekte“ des vCloud Director-Mandantenportals anzeigen. Die Seite „Gruppierungsobjekte“ ist auf den Bildschirmen „Dienste“ und „Edge-Gateway“ verfügbar.

Sie können keine Dienstgruppen mithilfe des Mandantenportals erstellen. Die Dienstgruppen, die von Ihnen verwendet werden können, werden von Ihrem vCloud Director-Systemadministrator verwaltet.

Verfahren

- 1 Öffnen Sie die Seite „Gruppierungsobjekte“.

Option	Aktion
Öffnen über Edge-Gateway-Dienste	<ol style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Edges. b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.
Öffnen über Sicherheitsdienste	<ol style="list-style-type: none"> a Navigieren Sie zu Netzwerk > Sicherheit. b Wählen Sie den zu bearbeitenden Sicherheitsdienst aus und klicken Sie auf Dienste konfigurieren. c Klicken Sie auf Gruppierungsobjekte.

- 2 Klicken Sie auf die Registerkarte **Dienstgruppen**.

Ergebnisse

Die verfügbaren Dienstgruppen werden auf dem Bildschirm angezeigt. In der Spalte „Beschreibung“ werden die Dienste angezeigt, die in jeder Dienstgruppe gruppiert sind.

Statistiken und Protokolle für ein Edge-Gateway

Sie können Statistiken und Protokolle für ein Edge-Gateway anzeigen.

Anzeigen von Statistiken

Sie können Statistiken auf dem Bildschirm **Edge-Gateway-Dienste** anzeigen.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- 2 Klicken Sie auf die Registerkarte **Statistik**.

- 3 Navigieren Sie durch die Registerkarten, je nachdem, welche Arten von Statistiken Sie anzeigen möchten.

Option	Beschreibung
Verbindungen	Der Bildschirm „Verbindungen“ bietet operative Transparenz. Der Bildschirm enthält Diagramme für den Datenverkehr, der über die Schnittstellen der ausgewählten Edge-Gateway-Instanz fließt, sowie Verbindungsstatistiken für die Firewall- und Lastausgleichsdienste. Wählen Sie den Zeitraum aus, für den Sie die Statistiken anzeigen möchten.
IPSec-VPN	Der Bildschirm „IPsec-VPN“ zeigt den Status und Statistiken für IPsec-VPN sowie den Status und Statistiken für jeden Tunnel an.
L2 VPN	Der Bildschirm „L2 VPN“ zeigt den Status und Statistiken für L2 VPN an.

Protokollierung aktivieren

Sie können die Protokollierung für ein Edge-Gateway aktivieren. Zusätzlich zur Aktivierung der Protokollierung für die Funktionen, für die Sie Protokolldaten erfassen möchten, müssen Sie zur Vervollständigung der Konfiguration einen Syslog-Server definieren, der die erfassten Protokolldaten empfangen soll. Wenn Sie einen Syslog-Server auf dem Bildschirm „Edge-Einstellungen“ konfigurieren, können Sie von diesem Syslog-Server aus auf die protokollierten Daten zugreifen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- Öffnen Sie „Edge-Gateway-Dienste“.
 - Navigieren Sie zu **Netzwerk > Edges**.
 - Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.
- Klicken Sie auf der Registerkarte **Edge-Einstellungen** auf die Schaltfläche **Syslog-Server bearbeiten**.

Sie können den Syslog-Server für die netzwerkbezogenen Protokolle Ihres Edge-Gateways für Dienste mit aktivierter Protokollierung anpassen.

Wenn der vCloud Director-Systemadministrator bereits einen Syslog-Server für die vCloud Director-Umgebung konfiguriert hat, verwendet das System standardmäßig diesen Syslog-Server. Die zugehörige IP-Adresse wird im Bildschirm **Edge-Einstellungen** angezeigt.

- Aktivieren Sie Protokollierung pro Funktion.
 - Klicken Sie auf der Registerkarte **NAT** auf die Schaltfläche **DNAT-Regel** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert die Adressübersetzung.

- Klicken Sie auf der Registerkarte **NAT** auf die Schaltfläche **SNAT-Regel** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert die Adressübersetzung.

- Klicken Sie auf der Registerkarte **Routing** auf **Routing-Konfiguration** und aktivieren Sie unter „Konfiguration für dynamisches Routing“ die Umschaltoption **Protokollierung aktivieren**.

Protokolliert die dynamischen Routing-Aktivitäten. Im Dropdown-Menü **Protokollebene** können Sie die untere Grenze der zu protokollierenden Nachrichtenstausebene festlegen.

- Klicken Sie auf der Registerkarte **Lastausgleichsdienst** auf **Globale Konfiguration** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert den Datenfluss für den Lastausgleichsdienst. Im Dropdown-Menü **Protokollebene** können Sie die untere Grenze der zu protokollierenden Nachrichtenstausebene festlegen.

- Gehen Sie auf der Registerkarte **VPN** zu **IPSec-VPN > Protokollierungseinstellungen** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert den Datenfluss zwischen dem lokalen Subnetz und dem Peer-Subnetz. Im Dropdown-Menü **Protokollebene** können Sie die untere Grenze der zu protokollierenden Nachrichtenstausebene festlegen.

- Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Allgemeine Einstellungen** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert den Datenfluss, der über das SSL-VPN-Gateway fließt.

- Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Servereinstellungen** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert die Aktivitäten, die auf dem SSL-VPN-Server für Syslog auftreten. Im Dropdown-Menü **Protokollebene** können Sie die untere Grenze der zu protokollierenden Nachrichtenstausebene festlegen.

Aktivieren des SSH-Befehlszeilenzugriffs auf ein Edge-Gateway

Sie können den SSH-Befehlszeilenzugriff über ein Edge-Gateway aktivieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Navigieren Sie zu **Netzwerk > Edges**.
 - b Wählen Sie das zu bearbeitende Edge-Gateway aus und klicken Sie auf **Dienste konfigurieren**.

- 2 Klicken Sie auf die Registerkarte **Edge-Einstellungen**.
- 3 Konfigurieren Sie die SSH-Einstellungen.

Option	Beschreibung
Benutzername	Geben Sie die Anmeldeinformationen für den SSH-Zugriff auf dieses Edge-Gateway ein.
Kennwort	
Kennwort erneut eingeben	Standardmäßig lautet der SSH-Benutzername admin .
Ablauf des Kennworts	Geben Sie den Ablaufzeitraum für das Kennwort in Tagen ein.
Anmelde-Banner	Geben Sie den Text ein, der Benutzern angezeigt werden soll, wenn sie eine SSH-Verbindung mit dem Edge-Gateway beginnen.

- 4 Aktivieren Sie die Option **Aktiviert**.

Nächste Schritte

Konfigurieren Sie die entsprechenden NAT- oder Firewallregeln, um den SSH-Zugriff auf dieses Edge-Gateway zu ermöglichen.

Arbeiten mit Sicherheitstags

Sicherheitstags sind Beschriftungen, die einer virtuellen Maschine oder einer Gruppe von virtuellen Maschinen zugeordnet werden können. Sicherheitstags sind zur Verwendung mit Sicherheitsgruppen konzipiert. Nachdem Sie die Sicherheitstags erstellt haben, ordnen Sie sie einer Sicherheitsgruppe zu, die in Firewallregeln verwendet werden kann. Sie können ein benutzerdefiniertes Sicherheitstag erstellen, bearbeiten oder zuweisen. Sie können auch anzeigen, für welche virtuellen Maschinen oder Sicherheitsgruppen ein bestimmtes Sicherheitstag angewendet wird.


Ein allgemeiner Anwendungsfall für Sicherheitstags ist die dynamische Gruppierung von Objekten, um Firewallregeln zu vereinfachen. Beispielsweise können Sie mehrere verschiedene Sicherheitstags basierend auf dem Typ der Aktivität erstellen, deren Auftreten Sie für eine bestimmte virtuelle Maschine erwarten. Erstellen Sie ein Sicherheitstag für Datenbankserver und ein Sicherheitstag für E-Mail-Server. Anschließend wenden Sie das entsprechende Tag auf virtuelle Maschinen an, die Datenbankserver oder E-Mail-Server enthalten. Später können Sie das Tag einer Sicherheitsgruppe zuweisen, eine Firewallregel dafür schreiben und verschiedene Sicherheitseinstellungen in Abhängigkeit davon anwenden, ob auf der virtuellen Maschine ein Datenbankserver oder ein E-Mail-Server ausgeführt wird. Wenn Sie im Anschluss daran die Funktionalität der virtuellen Maschine ändern, können Sie die virtuelle Maschine aus dem Sicherheitstag entfernen, anstatt die Firewallregel zu bearbeiten.

Erstellen und Zuweisen von Sicherheitstags

Sie können ein Sicherheitstag erstellen und es einer virtuellen Maschine oder einer Gruppe virtueller Maschinen zuweisen.

Sie erstellen ein Sicherheitstag und weisen es einer virtuellen Maschine oder einer Gruppe virtueller Maschinen zu.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie einen Sicherheitsdienst aus und klicken Sie auf **Dienste konfigurieren**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitstags**.
- 4 Klicken Sie auf die Schaltfläche **Erstellen** () und geben Sie einen Namen für das Sicherheitstag ein.
- 5 (Optional) Geben Sie eine Beschreibung für das Sicherheitstag ein.
- 6 (Optional) Weisen Sie das Sicherheitstag einer virtuellen Maschine oder einer Gruppe virtueller Maschinen zu.

Im Dropdown-Menü **Objekte dieses Typs durchsuchen** ist standardmäßig **Virtuelle Maschinen** ausgewählt.

- a Wählen Sie im linken Bereich eine virtuelle Maschine aus.
- b Klicken Sie auf den rechten Pfeil, um das Sicherheitstag der ausgewählten virtuellen Maschine zuzuweisen.

Die virtuelle Maschine wechselt in den rechten Bereich und wird dem Sicherheitstag zugewiesen.

- 7 Wenn Sie mit der Zuweisung des Tags zu den ausgewählten virtuellen Maschinen fertig sind, klicken Sie auf **Behalten**.

Ergebnisse

Das Sicherheitstag wird erstellt und wird den ausgewählten virtuellen Maschinen zugewiesen, wenn Sie diese Option ausgewählt haben.

Nächste Schritte


Sicherheitstags wurden für die Verwendung mit einer Sicherheitsgruppe konzipiert. Weitere Informationen zum Erstellen von Sicherheitsgruppen finden Sie unter [Erstellen einer Sicherheitsgruppe](#).

Ändern der Zuweisung von Sicherheitstags

Nachdem Sie ein Sicherheitstag erstellt haben, können Sie es manuell virtuellen Maschinen zuweisen. Sie können ein Sicherheitstag auch bearbeiten, um es von den virtuellen Maschinen zu entfernen, denen Sie es bereits zugewiesen haben.

Wenn Sie Sicherheitstags erstellt haben, können Sie sie virtuellen Maschinen zuweisen. Sie können Sicherheitstags zum Gruppieren von virtuellen Maschinen verwenden, um Firewallregeln zu schreiben. So können Sie z. B. einer Gruppe von virtuellen Maschinen mit sehr vertraulichen Daten ein Sicherheitstag zuweisen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie einen Sicherheitsdienst aus und klicken Sie auf **Dienste konfigurieren**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitstags**.
- 4 Wählen Sie in der Liste der Sicherheitstags das Sicherheitstag aus, das Sie bearbeiten möchten, und klicken Sie auf die Schaltfläche **Bearbeiten** ().
- 5 Wählen Sie im linken Fensterbereich virtuelle Maschinen aus und weisen Sie ihnen das Sicherheitstag zu, indem Sie auf den Rechtspfeil klicken.
Den virtuellen Maschinen im rechten Fensterbereich wird das Sicherheitstag zugewiesen.
- 6 Wählen Sie im rechten Fensterbereich virtuelle Maschinen aus und entfernen Sie das Tag von ihnen, indem Sie auf den Linkspfeil klicken.
Den virtuellen Maschinen im linken Fensterbereich ist kein Sicherheitstag zugewiesen.
- 7 Wenn Sie alle gewünschten Änderungen hinzugefügt haben, klicken Sie auf **Behalten**.

Ergebnisse

Das Sicherheitstag wird den ausgewählten virtuellen Maschinen zugewiesen.

Nächste Schritte

Sicherheitstags wurden für die Verwendung mit einer Sicherheitsgruppe konzipiert. Weitere Informationen zum Erstellen von Sicherheitsgruppen finden Sie unter [Erstellen einer Sicherheitsgruppe](#).

Anzeigen von angewendeten Sicherheitstags

Sie können die Sicherheitstags anzeigen, die auf virtuelle Maschinen in Ihrer Umgebung angewendet wurden. Sie können auch die Sicherheitstags anzeigen, die auf Sicherheitsgruppen in Ihrer Umgebung angewendet werden.

Voraussetzungen

Ein Sicherheitstag muss erstellt und auf eine virtuelle Maschine oder auf eine Sicherheitsgruppe angewendet worden sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie einen Sicherheitsdienst aus und klicken Sie auf **Dienste konfigurieren**.
- 3 Zeigen Sie die zugewiesenen Tags auf der Registerkarte **Sicherheitstags** an.
 - a Wählen Sie auf der Registerkarte **Sicherheitstags** das Sicherheitstag aus, dessen Zuweisungen Sie anzeigen möchten, und klicken Sie dann auf das Symbol **Bearbeiten**.
 - b Im Abschnitt **VMs zuweisen/Zuweisung von VMs aufheben** wird die Liste der dem Sicherheitstag zugewiesenen virtuellen Maschinen angezeigt.
 - c Klicken Sie auf **Verwerfen**.
- 4 Zeigen Sie die zugewiesenen Tags auf der Registerkarte **Sicherheitsgruppen** an .
 - a Klicken Sie auf die Registerkarte **Gruppierungsobjekte** und dann auf **Sicherheitsgruppen**.
 - b Wählen Sie eine Sicherheitsgruppe aus.
 - c In der Liste unter **Mitglieder einschließen** können Sie das einer Sicherheitsgruppe zugewiesene Sicherheitstag anzeigen.

Ergebnisse

Sie können die vorhandenen Sicherheitstags und die verknüpften virtuellen Maschinen und Sicherheitsgruppen anzeigen. Dadurch können Sie eine Strategie für die Erstellung von Firewallregeln basierend auf Sicherheitstags und Sicherheitsgruppen festlegen.


Bearbeiten eines Sicherheits-Tags

Sie können ein benutzerdefiniertes Sicherheits-Tag bearbeiten.

Wenn Sie die Umgebung oder die Funktion für eine virtuelle Maschine ändern, können Sie auch ein anderes Sicherheitstag verwenden, damit die Firewallregeln für die neue Maschinenkonfiguration korrekt sind. Wenn Sie z. B. auf einer virtuellen Maschine keine vertraulichen Daten mehr speichern, können Sie ihr ein anderes Sicherheitstag zuweisen, damit die Firewallregeln für vertrauliche Daten für diese virtuelle Maschine nicht mehr ausgeführt werden.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie einen Sicherheitsdienst aus und klicken Sie auf **Dienste konfigurieren**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitstags**.

- 4 Wählen Sie aus der Liste der Sicherheitstags das Sicherheitstag aus, das Sie bearbeiten möchten.
- 5 Klicken Sie auf die Schaltfläche **Bearbeiten** ().
- 6 Bearbeiten Sie den Namen und die Beschreibung der Sicherheitstags.
- 7 Weisen Sie das Tag den virtuellen Maschinen zu, die Sie auswählen, oder entfernen Sie die Zuweisung von den ausgewählten virtuellen Maschinen.
- 8 Klicken Sie zum Speichern der Änderungen auf **Behalten**.

Nächste Schritte


Wenn Sie ein Sicherheitstag bearbeiten, müssen Sie möglicherweise auch eine zugeordnete Sicherheitsgruppe oder Firewallregeln bearbeiten. Weitere Informationen zu Sicherheitsgruppen finden Sie unter [Arbeiten mit Sicherheitsgruppen](#).

Löschen eines Sicherheitstags

Sie können ein benutzerdefiniertes Sicherheitstag löschen.

Sie können ein Sicherheitstag löschen, wenn sich die Funktion oder Umgebung der virtuellen Maschine ändert. Wenn Sie z. B. ein Sicherheitstag für Oracle-Datenbanken haben, jedoch einen anderen Datenbankserver verwenden möchten, können Sie das Sicherheitstag entfernen, sodass für Oracle-Datenbanken geltende Firewallregeln nicht mehr für die virtuelle Maschine ausgeführt werden.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie unter **Netzwerk** die Option **Sicherheit** aus.
- 2 Wählen Sie einen Sicherheitsdienst aus und klicken Sie auf **Dienste konfigurieren**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitstags**.
- 4 Wählen Sie aus der Liste der Sicherheitstags das Sicherheitstag aus, das Sie löschen möchten.
- 5 Klicken Sie auf die Schaltfläche **Löschen** (.
- 6 Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Ergebnisse

Das Sicherheitstag wird gelöscht.

Nächste Schritte

Wenn Sie ein Sicherheitstag löschen, müssen Sie möglicherweise auch eine zugeordnete Sicherheitsgruppe oder Firewallregeln bearbeiten. Weitere Informationen zu Sicherheitsgruppen finden Sie unter [Arbeiten mit Sicherheitsgruppen](#).

Arbeiten mit Sicherheitsgruppen

Eine Sicherheitsgruppe ist eine Sammlung von Objekten oder Gruppierungsobjekten, wie z. B. virtuelle Maschinen, VDC-Organisationsnetzwerke oder Sicherheitstags.

Sicherheitsgruppen können dynamische Mitgliedschaftskriterien basierend auf Sicherheitstags, VM-Name, Name des VM-Gastbetriebssystems oder Name des VM-Gasthosts aufweisen.

Beispielsweise werden alle virtuellen Maschinen mit dem Sicherheitstag „Web“ automatisch zu einer bestimmten Sicherheitsgruppe hinzugefügt, die für Webserver vorgesehen ist. Nach dem Erstellen einer Sicherheitsgruppe wird eine Sicherheitsrichtlinie auf diese Gruppe angewendet.

Erstellen einer Sicherheitsgruppe

Sie können benutzerdefinierte Sicherheitsgruppen erstellen.

Voraussetzungen

Wenn Sie Sicherheits-Tags mit Sicherheitsgruppen verwenden möchten, nutzen Sie das Verfahren unter [Erstellen und Zuweisen von Sicherheitstags](#).

Verfahren

- 1 Öffnen Sie die Sicherheitsdienste.
 - a Navigieren Sie zu **Netzwerk > Sicherheit**.
 - b Wählen Sie das Organisations-VDC aus, auf das Sie Sicherheitseinstellungen anwenden möchten, und klicken Sie auf **Dienste konfigurieren**.

Das Mandantenportal öffnet die Sicherheitsdienste.

- 2 Navigieren Sie zu **Gruppierungsobjekte > Sicherheitsgruppen**.

Die Seite **Sicherheitsgruppen** wird geöffnet.

- 3 Klicken Sie auf die Schaltfläche **Erstellen** ().

- 4 Geben Sie einen Namen und optional eine Beschreibung für die Sicherheitsgruppe ein.

Die Beschreibung wird in der Liste der Sicherheitsgruppen angezeigt. Die Sicherheitsgruppe lässt sich also leichter auf einen Blick identifizieren, wenn Sie eine aussagekräftige Beschreibung hinzufügen.

5 (Optional) Fügen Sie eine dynamische Mitgliedergruppe hinzu.

- a Klicken Sie unter „Dynamische Mitgliedergruppen“ auf die Schaltfläche **Hinzufügen**



- b Wählen Sie **Beliebig** oder **Alle** aus, um die entsprechenden Kriterien in Ihrer Anweisung abzugleichen.
- c Geben Sie das erste Objekt ein, das abgeglichen werden soll.

Die Optionen sind **Sicherheitstag**, **Name des VM-Gastbetriebssystems**, **VM-Name** und **Name des VM-Gasthosts**.

- d Wählen Sie einen Operator aus, wie z. B. **Enthält**, **Beginnt mit** oder **Endet mit**.
- e Geben Sie einen Wert ein.
- f (Optional) Wenn Sie eine weitere Anweisung hinzufügen möchten, verwenden Sie den booleschen Operator **Und** oder **Oder**.

6 (Optional) Schließen Sie Mitglieder ein.

- a Wählen Sie im Dropdown-Menü **Objekte dieses Typs durchsuchen** den Typ der Objekte aus, beispielsweise **Virtuelle Maschinen**, **vDC-Organisationsnetzwerke**, **IP Sets**, **MAC Sets** oder **Sicherheitstags**.
- b Um ein Objekt in die Liste „Mitglieder einschließen“ aufzunehmen, wählen Sie es im linken Fensterbereich aus und verschieben es in den rechten Fensterbereich, indem Sie auf den Rechtspfeil klicken.

7 (Optional) Schließen Sie Mitglieder aus.

- a Wählen Sie im Dropdown-Menü **Objekte dieses Typs durchsuchen** den Typ der Objekte aus, beispielsweise **Virtuelle Maschinen**, **vDC-Organisationsnetzwerke**, **IP Sets**, **MAC Sets** oder **Sicherheitstags**.
- b Um ein Objekt in die Liste „Mitglieder ausschließen“ aufzunehmen, wählen Sie es im linken Fensterbereich aus und verschieben es in den rechten Fensterbereich, indem Sie auf den Rechtspfeil klicken.

8 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Ergebnisse

Die Sicherheitsgruppe kann jetzt in Regeln, z. B. in Firewallregeln, verwendet werden.

Bearbeiten einer Sicherheitsgruppe

Sie können benutzerdefinierte Sicherheitsgruppen bearbeiten.

Verfahren

1 Öffnen Sie die Sicherheitsdienste.

- a Navigieren Sie zu **Netzwerk > Sicherheit**.
- b Wählen Sie das Organisations-VDC aus, auf das Sie Sicherheitseinstellungen anwenden möchten, und klicken Sie auf **Dienste konfigurieren**.

Das Mandantenportal öffnet die Sicherheitsdienste.

2 Navigieren Sie zu **Gruppierungsobjekte > Sicherheitsgruppen**.


Die Seite **Sicherheitsgruppen** wird geöffnet.

3 Wählen Sie die Sicherheitsgruppe aus, die Sie bearbeiten möchten.

Die Details für die Sicherheitsgruppe werden unter der Liste der Sicherheitsgruppen angezeigt.

4 (Optional) Bearbeiten Sie den Namen und die Beschreibung der Sicherheitsgruppe.

5 (Optional) Fügen Sie eine dynamische Mitgliedergruppe hinzu.

- a Klicken Sie auf die Schaltfläche **Hinzufügen** () unter **Dynamische Mitgliedergruppen**.
- b Wählen Sie **Beliebig** oder **Alle** aus, um die entsprechenden Kriterien in Ihrer Anweisung abzugleichen.
- c Geben Sie das erste Objekt ein, das abgeglichen werden soll.
Die Optionen sind **Sicherheitstag**, **Name des VM-Gastbetriebssystems**, **VM-Name** und **Name des VM-Gasthosts**.
- d Wählen Sie einen Operator aus, wie z. B. **Enthält**, **Beginnt mit** oder **Endet mit**.
- e Geben Sie einen Wert ein.
- f (Optional) Wenn Sie eine weitere Anweisung hinzufügen möchten, verwenden Sie den booleschen Operator **Und** oder **Oder**.

6 (Optional) Bearbeiten Sie eine dynamische Mitgliedergruppe durch einen Klick auf das Symbol **Bearbeiten** () neben der Mitgliedergruppe, die Sie bearbeiten möchten.

- a Nehmen Sie die erforderlichen Änderungen für die dynamische Mitgliedergruppe vor.
- b Klicken Sie auf **OK**.

7 (Optional) Löschen Sie eine dynamische Mitgliedergruppe durch einen Klick auf das Symbol **Löschen** () neben der Mitgliedergruppe, die Sie löschen möchten.


- 8 (Optional) Bearbeiten Sie die Liste der eingeschlossenen Mitglieder durch einen Klick auf das Symbol **Bearbeiten** (⚙️) neben der Liste „Mitglieder einschließen“.
 - a Wählen Sie im Dropdown-Menü **Objekte dieses Typs durchsuchen** den Typ der Objekte aus, beispielsweise **Virtuelle Maschinen**, **vDC-Organisationsnetzwerke**, **IP Sets**, **MAC Sets** oder **Sicherheitstags**.
 - b Um ein Objekt in die Liste „Mitglieder einschließen“ aufzunehmen, wählen Sie es im linken Fensterbereich aus und verschieben es in den rechten Fensterbereich, indem Sie auf den Rechtspfeil klicken.
 - c Um ein Objekt aus der Liste eingeschlossener Mitglieder auszuschließen, wählen Sie das Objekt im rechten Bereich aus und verschieben Sie es mit einem Klick auf den Pfeil nach links in den linken Bereich.
- 9 (Optional) Bearbeiten Sie die Liste der ausgeschlossenen Mitglieder durch einen Klick auf das Symbol **Bearbeiten** (⚙️) neben der Liste „Mitglieder ausschließen“.
 - a Wählen Sie im Dropdown-Menü **Objekte dieses Typs durchsuchen** den Typ der Objekte aus, beispielsweise **Virtuelle Maschinen**, **vDC-Organisationsnetzwerke**, **IP Sets**, **MAC Sets** oder **Sicherheitstags**.
 - b Um ein Objekt in die Liste „Mitglieder ausschließen“ aufzunehmen, wählen Sie es im linken Fensterbereich aus und verschieben es in den rechten Fensterbereich, indem Sie auf den Rechtspfeil klicken.
 - c Um ein Objekt aus der Liste ausgeschlossener Mitglieder auszuschließen, wählen Sie das Objekt im rechten Bereich aus und verschieben Sie es mit einem Klick auf den Pfeil nach links in den linken Bereich.
- 10 Klicken Sie auf **Änderungen speichern**.
Die Änderungen an der Sicherheitsgruppe werden gespeichert.

Löschen einer Sicherheitsgruppe

Sie können eine benutzerdefinierte Sicherheitsgruppe löschen.

Verfahren

- 1 Öffnen Sie die Sicherheitsdienste.
 - a Navigieren Sie zu **Netzwerk > Sicherheit**.
 - b Wählen Sie das Organisations-VDC aus, auf das Sie Sicherheitseinstellungen anwenden möchten, und klicken Sie auf **Dienste konfigurieren**.
Das Mandantenportal öffnet die Sicherheitsdienste.
- 2 Navigieren Sie zu **Gruppierungsobjekte > Sicherheitsgruppen**.
Die Seite **Sicherheitsgruppen** wird geöffnet.
- 3 Wählen Sie die Sicherheitsgruppe aus, die Sie löschen möchten.

- 4 Klicken Sie auf die Schaltfläche **Löschen** ().
- 5 Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Ergebnisse

Die Sicherheitsgruppe wird gelöscht.

Verwendung unabhängiger Festplatten und Überprüfen von Speicherrichtlinien

7

Im vCloud Director-Mandantenportal können Sie unabhängige Festplatten erstellen und verwalten und die Speicherrichtlinien des Organisations-VDC überprüfen.

Dieses Kapitel enthält die folgenden Themen:

- Erstellen und Verwenden von unabhängigen Festplatten
- Überprüfen der Eigenschaften von Speicherrichtlinien

Erstellen und Verwenden von unabhängigen Festplatten

Unabhängige Festplatten sind eigenständige virtuelle Festplatten, die Sie in Organisations-VDCs erstellen. **Organisationsadministratoren** und -benutzer mit den entsprechenden Rechten können unabhängige Festplatten erstellen, entfernen und aktualisieren und mit virtuellen Maschinen verbinden.

Wenn Sie eine unabhängige Festplatte erstellen, wird diese mit einem Organisations-VDC, nicht aber mit einer virtuellen Maschine verknüpft. Nach dem Erstellen der Festplatte in einem VDC kann der Festplattenbesitzer oder ein Administrator die Festplatte unter Verwendung der vCloud-API an eine beliebige im VDC bereitgestellte virtuelle Maschine anhängen.

Der Festplattenbesitzer kann die Festplatteneigenschaften auch ändern, die Festplatte von einer virtuellen Maschine trennen und aus dem VDC entfernen. **Systemadministratoren** und **Organisationsadministratoren** haben die gleichen Rechte zum Verwenden und Ändern der Festplatte wie der Festplattenbesitzer.

Erstellen einer unabhängigen Festplatte

Sie können eine unabhängige Festplatte erstellen und sie zu einem späteren Zeitpunkt an eine virtuelle Maschine anhängen.

Zur Erstellung einer unabhängigen Festplatte müssen Sie deren Namen und Größe angeben. Sie können optional eine Beschreibung angeben und ein von der Festplatte zu verwendendes Speicherprofil festlegen.

Voraussetzungen

Sie müssen über eine Rolle als **Organisationsadministrator** oder die Rechte eines Festplattenbesitzers verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich unter **Speicher** die Option **Unabhängige Festplatten** aus.
- 2 Klicken Sie auf **Neu**.
- 3 Geben Sie einen Namen und optional eine Beschreibung der Festplatte ein.
- 4 Wählen Sie eine Speicherrichtlinie im Dropdown-Menü **Speicherrichtlinie** aus.
- 5 Geben Sie die Größe der unabhängigen Festplatte in Byte ein.
- 6 Wählen Sie in den Dropdown-Menüs **Bustyp** und **Bus-Subtyp** jeweils den Bustyp und den Bus-Subtyp aus und klicken Sie auf **Speichern**.

Nächste Schritte

Verwenden Sie die vCloud-API, um die unabhängige Festplatte an eine virtuelle Maschine anzuhängen. Siehe *vCloud API-Programmierhandbuch für Dienstleister* auf [VMware {code}](#).

Bearbeiten einer unabhängigen Festplatte

Nachdem Sie die Festplatte erstellt haben, können Sie deren Namen, Beschreibung, Speicherrichtlinie und Größe ändern.

Voraussetzungen

Sie müssen über eine Rolle als **Organisationsadministrator** oder die Rechte eines Festplattenbesitzers verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich unter **Speicher** die Option **Unabhängige Festplatten** aus.
- 2 Wählen Sie die zu ändernde Festplatte aus und klicken Sie auf **Bearbeiten**.
- 3 Bearbeiten Sie die Einstellungen, wie z. B. Name, Beschreibung, Speicherrichtlinie und Größe in Byte.
- 4 Klicken Sie auf **Speichern**.

Löschen einer unabhängigen Festplatte

Voraussetzungen

Sie müssen über eine Rolle als **Organisationsadministrator** oder die Rechte eines Festplattenbesitzers verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich unter **Speicher** die Option **Unabhängige Festplatten** aus.
- 2 Wählen Sie die zu löschende Festplatte aus und klicken Sie auf **Löschen**.
- 3 Klicken Sie auf **OK**.

Überprüfen der Eigenschaften von Speicherrichtlinien

Sie können die Speicherrichtlinien und die Details der Speicherrichtlinien überprüfen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie durchsuchen möchten.
- 2 Klicken Sie unter **Speicher** auf **Speicherrichtlinien**.
Die Liste der verfügbaren Speicherrichtlinien wird angezeigt.
- 3 Klicken Sie zum Anzeigen der Details einer Speicherrichtlinie auf den Namen der Speicherrichtlinie.
- 4 Überprüfen Sie die Details auf den Registerkarten **Allgemein** und **Metadaten** und klicken Sie auf **OK**.

Überprüfen der Eigenschaften von virtuellen Datencentern



Als **Organisationsadministrator** können Sie die Eigenschaften des virtuellen Datencenters überprüfen.

Dieses Kapitel enthält die folgenden Themen:

- Überprüfen der Eigenschaften von virtuellen Datencentern
- Überprüfen der Metadaten des virtuellen Datencenters

Überprüfen der Eigenschaften von virtuellen Datencentern

Sie können die Eigenschaften der virtuellen Datentcenter überprüfen, die Ihrer Organisation zugewiesen sind.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datentcenter** auf die Karte des virtuellen Datencenters, das Sie durchsuchen möchten.
- 2 Klicken Sie unter **Einstellungen** auf **Allgemein**.

Ergebnisse

Sie können die Eigenschaften des virtuellen Datencenters überprüfen, wie z. B. Name, Beschreibung und Status. Zu den Metrikinformationen für das Datentcenter gehören das Zuweisungsmodell und die vCPU sowie die CPU- und Speichernutzung.

Überprüfen der Metadaten des virtuellen Datencenters

vCloud Director bietet eine allgemeine Funktion, um benutzerdefinierte Metadaten einem Objekt zuzuordnen. Wenn der Systemadministrator Metadaten für das Organisations-VDC erstellt hat, können Sie die Metadaten des Organisations-Datencenters überprüfen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelle Datencenter** auf die Karte des virtuellen Datencenters, das Sie durchsuchen möchten.
- 2 Klicken Sie unter **Einstellungen** auf **Metadaten**.
Die Liste der verfügbaren Metadaten wird angezeigt.

Arbeiten mit SDDCs und SDDC-Proxys

9

Ab vCloud Director 9.7 können Sie auf eine vCenter Server-Umgebung über vCloud Director zugreifen. vCloud Director kann als HTTP-Proxy-Server fungieren und den Zugriff auf Komponenten aus der zugrundeliegenden vSphere-Umgebung ermöglichen.

In vCloud Director umfasst ein SDDC (Software-Defined Data Center) eine gesamte vCenter Server-Umgebung. Ein SDDC kann einen oder mehrere SDDC-Proxys enthalten, die Zugriff auf verschiedene Komponenten aus der zugrundeliegenden Umgebung bereitstellen. Der **Systemadministrator** kann ein oder mehrere SDDCs in Ihrer Organisation veröffentlichen. Sie können die enthaltenen SDDC-Proxys verwenden, um auf die Benutzeroberfläche oder API der Proxy-Komponenten zuzugreifen.

Dieses Kapitel enthält die folgenden Themen:

- Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen
- Aktivieren oder Deaktivieren eines SDDC-Proxys
- Anmelden bei der Benutzeroberfläche einer Proxy-SDDC-Komponente

Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen

Bevor Sie auf die Benutzeroberfläche einer vSphere-Proxy-Komponente zugreifen können, müssen Sie Ihren Browser zur Verwendung der SDDC-Proxys konfigurieren, die in Ihrer Organisation veröffentlicht werden.

Um Ihren Browser zur Verwendung der veröffentlichten SDDC-Proxys zu konfigurieren, laden Sie eine PAC-Datei herunter und importieren Sie sie.


Hinweis Sie müssen diesen Vorgang jedes Mal wiederholen, wenn der **Systemadministrator** ein SDDC für Ihre Organisation veröffentlicht oder dessen Veröffentlichung aufhebt und wenn der **Systemadministrator** einen Proxy zum SDDC hinzufügt oder daraus entfernt. Wenn Sie den Satz an SDDCs und SDDC-Proxys ändern, hat dies Auswirkungen auf die PAC-Datei.

Wenn bestimmte Proxy-Komponenten selbstsignierte Zertifikate verwenden, müssen Sie diese dem Browser hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass der **Systemadministrator** mindestens eine dedizierte und aktivierte vCenter Server-Instanz für Ihre Organisation veröffentlicht hat.
- Stellen Sie sicher, dass der **Systemadministrator** die Rechte **SDDC_VIEW** und **Token: Verwalten** für Ihre Organisation veröffentlicht hat und dass Ihre Rolle diese Rechte umfasst.
- Stellen Sie sicher, dass der **Systemadministrator** das Plug-In **CPOM-Erweiterung** für Ihre Organisation veröffentlicht und aktiviert hat. Dieses Plug-In enthält die Funktion zum Anzeigen und Verwenden von dedizierten vSphere-Datencentern im vCloud Director Tenant Portal.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter** aus.
- 2 Klicken Sie im Bereich **SDDCs** auf **Proxy-Konfiguration herunterladen (.PAC)**.
- 3 Konfigurieren Sie Ihren Browser zur Verwendung der heruntergeladenen PAC-Datei.
Weitere Informationen finden Sie im Benutzerhandbuch Ihres Browsers.
- 4 Klicken Sie auf der Karte des Ziel-SDDC auf **Standard-Proxy aktivieren**.
- 5 Wenn die Proxy-Standardkomponente selbstsignierte Zertifikate verwendet, fügen Sie die Zertifikate Ihrem Browser hinzu.
 - a Klicken Sie auf der Karte des Ziel-SDDC auf **Mehr** und dann auf **Proxy-Standardzertifikat herunterladen (.PEM)**.
 - b Importieren Sie das heruntergeladene PEM-Zertifikat in Ihren Browser.
Weitere Informationen finden Sie im Benutzerhandbuch Ihres Browsers.
- 6 Wenn eine nicht standardmäßige Proxy-Komponente selbstsignierte Zertifikate verwendet, fügen Sie die Zertifikate Ihrem Browser hinzu.
 - a Klicken Sie auf der Karte des Ziel-SDDC auf **Mehr** und dann auf **Proxys verwalten**.
 - b Wenn der Ziel-Proxy nicht aktiviert ist, wählen Sie das Optionsfeld neben dem Namen des Proxys aus und klicken Sie auf **Aktivieren**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des Ziel-Proxys und anschließend auf **Zertifikat herunterladen (.PEM)**.
 - d Importieren Sie das heruntergeladene PEM-Zertifikat in Ihren Browser.
Weitere Informationen finden Sie im Benutzerhandbuch Ihres Browsers.

Aktivieren oder Deaktivieren eines SDDC-Proxys

Um ein Token für den Zugriff auf eine Proxy-SDDC-Komponente zu generieren, müssen Sie diesen Proxy aktivieren. Ein Proxy wird für die aktuelle Benutzersitzung aktiviert. Wenn Sie einen Proxy

deaktivieren oder wenn die Benutzersitzung abgelaufen ist, ist der Proxy nicht mehr aktiv und das Token funktioniert nicht mehr.

Hinweis Möglicherweise bestehen Einschränkungen bei der Anzahl der gleichzeitig aktiven Proxys. Weitere Informationen erhalten Sie von Ihrem **Systemadministrator**.

Voraussetzungen

Wenn Sie einen Proxy aktivieren möchten, stellen Sie sicher, dass der **Systemadministrator** diesen Proxy aktiviert hat.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter** aus.
- 2 Aktivieren Sie einen Proxy.
 - Um den Standard-Proxy zu aktivieren, klicken Sie auf der Karte des gewünschten SDDC auf **Standard-Proxy aktivieren**.
 - Um einen anderen als den Standard-Proxy zu aktivieren, führen Sie die folgenden Schritte aus:
 - a Klicken Sie auf der Karte des gewünschten SDDC auf **Mehr** und klicken Sie auf **Proxys verwalten**.
 - b Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Proxys und dann auf **Aktivieren**.
- 3 Deaktivieren Sie einen Proxy.
 - Um den Standard-Proxy zu deaktivieren, klicken Sie auf der Karte des gewünschten SDDC auf **Mehr** und dann auf **Standard-Proxy deaktivieren**.
 - So aktivieren Sie einen anderen als den Standard-Proxy:
 - a Klicken Sie auf der Karte des gewünschten SDDC auf **Mehr** und klicken Sie auf **Proxys verwalten**.
 - b Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Proxys und dann auf **Deaktivieren**.

Ergebnisse

Wenn Sie einen Proxy aktiviert haben, finden Sie weitere Informationen unter [Anmelden bei der Benutzeroberfläche einer Proxy-SDDC-Komponente](#).


Anmelden bei der Benutzeroberfläche einer Proxy-SDDC-Komponente

Sie können mit Ihrem vCloud Director-Konto auf die Benutzeroberfläche einer Proxy-SDDC-Komponente zugreifen.

Voraussetzungen

- Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen
- Aktivieren Sie den Ziel-Proxy. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren eines SDDC-Proxys](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Datencenter** aus.
- 2 Öffnen Sie den Proxy.
 - Um den Standard-Proxy zu öffnen, klicken Sie auf **Zugriffstoken kopieren und öffnen**.
 - Um einen nicht standardmäßigen Proxy zu öffnen, führen Sie die folgenden Schritte aus:
 - Klicken Sie auf der Karte des gewünschten SDDC auf **Mehr** und klicken Sie auf **Proxys verwalten**.
 - Klicken Sie auf das Optionsfeld neben dem gewünschten Proxy und dann auf **Zugriffstoken kopieren und öffnen**.

Das Zugriffstoken wird in die Zwischenablage kopiert. Eine neue Registerkarte wird geöffnet und fordert Sie zur Authentifizierung anhand des Proxys auf.

- 3 Geben Sie im Textfeld **Benutzername** Ihren vCloud Director-Benutzernamen und den Namen Ihrer Organisation ein, indem Sie das Format *vCD_user_name@organization_name* verwenden.

Beispiel: **johndoe@orgOne**.

- 4 Fügen Sie im Textfeld **Kennwort** das kopierte Zugriffstoken ein.
- 5 Klicken Sie auf **OK**.

Ergebnisse

Die Benutzeroberfläche der Proxy-Komponente wird geöffnet.

Arbeiten mit vApp-Vorlagen

10

Eine vApp-Vorlage ist ein Image einer virtuellen Maschine, das mit einem Betriebssystem, Anwendungen und Daten geladen wird. Diese Vorlagen stellen sicher, dass virtuelle Maschinen organisationsweit einheitlich konfiguriert sind. vApp-Vorlagen werden zu Katalogen hinzugefügt.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen einer vApp-Vorlage](#)
- [vApp-Vorlage aus einer OVF-Datei erstellen](#)
- [vApp-Vorlage herunterladen](#)
- [Löschen einer vApp-Vorlage](#)

Anzeigen einer vApp-Vorlage

Sie können die Liste der vApp-Vorlagen anzeigen, die in den Katalogen verfügbar sind, auf die Sie zugreifen können. Sie können eine vApp-Vorlage anzeigen und die darin enthaltenen virtuellen Maschinen überprüfen.

Sie können nur auf die vApp-Vorlagen zugreifen, die in den für Sie freigegebenen Katalogelementen enthalten sind. Weitere Informationen zur Freigabe von Katalogen finden Sie unter [Freigabe eines Katalogs](#).


Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **vApp-Vorlagen** aus.

Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.

- 2 (Optional) Konfigurieren Sie die Rasteransicht so, dass sie die gewünschten Elemente enthält.
 - a Klicken Sie in der Rasteransicht auf das Symbol des Rastereditors (), das unterhalb der Liste mit vApp-Vorlagen angezeigt wird.
 - b Wählen Sie die Elemente aus, die Sie in die Rasteransicht aufnehmen möchten, wie z. B. Version, Status, Katalog, Besitzer usw.
 - c Klicken Sie auf **OK**.

Das Raster zeigt die Elemente an, die Sie für jede vApp-Vorlage in der Liste ausgewählt haben.
- 3 Zur Anzeige der in einer vApp-Vorlage enthaltenen virtuellen Maschinen klicken Sie auf den Namen der vApp-Vorlage.

Die virtuellen Maschinen, die die vApp-Vorlage enthält, werden in einem Raster angezeigt.
- 4 (Optional) Zur Auswahl der in der Rasteransicht anzuzeigenden Elemente klicken Sie auf das Symbol des Rastereditors () unterhalb der Liste der virtuellen Maschinen.
 - a Wählen Sie die Elemente aus, die Sie in die Rasteransicht aufnehmen möchten.
 - b Klicken Sie auf **OK**.

vApp-Vorlage aus einer OVF-Datei erstellen


Sie können ein OVF-Paket zum Erstellen einer vApp-Vorlage in einem Katalog hochladen.

vCloud Director unterstützt folgende Spezifikationen: Open Virtualization Format (OVF) und Open Virtualization Appliance (OVA). Wenn Sie eine OVF-Datei hochladen, die OVF-Eigenschaften zur Anpassung ihrer virtuellen Maschinen einschließt, werden diese Eigenschaften in der vApp-Vorlage beibehalten. Weitere Informationen zum Erstellen von OVF-Paketen finden Sie im *OVF Tool User Guide* und im *VMware vCenter Converter User's Guide*.


Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **vApp-Vorlagen** aus.

Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf **Hinzufügen**.

- 3 Geben Sie eine URL-Adresse für die OVF-Datei ein oder klicken Sie auf das Symbol **Hochladen** () , um zu einem Speicherort zu navigieren, auf den Sie über Ihren Computer zugreifen können, und wählen Sie die OVF/OVA-Vorlagendatei aus.

Der Speicherort kann Ihre lokale Festplatte, eine Netzwerkfreigabe oder ein CD/DVD-Laufwerk sein. Zu den unterstützten Dateierweiterungen gehören .ova, .ovf, .vmdk, .mf, .cert und .strings. Wenn Sie eine OVF-Datei hochladen möchten, die mehr Dateien referenziert, als Sie hochladen möchten (z. B. eine VMDK-Datei), müssen Sie alle Dateien durchsuchen und auswählen.
- 4 Überprüfen Sie die Details der OVF/OVA-Vorlage, die Sie bereitstellen möchten, und klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für die vApp-Vorlage ein und klicken Sie auf **Weiter**.
- 6 Wählen Sie im Dropdown-Menü **Katalog** den Katalog aus, zu dem Sie die Vorlage hinzufügen möchten.
- 7 Überprüfen Sie die Einstellungen der vApp-Vorlage und klicken Sie auf **Fertigstellen**.

Ergebnisse

Die neue vApp-Vorlage wird in der Vorlagen-Rasteransicht angezeigt.


vApp-Vorlage herunterladen


Sie können eine vApp-Vorlage aus einem Katalog als OVA-Datei auf Ihrem lokalen Computer herunterladen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **vApp-Vorlagen** aus.

Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf die Listenleiste () links neben der herunterzuladenden vApp-Vorlage und wählen Sie **Herunterladen** aus.

Hinweis Sie können vApp-Vorlagen aus den Katalogen Ihrer Organisation herunterladen. Als Organisationsadministrator können Sie vApp-Vorlagen aus einem öffentlichen Katalog herunterladen. Ansonsten wird die Schaltfläche **Herunterladen** abgeblendet dargestellt.

- 3 (Optional) Aktivieren Sie zur Beibehaltung der UUIDs und MAC-Adressen der virtuellen Maschinen im heruntergeladenen OVA-Paket das Kontrollkästchen **Identitätsinformationen beibehalten**.

- 4 Klicken Sie auf **OK** und warten Sie, bis der Download abgeschlossen ist.

Die OVA-Datei wird im Standardverzeichnis für Downloads des Webbrowsers gespeichert.

Löschen einer vApp-Vorlage

Sie können eine vApp-Vorlage aus einem Organisationskatalog löschen. Wenn der Katalog veröffentlicht ist, wird die vApp-Vorlage auch aus den öffentlichen Katalogen entfernt.


Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **vApp-Autor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **vApp-Vorlagen** aus.

Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf die Listenleiste () links neben der zu löschenden vApp-Vorlage und wählen Sie **Löschen** aus.

- 3 Bestätigen Sie den Löschvorgang.

Die gelöschte vApp-Vorlage wird aus der Rasteransicht entfernt.

Über den Katalog können Sie Mediendateien hochladen, kopieren, verschieben und Eigenschaften von Mediendateien bearbeiten.

Dieses Kapitel enthält die folgenden Themen:

- [Hochladen von Mediendateien](#)
- [Löschen einer Mediendatei](#)
- [Herunterladen einer Mediendatei](#)



Hochladen von Mediendateien

Sie können neue Mediendateien oder neue Versionen der vorhandenen Mediendateien in einen Katalog hochladen. Benutzer mit Zugriff auf den Katalog können die Mediendateien mit ihren virtuellen Maschinen öffnen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Medien und andere** aus.
Die Liste der Mediendateien wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Wählen Sie im Dropdown-Menü **Katalog** einen Katalog aus, in den die Mediendatei hochgeladen werden soll.
- 4 Geben Sie einen Namen für die Mediendatei ein.
Wenn Sie keinen Namen eingeben, wird das Namenstextfeld automatisch mit dem Namen der Mediendatei befüllt.
- 5 Klicken Sie auf das Symbol zum Hochladen () , um nach der Festplattenimagedatei zu suchen und diese auszuwählen, z. B. eine Datei mit der Erweiterung `.iso`.

6 Klicken Sie auf **OK**.

Nach dem Start des Uploads wird die Mediendatei in der Rasteransicht angezeigt.

Nächste Schritte

Je nach Dateigröße kann der Upload einige Zeit in Anspruch nehmen. Sie können in der Ansicht **Kürzlich bearbeitete Aufgaben** den Uploadstatus überwachen. Weitere Informationen finden Sie unter [Anzeigen von Aufgaben](#).



Löschen einer Mediendatei

Sie können Mediendateien, die Sie nicht mehr verwenden möchten, aus dem Katalog löschen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Medien und andere** aus.
Die Liste der Mediendateien wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf die Listenleiste () links neben der zu löschenden Mediendatei und wählen Sie **Löschen** aus.
- 3 Bestätigen Sie den Löschvorgang.
Die gelöschte Mediendatei wird aus der Rasteransicht entfernt.


Herunterladen einer Mediendatei


Sie können eine Mediendatei aus einem Katalog herunterladen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Medien und andere** aus.
Die Liste der Mediendateien wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf die Listenleiste () links neben der herunterzuladenden Mediendatei und wählen Sie **Herunterladen** aus.

Der Download wird gestartet, und die Datei wird im Standardverzeichnis für Downloads des Webbrowsers gespeichert.

Nächste Schritte

Je nach Dateigröße kann der Download einige Zeit in Anspruch nehmen. Im Bereich **Kürzlich bearbeitete Aufgaben** können Sie den Downloadstatus überwachen. Weitere Informationen finden Sie unter [Anzeigen von Aufgaben](#).

Ein Katalog ist ein "Container" für vApp-Vorlagen und Mediendateien in einer Organisation. Administratoren der Organisation und Katalogautoren können Kataloge in einer Organisation erstellen. Die Kataloginhalte können für andere Benutzer oder Organisationen in der vCloud Director-Installation freigegeben oder extern veröffentlicht werden, um den Zugriff für Organisationen außerhalb der vCloud Director-Installation zu ermöglichen.

vCloud Director enthält private Kataloge, gemeinsam genutzte Kataloge und extern zugängliche Kataloge. Private Kataloge enthalten vApp-Vorlagen und Mediendateien, die Sie mit anderen Benutzern der Organisation gemeinsam nutzen können. Wenn ein Systemadministrator das Freigeben von Katalogen für Ihre Organisation aktiviert, können Sie einen Organisationskatalog freigeben, um einen Katalog zu erstellen, auf den andere Organisationen in der vCloud Director-Installation zugreifen können. Wenn ein Systemadministrator das externe Veröffentlichen von Katalogen für Ihre Organisation aktiviert, können Sie einen Organisationskatalog veröffentlichen, auf den Organisationen außerhalb der vCloud Director-Installation zugreifen können. Eine Organisation außerhalb der vCloud Director-Installation muss einen extern veröffentlichten Katalog abonnieren, um auf dessen Inhalte zugreifen zu können.

Sie können ein OVF-Paket direkt in einen Katalog hochladen, eine vApp als eine vApp-Vorlage speichern oder eine vApp-Vorlage aus vSphere importieren. Weitere Informationen erhalten Sie unter [vApp-Vorlage aus einer OVF-Datei erstellen](#) und [Speichern einer vApp als vApp-Vorlage in einem Katalog](#).

Mitglieder einer Organisation können auf vApp-Vorlagen und Mediendateien zugreifen, die ihnen gehören oder die mit ihnen gemeinsam genutzt werden. Organisationsadministratoren und Systemadministratoren können einen Katalog mit jedem in der Organisation oder mit spezifischen Benutzern oder Gruppen der Organisation gemeinsam nutzen. Weitere Informationen finden Sie unter [Freigeben eines Katalogs](#).

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen von Katalogen](#)
- [Erstellen eines Katalogs](#)
- [Freigeben eines Katalogs](#)
- [Löschen eines Katalogs](#)
- [Verwalten von Metadaten für einen Katalog](#)



- [Veröffentlichen eines Katalogs](#)
- [Abonnieren eines externen Katalogs](#)
- [Aktualisieren der Speicherort-URL und des Kennworts für einen abonnierten Katalog](#)
- [Synchronisieren eines abonnierten Katalogs](#)

Anzeigen von Katalogen


Sie können auf für Sie freigegebene Kataloge innerhalb Ihrer Organisation zugreifen. Sie können auf öffentliche Kataloge zugreifen, wenn ein Organisationsadministrator Zugriff auf diese Kataloge innerhalb Ihrer Organisation erteilt hat.

Der Katalogzugriff wird durch die Freigabe von Katalogen gesteuert, nicht durch die Rechte Ihrer Rolle. Sie können nur auf die Kataloge oder Katalogelemente zugreifen, die für Sie freigegeben sind. Weitere Informationen finden Sie unter [Freigeben eines Katalogs](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.
Die Liste der Kataloge wird in einer Rasteransicht angezeigt.
- 2 (Optional) Konfigurieren Sie die Rasteransicht so, dass sie die gewünschten Elemente enthält.
 - a Klicken Sie in der Rasteransicht auf das Symbol des Rastereditors () , das unterhalb der Katalogliste angezeigt wird.
 - b Wählen Sie die Elemente aus, die Sie in die Rasteransicht aufnehmen möchten, wie z. B. Version, Beschreibung, Status usw.
 - c Klicken Sie auf **OK**.

Im Raster werden die Elemente angezeigt, die Sie für jeden Katalog ausgewählt haben.

- 3 (Optional) Zeigen Sie in der Rasteransicht über die Listenleiste () die Aktionen an, die für die einzelnen Kataloge ausgeführt werden können.
Sie können einen Katalog z. B. freigeben oder löschen.


Erstellen eines Katalogs

Sie können neue Kataloge erstellen und mit einer Speicherrichtlinie verknüpfen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.
Die Liste der Kataloge wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf **Neu**, um einen neuen Katalog zu erstellen.
- 3 Geben Sie den Namen und optional eine Beschreibung des Katalogs ein.
- 4 (Optional) Geben Sie an, ob Sie dem Katalog eine Speicherrichtlinie zuweisen möchten, und wählen Sie eine Speicherrichtlinie aus.
- 5 Klicken Sie auf **OK**.

Ergebnisse

Der neue Katalog wird in der Rasteransicht auf der Registerkarte **Kataloge** angezeigt.



Freigeben eines Katalogs

Sie können einen Katalog gemeinsam mit allen Mitgliedern Ihrer Organisation oder mit bestimmten Mitgliedern nutzen.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.
- Sie müssen der Besitzer des Katalogs sein.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.
Die Liste der Kataloge wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf die Listenleiste () links neben dem freizugebenden Katalog und wählen Sie **Freigeben** aus.
Die Liste der Benutzer, die auf den Katalog zugreifen können, wird in der Rasteransicht des Dialogfelds **Katalog gemeinsam nutzen** angezeigt.
- 3 Klicken Sie auf **Hinzufügen**, um den Katalog mit anderen Benutzern gemeinsam zu nutzen.

Option	Beschreibung
Mit allen in dieser Organisation gemeinsam nutzen	Gewähren Sie allen Benutzern und Gruppen in der Organisation Zugriff.
Mit bestimmten Benutzern oder Gruppen gemeinsam nutzen	Wählen Sie die Benutzer oder Gruppen aus, denen Zugriff gewährt werden soll, und klicken Sie auf Hinzufügen .

4 Wählen Sie die Zugriffsebene aus.

Option	Beschreibung
Schreibgeschützt	Benutzer mit Zugriff auf diesen Katalog verfügen über Lesezugriff auf die vApp-Vorlagen und ISO-Dateien des Katalogs.
Lesen/Schreiben	Benutzer mit Zugriff auf diesen Katalog verfügen über Lesezugriff auf die vApp-Vorlagen und ISO-Dateien des Katalogs und können vApp-Vorlagen und ISO-Dateien zum Katalog hinzufügen.
Vollständige Kontrolle	Benutzer mit Zugriff auf diesen Katalog verfügen über Vollzugriff auf die Inhalte und Einstellungen des Katalogs.

5 Klicken Sie auf **OK**.

Die Benutzer oder Gruppen, die nun auf den Katalog zugreifen können, werden in der Rasteransicht des Dialogfelds **Katalog gemeinsam nutzen** angezeigt.

6 (Optional) Wählen Sie diese Option aus, um schreibgeschützten Zugriff für die Administratoren aller anderen Organisationen freizugeben

7 Klicken Sie auf **Speichern**.

Ergebnisse

Auf der Registerkarte **Kataloge** ändert sich der Status für die gemeinsame Nutzung für diesen Katalog in der Rasteransicht.

Löschen eines Katalogs

Sie können einen Katalog aus der Organisation löschen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Katalogautor** enthaltenen Rechte oder entsprechende Rechte.

Hinweis Der Katalog darf keine vApp-Vorlagen oder Mediendateien enthalten. Sie können diese Objekte in einen anderen Katalog verschieben oder löschen.

Verfahren

1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.

Die Liste der Kataloge wird in einer Rasteransicht angezeigt.

2 Klicken Sie auf die Listenleiste () links neben dem zu löschenden Katalog und wählen Sie **Löschen** aus.


3 Bestätigen Sie den Löschvorgang.

Das gelöschte Katalogelement wird aus der Rasteransicht entfernt.

Verwalten von Metadaten für einen Katalog

Als **Organisationsadministrator** oder **Katalogbesitzer** können Sie die Metadaten für die Kataloge, die Sie besitzen, erstellen oder aktualisieren.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.
Die Liste der Kataloge wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf die Listenleiste () links neben einem Katalog und wählen Sie **Metadaten** aus.
Die Metadaten für den ausgewählten Katalog werden in einer Rasteransicht angezeigt.
- 3 (Optional) Klicken Sie auf **Hinzufügen**, um Metadaten hinzuzufügen.
 - a Geben Sie den Metadatennamen ein.
Der Name muss innerhalb der Metadatenamen, die mit diesem Objekt verknüpft sind, eindeutig sein.
 - b Wählen Sie den Metadatentyp aus, wie z. B. **Text**, **Zahl**, **Datum und Uhrzeit** oder **Ja oder Nein**.
 - c Geben Sie den Metadatenwert ein.
 - d Klicken Sie auf **Speichern**.
- 4 (Optional) Aktualisieren Sie vorhandene Metadaten.
Sie können den Metadatenamen nicht aktualisieren.
 - a Aktualisieren Sie den Metadatentyp.
 - b Geben Sie den neuen Metadatenwert ein.
 - c Klicken Sie auf **Speichern**.
- 5 (Optional) Löschen Sie vorhandene Metadaten.
 - a Klicken Sie auf das Symbol zum Löschen.
 - b Klicken Sie auf **Speichern**.

Veröffentlichen eines Katalogs

Wenn Ihnen der **Systemadministrator** Katalogzugriff gewährt hat, können Sie einen Katalog extern veröffentlichen, damit Organisationen außerhalb der vCloud Director-Installation dessen vApp-Vorlagen und Mediendateien abonnieren können.


Voraussetzungen

Stellen Sie sicher, dass der **Systemadministrator** das externe Veröffentlichen von Katalogen für die Organisation aktiviert und Ihnen den Katalogzugriff gewährt hat.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.

Die Liste der Kataloge wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf die Listenleiste () links neben dem zu veröffentlichenden Katalog und wählen Sie **Einstellungen veröffentlichen** aus.

- 3 Wählen Sie **Veröffentlichung aktivieren** aus und geben Sie optional ein Kennwort für den Zugriff auf den Katalog ein.

Nur ASCII-Zeichen werden unterstützt.

- 4 Klicken Sie auf **Speichern**.

Abonnieren eines externen Katalogs

Sie können einen externen Katalog abonnieren und so eine schreibgeschützte Kopie eines extern veröffentlichten Katalogs erstellen. Sie können einen abonnierten Katalog nicht ändern.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Der **Systemadministrator** muss Ihrer Organisation die Berechtigung zum Abonnieren externer Kataloge erteilen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.

Die Liste der Kataloge wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf **Neu**, um einen neuen Katalog zu erstellen.
- 3 Geben Sie den Namen und optional eine Beschreibung des Katalogs ein.
- 4 Abonnieren Sie einen externen Katalog und geben Sie die Abonnement-URL ein.
- 5 Geben Sie ein optionales Kennwort für den Zugriff auf den Katalog ein.
- 6 Geben Sie an, ob der Inhalt automatisch aus dem externen Katalog heruntergeladen werden soll.
- 7 Klicken Sie auf **OK**.



Aktualisieren der Speicherort-URL und des Kennworts für einen abonnierten Katalog

Nach der Erstellung eines abonnierten Katalogs können Sie die Speicher-URL und das Kennwort für den abonnierten Katalog aktualisieren.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Sie müssen einen abonnierten Katalog erstellt haben.
- Der **Systemadministrator** muss Ihrer Organisation die Berechtigung zum Abonnieren externer Kataloge erteilen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.
Die Liste der Kataloge wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf die Listenleiste () links neben einem abonnierten Katalog und wählen Sie **Einstellungen für das Abonnieren** aus.
Wenn der Katalog nicht abonniert ist, wird die Option abgeblendet dargestellt.
- 3 Aktualisieren Sie die URL des Speicherorts und das Kennwort für diesen abonnierten Katalog.
- 4 Geben Sie an, ob der Inhalt automatisch aus dem externen Katalog heruntergeladen werden soll.
- 5 Klicken Sie auf **Speichern**.

Synchronisieren eines abonnierten Katalogs

Nach der Erstellung eines abonnierten Katalogs können Sie ihn mit dem ursprünglichen Katalog synchronisieren, um mögliche Änderungen anzuzeigen. Wenn die Metadaten des ursprünglichen Katalogs beispielsweise geändert werden und Sie eine Synchronisierung durchführen, werden die Metadaten des abonnierten Katalogs aktualisiert.


Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Sie müssen einen abonnierten Katalog erstellt haben.
- Der **Systemadministrator** muss Ihrer Organisation die Berechtigung zum Abonnieren externer Kataloge erteilen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **Kataloge** aus.

Die Liste der Kataloge wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf die Listenleiste () links neben einem abonnierten Katalog und wählen Sie **Synchronisieren** aus.

Wenn der Katalog nicht abonniert ist, wird die Option abgeblendet dargestellt.

Der abonnierte Katalog wird mit dem ursprünglichen Katalog synchronisiert.

Arbeiten mit VDC-Organisationsvorlagen

13

Als Organisationsadministrator oder in einer anderen Rolle mit Rechten zum Anzeigen und Instanzieren von Vorlagen für Organisations-VDCs können Sie zusätzliche Organisations-VDCs erstellen.

Eine Vorlage für Organisations-VDCs gibt eine Konfiguration für ein Organisations-VDC sowie optional ein Edge-Gateway und ein Netzwerk für das Organisations-VDC an. Systemadministratoren können Organisationsadministratoren zum Erstellen dieser Ressourcen in ihrer Organisation berechtigen, indem sie Vorlagen für Organisations-VDCs erstellen und sie an diese Organisationen freigeben.

Durch das Erstellen und Freigeben von Vorlagen virtueller Datacenter aktivieren Systemadministratoren die Self-Service-Bereitstellung von Organisations-VDCs und behalten gleichzeitig die Verwaltungskontrolle über die Zuteilung von Systemressourcen wie virtuellen Provider-Datacentern und externen Netzwerken bei.

Systemadministratoren erstellen Vorlagen für Organisations-VDCs und ermöglichen verschiedenen Organisationen den Zugriff auf die Vorlagen über die vCloud Director Webbenutzerschnittstelle. Informationen hierzu finden Sie unter *Verwalten von Vorlagen für Organisations-VDCs* im *vCloud Director Administratorhandbuch*. Wenn Ihrer Organisation der Zugriff auf Vorlagen für virtuelle Datacenter bereitgestellt wurde, können Sie über das vCloud Director-Mandantenportal anhand der verfügbaren Vorlagen virtuelle Datacenter erstellen.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen verfügbarer Vorlagen für virtuelle Datacenter](#)
- [Erstellen eines virtuellen Datacenters aus einer Vorlage](#)

Anzeigen verfügbarer Vorlagen für virtuelle Datacenter

Sie können die Vorlagen für Organisations-VDCs anzeigen, die ein Systemadministrator für Sie erstellt hat.

Sehen Sie sich die Vorlagen virtueller Datacenter an, bevor Sie ein neues Organisations-VDC anhand der Vorlage virtueller Datacenter erstellen.

Voraussetzungen

Für diesen Vorgang sind die Rechte erforderlich, die in der vordefinierten **Organisationsadministrator**-Rolle oder einer Rolle mit Rechten zum Anzeigen und Instanzieren von Vorlagen für Organisations-VDCs enthaltenen sind.

Verfahren

- ◆ Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **VDC-Vorlagen** aus.

Die Liste der Vorlagen für virtuelle Datacenter wird in einer Rasteransicht angezeigt.

Nächste Schritte

Überprüfen Sie die Beschreibungen der Vorlagen für Organisations-VDCs und wählen Sie die Vorlage aus, mit der Sie ein neues Organisations-VDC erstellen möchten.

Erstellen eines virtuellen Datacenters aus einer Vorlage

Sie können ein Organisations-VDC von einer Vorlage für virtuelle Datacenter erstellen, die Ihr Systemadministrator erstellt hat.

Voraussetzungen

Für diesen Vorgang sind die Rechte erforderlich, die in der vordefinierten **Organisationsadministrator**-Rolle oder einer Rolle mit Rechten zum Anzeigen und Instanzieren von Vorlagen für Organisations-VDCs enthaltenen sind.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und im linken Bereich die Option **VDC-Vorlagen** aus.

Die Liste der Vorlagen für virtuelle Datacenter wird in einer Rasteransicht angezeigt.

- 2 Wählen Sie eine Vorlage aus und klicken Sie auf **Neues VDC**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für das virtuelle Datacenter ein.
- 4 Klicken Sie auf **Erstellen**.

Ergebnisse

Die Erstellung des neuen Organisations-VDC wird instanziiert. Dieser Vorgang kann einige Minuten dauern. Sie können den Fortschritt der Aufgabe im Bereich **Kürzlich bearbeitete Aufgaben** anzeigen.

Nächste Schritte

Sie können Ihr neu erstelltes Organisations-VDC verwalten: durch das Erstellen virtueller Maschinen oder vApps, die Verwaltung der Netzwerk- und Sicherheitseinstellungen usw.

Verwalten von Benutzern, Gruppen und Rollen

14

Sie können Organisationsadministratoren einzeln oder als Teil einer LDAP-Gruppe zu vCloud Director hinzufügen. Sie können auch Rollen hinzufügen und bearbeiten, über die die Berechtigungen der Benutzer in ihrer Organisation festgelegt werden.

Wichtig Sie müssen **Organisationsadministrator** sein, um die Benutzer, Gruppen und Rollen in Ihrer Organisation verwalten zu können. Ihr **Systemadministrator** kann eine oder mehrere globale Mandantenrollen für Ihren Mandanten veröffentlichen, und als **Organisationsadministrator** können Sie diese in der Liste der Rollen sehen. Beispielsweise kann es sich um folgende Rollen handeln: **Katalogautor**, **vApp-Autor**, **vApp-Benutzer**, **Organisationsadministrator** usw. Die vordefinierten globalen Mandantenrollen können Sie nicht ändern, aber Sie können ähnliche benutzerdefinierte Mandantenrollen erstellen und aktualisieren und diese Benutzern in Ihrem Mandanten zuweisen.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von Benutzern](#)
- [Verwalten von Gruppen](#)
- [Rollen und Rechte](#)

Verwalten von Benutzern

Über das Mandantenportal können Sie Benutzer erstellen, bearbeiten, importieren und löschen. Darüber hinaus können Sie auch Benutzerkonten entsperren, falls ein Benutzer versucht hat, sich mit einem falschen Kennwort anzumelden und deshalb sein eigenes Benutzerkonto gesperrt wurde.


Erstellen eines Benutzers

Sie können einen Benutzer innerhalb Ihrer vCloud Director-Organisation erstellen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
Die Liste der Benutzer wird angezeigt.
- 3 Klicken Sie auf **Erstellen**.
- 4 (Optional) Geben Sie einen Benutzernamen und die Kennworteinstellung des Benutzers ein.
Die minimale Kennwortlänge beträgt sechs Zeichen.
- 5 Wählen Sie aus, ob der Benutzer bei der Erstellung aktiviert werden soll.
- 6 Wählen Sie die Rolle aus, die Sie dem Benutzer zuweisen möchten.

Das Menü **Verfügbare Rollen** besteht aus einer Liste vordefinierter Rollen und aller benutzerdefinierten Rollen, die Sie oder der Systemadministrator erstellt haben.

Vordefinierte Rolle	Beschreibung
vApp-Autor	Die mit der vordefinierten Rolle vApp-Autor verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu verwenden und vApps zu erstellen.
Nur Konsolenzugriff	Die mit den vordefinierten Rolle Nur Konsolenzugriff verknüpften Rechte ermöglichen es einem Benutzer, den Status und die Eigenschaften von virtuellen Maschinen anzuzeigen und das Gastbetriebssystem zu verwenden.
vApp-Benutzer	Die mit der vordefinierten Rolle vApp-Benutzer verknüpften Rechte ermöglichen es einem Benutzer, vorhandene vApps zu verwenden.
Organisationsadministrator	Ein Benutzer mit der vordefinierten Rolle Organisationsadministrator kann das vCloud Director-Mandantenportal oder die vCloud-API verwenden, um Benutzer und Gruppen in seiner Organisation zu verwalten und ihnen Rollen zuzuweisen, einschließlich der vordefinierten Rolle Organisationsadministrator . Ein Organisationsadministrator kann die vCloud-API zum Erstellen oder Aktualisieren der für die Organisation lokalen Rollenobjekte verwenden. Von einem Organisationsadministrator erstellte oder geänderte Rollen sind für andere Organisationen nicht sichtbar.
Nach Identitätsanbieter verschieben	Die mit der vordefinierten Rolle Auf Identitätsanbieter zurückstellen verknüpften Rechte werden basierend auf vom OAuth- oder SAML-Identitätsanbieter empfangenen Informationen festgelegt. Um sich für die Aufnahme zu qualifizieren, wenn einem Benutzer die Rolle Auf Identitätsanbieter zurückstellen zugewiesen ist, muss ein vom Identitätsanbieter bereitgestellter Rollename eine exakte Übereinstimmung (unter Berücksichtigung von Groß-/Kleinschreibung) mit einem innerhalb Ihrer Organisation definierten Rollennamen sein.
Katalogautor	Die mit der vordefinierten Rolle Katalogautor verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu erstellen und zu veröffentlichen.

- 7 (Optional) Geben Sie die Kontaktinformationen wie Name, E-Mail-Adresse, Telefonnummer und Instant Messaging-ID ein.

- 8 (Optional) Geben Sie das Kontingent für virtuelle Maschinen für den Benutzer ein.

Das Kontingent legt fest, wie viele virtuelle Maschinen und laufende virtuelle Maschinen der Benutzer verwalten kann. Wählen Sie **Unbegrenzt**, wenn Sie dem Benutzer eine unbegrenzte Anzahl von virtuellen Maschinen zur Verfügung stellen möchten.

- 9 Klicken Sie auf **Speichern**.


Benutzer importieren

Sie können Benutzer Ihren Organisationen hinzufügen, indem Sie einen LDAP-Benutzer oder einen SAML-Benutzer importieren und ihm eine bestimmte Rolle zuweisen.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Vergewissern Sie sich, dass Sie über eine gültige Verbindung zu einem LDAP-Server verfügen oder dass Sie [Kapitel 15 Aktivieren der Verwendung eines SAML-Identitätsanbieters für die Organisation](#). Weitere Informationen finden Sie unter *vCloud Director-Administratorhandbuch*.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
Die Liste der Benutzer wird angezeigt.
- 3 Klicken Sie auf **Benutzer importieren**.

4 Wählen Sie eine Quelle aus, aus der Sie die Benutzer importieren möchten.

Sie sehen nur den quellseitigen LDAP-Server oder SAML-Server, den Sie als Identitätsanbieter konfiguriert haben.

Quelle	Aktion
LDAP	<p>Importieren Sie Benutzer von einem LDAP-Server.</p> <ol style="list-style-type: none"> Geben Sie einen Namen oder den Teil eines Namens in das Textfeld ein und klicken Sie dann auf Suchen. Wählen Sie die Benutzer aus, die Sie importieren möchten, und klicken Sie auf Hinzufügen.
SAML	<p>Importieren Sie Benutzer von einem SAML-Server. Geben Sie die Benutzernamen der Benutzer ein, die Sie importieren möchten.</p> <p>Benutzernamen müssen in dem Namensbezeichnerformat angegeben werden, das von dem für diese Organisation konfigurierten SAML-Identitätsanbieter unterstützt wird.</p> <hr/> <p>Hinweis Wenn Sie vCenter Single Sign-On als SAML-Identitätsanbieter verwenden, müssen die Benutzernamen, die Sie aus einer vCenter Single Sign-On-Domäne importieren, im UPN-Format (User Principal Name) angegeben werden, z. B. jdoe@mydomain.com.</p> <hr/> <p>Verwenden Sie für jeden Benutzernamen eine neue Zeile.</p>

5 Wählen Sie die Rolle aus, die Sie den zu importierenden Benutzern zuweisen möchten.

6 Klicken Sie auf **Speichern**.


Ändern eines Benutzers

Als Organisationsadministrator können Sie das Kennwort, den Kontakt und die Kontingenteinstellungen für die virtuelle Maschine eines vorhandenen Benutzers ändern. Darüber hinaus können Sie auch die Rolle des Benutzers ändern.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- Wählen Sie im Hauptmenü () die Option **Administration** aus.
- Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
Die Liste der Benutzer wird angezeigt.
- Klicken Sie auf das Optionsfeld neben dem Namen des zu bearbeitenden Benutzers und klicken Sie auf **Ändern**.

- 4 Aktualisieren Sie die Einstellungen, die Sie ändern möchten.
 - a Ändern Sie das Kennwort nach Bedarf.
 - b Wählen Sie aus, ob der Benutzer aktiviert oder deaktiviert werden soll.
 - c Aktualisieren Sie die Benutzerrolle.
 - d Aktualisieren Sie die Kontaktinformationen wie Name, E-Mail-Adresse, Telefonnummer und Instant Messaging-ID.
 - e Bearbeiten Sie das Kontingent für virtuelle Maschinen für den Benutzer.
- 5 Klicken Sie auf **Speichern**.


Deaktivieren oder Aktivieren eines Benutzerkontos

Sie können ein Benutzerkonto deaktivieren, um zu verhindern, dass sich dieser Benutzer bei vCloud Director anmeldet. Wenn Sie einen Benutzer löschen möchten, müssen Sie zunächst sein Konto deaktivieren.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
Die Liste der Benutzer wird angezeigt.
- 3 Um ein Benutzerkonto zu deaktivieren, klicken Sie auf das Optionsfeld neben dem Benutzernamen, klicken Sie auf **Deaktivieren** und bestätigen Sie, dass Sie das Konto deaktivieren möchten.
- 4 Um ein bereits deaktiviertes Benutzerkonto zu aktivieren, klicken Sie auf das Optionsfeld neben dem Benutzernamen und dann auf **Aktivieren**.


Löschen eines Benutzers

Sie können einen Benutzer aus der vCloud Director-Organisation entfernen, indem Sie das Benutzerkonto löschen.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Deaktivieren Sie das Konto, das Sie löschen möchten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
Die Liste der Benutzer wird angezeigt.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des zu löschenden Benutzers und klicken Sie auf **Löschen**.
- 4 Um zu bestätigen, dass Sie das Benutzerkonto löschen möchten, klicken Sie auf **OK**.


Entsperren eines gesperrten Benutzerkontos

Für den Fall, dass Sie eine Sperrrichtlinie in Ihrer vCloud Director-Organisation aktiviert haben, wird ein Benutzerkonto nach einer bestimmten Anzahl ungültiger Anmeldeversuche gesperrt. Sie können das gesperrte Benutzerkonto entsperren. Eine bewährte Methode besteht darin, das Kennwort des Benutzers zu ändern und das Konto zu entsperren.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
Die Liste der Benutzer wird angezeigt.
- 3 Klicken Sie auf das Optionsfeld neben dem Benutzernamen und klicken Sie dann auf **Entsperren**.

Verwalten von Gruppen

Wenn Sie über eine gültige Verbindung zu einem LDAP-Server verfügen oder ermöglicht haben, dass Ihre Organisation einen SAML-Identitätsanbieter verwendet, können Sie eine LDAP-Gruppe oder eine SAML-Gruppe importieren. Eine importierte Gruppe kann auch bearbeitet oder gelöscht werden.


Importieren einer Gruppe

Um eine Gruppe von Benutzern hinzuzufügen, können Sie eine LDAP-Gruppe oder eine SAML-Gruppe importieren.

Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.
- Vergewissern Sie sich, dass Sie über eine gültige Verbindung zu einem LDAP-Server verfügen oder dass Sie [Kapitel 15 Aktivieren der Verwendung eines SAML-Identitätsanbieters für die Organisation](#). Weitere Informationen finden Sie unter *vCloud Director-Administratorhandbuch*.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Gruppen**.
Die Liste der Benutzergruppen wird angezeigt.
- 3 Klicken Sie auf **Gruppe importieren**.
- 4 Wählen Sie eine Quelle aus, aus der Sie die Benutzergruppe importieren möchten.
Sie sehen nur den quellseitigen LDAP-Server oder SAML-Server, den Sie als Identitätsanbieter konfiguriert haben.

Quelle	Aktion
LDAP	Importieren Sie Benutzer von einem LDAP-Server. <ol style="list-style-type: none"> a Geben Sie einen Namen oder den Teil eines Namens in das Textfeld ein und klicken Sie dann auf Suchen. b Wählen Sie die Benutzer aus, die Sie importieren möchten, und klicken Sie auf Hinzufügen.
SAML	Importieren Sie Benutzergruppen von einem SAML-Server. Geben Sie die Namen der Gruppen ein, die Sie importieren möchten. Verwenden Sie für jeden Gruppennamen eine neue Zeile.

- 5 Wählen Sie die Rolle aus, die Sie der zu importierenden Gruppe von Benutzern zuweisen möchten.
- 6 Klicken Sie auf **Speichern**.

Löschen einer Gruppe


Sie können eine Gruppe aus der vCloud Director-Organisation entfernen, indem Sie die entsprechende LDAP-Gruppe löschen.

Wenn Sie eine LDAP-Gruppe löschen, werden Benutzer, deren vCloud Director-Konto ausschließlich auf der Grundlage ihrer Mitgliedschaft in dieser Gruppe beruht, isoliert und können sich nicht mehr anmelden.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Gruppen**.
Die Liste der Benutzergruppen wird angezeigt.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der zu löschenden Gruppe und anschließend auf **Löschen**.
- 4 Um zu bestätigen, dass Sie die Gruppe löschen möchten, klicken Sie auf **OK**.


Bearbeiten einer Gruppe

Sie können eine Gruppe im vCloud Director-Mandantenportal bearbeiten.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Gruppen**.
Die Liste der Benutzergruppen wird angezeigt.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der zu löschenden Gruppe und dann auf **Bearbeiten**.
- 4 Bearbeiten Sie die Gruppe nach Bedarf.
 - a Ändern Sie die Beschreibung.
 - b Ändern Sie die Rolle der Mitglieder der Gruppe nach Bedarf.
- 5 Klicken Sie auf **Speichern**.

Rollen und Rechte

vCloud Director verwendet Rollen und Rechte, um zu bestimmen, welche Aktionen Benutzer in einer Organisation durchführen dürfen. In vCloud Director sind einige Rollen mit bestimmten Rechten vordefiniert.

Systemadministratoren und **Organisationsadministratoren** müssen jedem Benutzer und jeder Gruppe eine Rolle zuweisen. Ein Benutzer kann in verschiedenen Organisationen verschiedene Rollen haben. **Systemadministratoren** können Rollen erstellen und bestehende Rollen für das gesamte System bearbeiten, während die **Organisationsadministratoren** Rollen nur für die Organisation, die sie verwalten, erstellen und ändern können.

Im vCloud Director-Mandantenportal können **Organisationsadministratoren** die Rollen in ihrer Organisation verwalten. Wenn ein **Systemadministrator** vordefinierte Mandantenrollen für Ihre Organisation veröffentlicht, können Sie als **Organisationsadministrator** diese Rollen zwar sehen, aber nicht ändern. Allerdings können Sie benutzerdefinierte Mandantenrollen mit ähnlichen Rechten erstellen und diese den Benutzern in Ihrer Organisation zuweisen.

Weitere Informationen zu den vordefinierten Rollen und den jeweiligen Rechten erhalten Sie unter [Vordefinierte Rollen und ihre Rechte](#).

Vordefinierte Rollen und ihre Rechte

Jede vordefinierte vCloud Director-Rolle enthält einen Standardsatz an Rechten, die erforderlich sind, um in gemeinsamen Workflows enthaltene Vorgänge auszuführen. Standardmäßig werden alle globalen vordefinierten Mandantenrollen für jede Organisation im System veröffentlicht:

Vordefinierte Anbieterrollen

Standardmäßig gibt es als lokale Anbieterrollen für die Anbieterorganisationen nur die Rollen **Systemadministrator** und **Multisite-System**. **Systemadministratoren** können zusätzliche benutzerdefinierte Anbieterrollen erstellen.

Systemadministrator

Die Rolle **Systemadministrator** ist nur in der Anbieterorganisation vorhanden. Die Rolle **Systemadministrator** umfasst alle Rechte im System. Die Anmeldeinformationen des **Systemadministrators** werden während der Installation und Konfiguration festgelegt. Ein **Systemadministrator** kann zusätzliche Systemadministrator- und Benutzerkonten in der Anbieterorganisation einrichten.

Multisite-System

Wird zur Ausführung des Heartbeat-Prozesses für Bereitstellungen mit mehreren Standorten verwendet. Diese Rolle verfügt lediglich über das Recht **Multisite: Systemvorgänge**, mit dem eine vCloud-API-Anforderung zum Abrufen des Status des Remotemitglieds einer Sitezuordnung gestellt werden kann.

Vordefinierte globale Mandantenrollen

Standardmäßig werden die vordefinierten globalen Mandantenrollen und die darin enthaltenen Rechte für alle Organisationen veröffentlicht. **Systemadministratoren** können die Veröffentlichung von Rechten und globalen Mandantenrollen einzelner Organisationen rückgängig machen.

Systemadministratoren können vordefinierte globale Mandantenrollen bearbeiten oder löschen. **Systemadministratoren** können zusätzliche globale Mandantenrollen erstellen und veröffentlichen.

Organisationsadministrator

Nach dem Erstellen einer Organisation kann ein **Systemadministrator** einem beliebigen Benutzer in der Organisation die Rolle **Organisationsadministrator** zuweisen. Ein Benutzer mit der vordefinierten Rolle **Organisationsadministrator** kann die vCloud Director-Webkonsole, das Mandantenportal oder die vCloud OpenAPI verwenden, um Benutzer und Gruppen in seiner Organisation zu verwalten und ihnen Rollen zuzuweisen, einschließlich der vordefinierten Rolle **Organisationsadministrator**. Von einem **Organisationsadministrator** erstellte oder geänderte Rollen sind für andere Organisationen nicht sichtbar.

Katalogautor

Die mit der vordefinierten Rolle **Katalogautor** verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu erstellen und zu veröffentlichen.

vApp-Autor

Die mit der vordefinierten Rolle **vApp-Autor** verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu verwenden und vApps zu erstellen.

vApp-Benutzer

Die mit der vordefinierten Rolle **vApp-Benutzer** verknüpften Rechte ermöglichen es einem Benutzer, vorhandene vApps zu verwenden.

Nur Konsolenzugriff

Die mit den vordefinierten Rolle **Nur Konsolenzugriff** verknüpften Rechte ermöglichen es einem Benutzer, den Status und die Eigenschaften von virtuellen Maschinen anzuzeigen und das Gastbetriebssystem zu verwenden.

Auf Identitätsanbieter zurückstellen

Die mit der vordefinierten Rolle **Auf Identitätsanbieter zurückstellen** verknüpften Rechte werden basierend auf vom OAuth- oder SAML-Identitätsanbieter empfangenen Informationen festgelegt. Um sich für die Aufnahme zu qualifizieren, wenn einem Benutzer oder einer Gruppe die Rolle **Auf Identitätsanbieter zurückstellen** zugewiesen ist, muss ein vom Identitätsanbieter bereitgestellter Rollen- oder Gruppenname exakt (unter Berücksichtigung von Groß-/Kleinschreibung) mit einem innerhalb Ihrer Organisation definierten Rollen- oder Gruppennamen übereinstimmen.

- Wenn der Benutzer von einem OAuth-Identitätsanbieter definiert wird, werden dem Benutzer die im Array `roles` des benutzereigenen OAuth-Tokens benannten Rollen zugewiesen.
- Einem von einem SAML-Identitätsanbieter definierten Benutzer werden die Rollen zugewiesen, die in dem SAML-Attribut angegeben werden, dessen Name im Element `RoleAttributeName` angezeigt wird, das sich wiederum im Element `SamlAttributeMapping` in `OrgFederationSettings` der Organisation befindet.

Wenn einem Benutzer die Rolle **Auf Identitätsanbieter zurückstellen** zugewiesen wird, jedoch keine übereinstimmende Rolle bzw. kein übereinstimmender Gruppenname in Ihrer Organisation vorhanden ist, kann sich der Benutzer bei der Organisation anmelden, verfügt jedoch über keine Rechte. Wenn ein Identitätsanbieter einem Benutzer eine Rolle auf Systemebene zuweist, wie beispielsweise die eines **Systemadministrators**, kann sich der Benutzer bei der Organisation anmelden, verfügt jedoch über keine Rechte. Solchen Benutzern müssen Sie eine Rolle manuell zuweisen.

Mit Ausnahme der Rolle **Auf Identitätsanbieter zurückstellen** enthält jede vordefinierte Rolle einen Satz von Standardrechten. Nur ein **Systemadministrator** kann die Rechte in einer vordefinierten Rolle ändern. Wenn ein **Systemadministrator** eine vordefinierte Rolle ändert, werden die Änderungen an alle Instanzen der Rolle im System weitergegeben.

Rechte in vordefinierten globalen Mandantenrollen

Mehrere vordefinierte globale Rollen haben verschiedene Rechte gemein. Diese Rechte werden standardmäßig allen neuen Organisationen gewährt und können in anderen Rollen verwendet werden, die vom **Organisationsadministrator** erstellt werden.

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolen zugriff
Katalog: vApp von „Meine Cloud“ hinzufügen	X	X	X		
Katalog: Externe Veröffentlichung/ Externe Abonnements für die Kataloge zulassen	X	X			
Katalog: Besitzer ändern	X				
Katalog: Katalog erstellen/löschen	X	X			

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolen zugriff
Katalog: Katalogeigenschaften bearbeiten	X	X			
Katalog: Katalog für andere Organisationen freigeben	X	X			
Katalog: Katalog für andere Benutzer/ Gruppen innerhalb der aktuellen Organisation freigeben	X	X			
Katalog: Private und freigegebene Kataloge innerhalb der aktuellen Organisation anzeigen	X	X	X		
Katalog: Freigegebene Kataloge von anderen Organisationen anzeigen	X				
Katalogelement: Zu „Meine Cloud“ hinzufügen	X	X	X	X	
Katalogelement: vApp-Vorlage/Medien kopieren/verschieben	X	X	X		
Katalogelement: vApp-Vorlage/Medien erstellen/hochladen	X	X			
Katalogelement: vApp-Vorlage/Medien bearbeiten	X	X			
Katalogelement: Herunterladen von vApp-Vorlagen/-Medien aktivieren	X	X			
Katalogelement: vApp-Vorlagen/Medien anzeigen	X	X	X	X	
Benutzerdefinierte Entität: Alle benutzerdefinierten Entitätsinstanzen in der Organisation anzeigen	X				
Benutzerdefinierte Entität: Benutzerdefinierte Entitätsinstanz anzeigen	X				
Datenträger: Besitzer ändern	X	X			
Datenträger: Datenträger erstellen	X	X	X		
Datenträger: Datenträger löschen	X	X	X		
Datenträger: Datenträgereigenschaften bearbeiten	X	X	X		
Datenträger: Datenträgereigenschaften anzeigen	X	X	X	X	
Verteilte Firewall: Regeln der verteilten Firewall konfigurieren	X				

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolen zugriff
Distributed Firewall: Distributed Firewall aktivieren/deaktivieren	X				
Verteilte Firewall: Regeln der verteilten Firewall anzeigen	X				
Edge-Cluster: Edge-Cluster anzeigen	X				
Edge-Cluster: Edge-Cluster verwalten	X				
Gateway: Syslog-Server konfigurieren	X				
Gateway: Systemprotokollierung konfigurieren	X				
Gateway: In erweitertes Gateway konvertieren	X				
Gateway: Gateway anzeigen	X				
Gateway: Distributed Routing aktivieren	X				
Gateway: Edge-Gateway importieren	X				
Gateway-Dienste: BGP-Routing konfigurieren					
Gateway-Dienste: DHCP konfigurieren	X				
Gateway-Dienste: Firewall konfigurieren	X				
Gateway-Dienste: IPSEC-VPN konfigurieren	X				
Gateway-Dienste: L2-VPN konfigurieren					
Gateway-Dienste: Lastausgleichsdienst konfigurieren	X				
Gateway-Dienste: NAT konfigurieren	X				
Gateway-Dienste: OSPF-Routing konfigurieren	X				
Gateway-Dienste: Remotezugriff konfigurieren	X				
Gateway-Dienste: SSL-VPN konfigurieren	X				
Gateway-Dienste: Statisches Routing konfigurieren	X				
Gateway-Dienste: Nur Ansicht „ BGP-Routing“	X				

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadministrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolen zugriff
Gateway-Dienste: Nur Ansicht „DHCP“	X				
Gateway-Dienste: Nur Ansicht „Firewall“	X				
Gateway-Dienste: Nur Ansicht „IPSEC-VPN“	X				
Gateway-Dienste: Nur Ansicht „L2 VPN“	X				
Gateway-Dienste: Nur Ansicht „Lastausgleichsdienst“	X				
Gateway-Dienste: Nur Ansicht „NAT“	X				
Gateway-Dienste: Nur Ansicht „OSPF-Routing“	X				
Gateway-Dienste: Nur Ansicht „Remotezugriff“	X				
Gateway-Dienste: Nur Ansicht „SSL-VPN“	X				
Gateway-Dienste: Nur Ansicht „Statisches Routing“	X				
Allgemein: Administratorsteuerung	X				
Allgemein: Administratoransicht	X				
Allgemein: Benachrichtigung senden	X				
Hybrid-Tunnel: Ticket zur Steuerung abrufen	X				
Hybrid-Tunnel: Ticket für Aus-der-Cloud-Tunnel abrufen	X				
Hybrid-Tunnel: Cloud-Tunnel-Ticket abrufen	X				
Hybrid-Tunnel: Aus-der-Cloud-Tunnel erstellen	X				
Hybrid-Tunnel: Cloud-Tunnel erstellen	X				
Hybrid-Tunnel: Aus-der-Cloud-Tunnel löschen	X				
Hybrid-Tunnel: Cloud-Tunnel löschen	X				
Hybrid-Tunnel: Endpunkt-Tag des Aus-der-Cloud-Tunnels aktualisieren	X				
Hybrid-Tunnel: Cloud-Tunnel-Server-Einstellungen anzeigen	X				

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolen zugriff
Hybrid-Tunnel: Aus-der-Cloud-Tunnel anzeigen	X				
Hybrid-Tunnel: Cloud-Tunnel anzeigen	X				
Organisation: Zugriff auf alle Organisations-VDCs zulassen	X				
Organisation: Zugriffskontrollliste von Organisations-VDCs bearbeiten	X				
Organisation: Verbundeinstellungen bearbeiten	X				
Organisation: Lease-Richtlinie bearbeiten	X				
Organisation: Organisationsverknüpfungen bearbeiten	X				
Organisation: Netzwerkeinstellungen einer Organisation bearbeiten	X				
Organisation: OAuth-Einstellungen der Organisation bearbeiten	X				
Organisation: Organisationseigenschaften bearbeiten	X				
Organisation: Kennwortrichtlinie bearbeiten	X				
Organisation: Kontingent-Richtlinie bearbeiten	X				
Organisation: SMTP-Einstellungen bearbeiten	X				
Organisation: Benutzer/Gruppe beim Bearbeiten der VDC-ACL implizit aus Identitätsanbieter importieren	X				
Organisation: Zugriffskontrollliste von Organisations-VDCs anzeigen	X				
Organisation: Katalog-ACL anzeigen	X	X			
Organisation: Organisationsnetzwerke anzeigen	X				
Organisation: Organisationen anzeigen	X	X	X		
Organisation: vApp-ACL anzeigen	X	X	X	X	
Organisations-VDC: VDC-Namen und -Beschreibung der Organisation bearbeiten	X				

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolen zugriff
Organisations-VDC: VM-VM-Affinitätsregel bearbeiten	X	X	X		
Organisations-VDC: Erweiterte Eigenschaften des Organisations-VDC bearbeiten	X				
Organisations-VDC: Firewall verwalten	X				
Organisations-VDC: Standardmäßige Speicherrichtlinie festlegen	X				
Organisations-VDC: Computing-Richtlinien für ein Organisations-VDC anzeigen	X	X	X	X	
Organisations-VDC: Erweiterte Eigenschaften des Organisations-VDC anzeigen	X				
VDC-Organisationsnetzwerk: Eigenschaften anzeigen	X				
VDC-Organisationsnetzwerk: Eigenschaften bearbeiten	X				
VDC-Organisationsnetzwerk: Netzwerk importieren	X				
Organisations-VDC: Organisations-VDCs anzeigen	X				
Organisations-VDC-Vorlage: Organisations-VDC-Vorlagen instanziiieren	X				
Organisations-VDC-Vorlage: VDC-Vorlagen anzeigen	X				
Provider-Netzwerk: Provider-Netzwerk anzeigen	X				
Provider-Netzwerk: Provider-Netzwerk erstellen/löschen	X				
Rolle: Rolle erstellen/aktualisieren/löschen	X				
Dienstbibliothek: Dienste anzeigen, die in der Dienstbibliothek enthalten sind	X				
Benutzer: Gruppe/Benutzer anzeigen	X				
VCD-Erweiterung: Informationen zum Mandantenportal-Plug-In anzeigen	X	X	X	X	
VDC-Gruppe: VDC-Gruppe anzeigen	X				

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolen zugriff
VDC-Gruppe: VDC-Gruppe konfigurieren	X				
VM-Überwachung: Historische Metriken für die Organisation anzeigen	X				
VM-Überwachung: Historische Metriken für das Organisations-VDC anzeigen	X				
vApp: Auf die VM-Konsole zugreifen	X	X	X	X	X
vApp: Zulassen, dass Metadaten Domäne zu vCenter Server zuordnen	X	X	X		
vApp: Besitzer ändern	X				
vApp: vApp-Vorlagenbesitzer ändern	X	X			
vApp: vApp kopieren	X	X	X	X	
vApp: vApp erstellen/neu konfigurieren	X	X	X		
vApp: Snapshot erstellen/ wiederherstellen/entfernen	X	X	X	X	
vApp: vApp löschen	X	X	X	X	
vApp: vApp herunterladen	X	X	X		
vApp: VM-Startoptionen bearbeiten/ anzeigen	X	X	X		
vApp: CPU der VM bearbeiten	X	X	X		
vApp: Festplatte der VM bearbeiten	X	X	X		
vApp: Arbeitsspeicher der VM bearbeiten	X	X	X		
vApp: VM-Netzwerk bearbeiten	X	X	X	X	
vApp: VM-Eigenschaften bearbeiten	X	X	X	X	
vApp: vApp-Eigenschaften bearbeiten	X	X	X	X	
vApp: VM-Computing-Richtlinie bearbeiten	X	X	X		
vApp: VM-Kennworteinstellungen verwalten	X	X	X	X	X
vApp: vApp freigeben	X	X	X	X	
vApp: vApp starten/beenden/anhalten/ zurücksetzen	X	X	X	X	

Tabelle 14-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolen zugriff
vApp: vApp hochladen	X	X	X		
vApp: VM-Metriken anzeigen	X		X	X	

Informationen zu den neuen Rechten, die von vCloud Director 9.7 eingeführt werden, finden Sie unter [#unique_269](#).


Erstellen einer benutzerdefinierten Mandantenrolle

Organisationsadministratoren können das Mandantenportal zum Erstellen benutzerdefinierter Mandantenrollenobjekte in den von ihnen verwalteten Organisationen verwenden.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Rollen**.
Die Liste der Rollen wird angezeigt.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung der Rolle ein.
- 5 Erweitern Sie die Rechte für die Rolle und wählen Sie die Rechte für die Rolle aus.

Die Rechte sind in Kategorien und Unterkategorien zusammengefasst, die entweder die Anzeige oder die Verwaltung von Objekten zulassen.

Option	Beschreibung
Zugriffssteuerung	Rechte, die den Zugriff auf bestimmte Objekte steuern, um diese anzuzeigen und zu verwalten.
Administration	Rechte, die den Verwaltungszugriff steuern.
Computing	Rechte, die den Zugriff auf die Organisations- und Anbieter-VDCs, die vApps, die VDC-Organisationsvorlagen, die VM-Gruppen und die VM-Überwachung sowie deren Verwaltung steuern.
Erweiterungen	Rechte, die den Zugriff auf zusätzliche Plug-Ins und vCloud Director-Erweiterungen steuern.
Infrastruktur	Rechte, die den Zugriff auf und die Verwaltung der Infrastrukturobjekte steuern, wie z. B. Datenspeicher, Festplatten, Hosts usw.

Option	Beschreibung
Bibliotheken	Rechte, die den Zugriff auf und die Verwaltung aller Kataloge und Katalogelemente steuern.
Netzwerk	Rechte, die den Zugriff auf die Netzwerkeinstellungen sowie deren Verwaltung steuern.

6 Klicken Sie auf **Speichern**.


Bearbeiten einer benutzerdefinierten Mandantenrolle

Organisationsadministratoren können das Mandantenportal zum Bearbeiten der benutzerdefinierten Mandantenrollenobjekte in den von ihnen verwalteten Organisationen verwenden. Als Organisationsadministrator können Sie die globalen Mandantenrollen, die ein Systemadministrator für Ihre Organisation veröffentlicht hat, nur anzeigen, aber nicht bearbeiten.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Rollen**.
Die Liste der Rollen wird angezeigt.
- 3 Klicken Sie auf das Optionsfeld neben der zu bearbeitenden Rolle und klicken Sie auf **Bearbeiten**.
- 4 Ändern Sie die Rolleneinstellungen je nach Bedarf.
 - a Ändern Sie den Namen und optional die Beschreibung der Rolle.
 - b Bearbeiten Sie die Rechte für die Rolle.
- 5 Klicken Sie auf **Speichern**.


Löschen einer Rolle

Organisationsadministratoren können das Mandantenportal zum Löschen der Rollenobjekte in den von ihnen verwalteten Organisationen verwenden.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.

- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Rollen**.

Die Liste der Rollen wird angezeigt.

- 3 Klicken Sie auf das Optionsfeld neben der zu löschenden Rolle und klicken Sie auf **Löschen**.
- 4 Bestätigen Sie, dass Sie die Rolle löschen möchten, indem Sie auf **OK** klicken.

Aktivieren der Verwendung eines SAML-Identitätsanbieter für die Organisation

15

Aktivieren Sie für Ihre Organisation die Verwendung eines SAML-Identitätsanbieters (Security Assertion Markup Language), auch als Single Sign-On bezeichnet, um Benutzer und Gruppen aus einem SAML-Identitätsanbieter zu importieren und zuzulassen, dass importierte Benutzer sich bei der Organisation mit den im SAML-Identitätsanbieter festgelegten Anmeldeinformationen anmelden.

Wenn Sie Benutzer und Gruppen importieren, extrahiert das System eine Liste der Attribute aus dem SAML-Token, sofern verfügbar, und verwendet diese für die Interpretation der entsprechenden Informationen über den Benutzer, der den Anmeldeversuch unternimmt.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

Das Rollenattribut ist konfigurierbar.

Gruppeninformationen sind notwendig, wenn der Benutzer nicht direkt importiert wird, sondern wenn von ihm erwartet wird, dass er sich aufgrund seiner Mitgliedschaft in importierten Gruppen selbst anmelden kann. Ein Benutzer kann mehreren Gruppen angehören und während einer Sitzung mehrere Rollen einnehmen.

Wenn einem importierten Benutzer oder einer importierten Gruppe die Rolle **Auf Identitätsanbieter zurückstellen** zugewiesen ist, werden die Rollen basierend auf den aus dem Attribut „Rollen“ im Token ermittelten Informationen zugewiesen. Wenn ein anderes Attribut verwendet wird, kann dieser Attributname nur über die API konfiguriert werden und einzig das Attribut „Rollen“ ist konfigurierbar. Wenn die Rolle **Auf Identitätsanbieter zurückstellen** verwendet wird, jedoch keine Rolleninformationen extrahiert werden können, kann der Benutzer sich anmelden, verfügt jedoch über keine Rechte zum Durchführen von Aktivitäten.


Voraussetzungen

- Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

- Stellen Sie sicher, dass Sie Zugriff auf einen SAML 2.0-konformen Identitätsanbieter haben.
- Stellen Sie sicher, dass Sie die erforderlichen Metadaten von Ihrem SAML-Identitätsanbieter erhalten. Sie müssen die Metadaten entweder manuell oder als XML-Datei in vCloud Director importieren. Die Metadaten müssen die folgenden Informationen enthalten:
 - Der Speicherort des Single Sign On-Diensts
 - Der Speicherort des Diensts für die einmalige Abmeldung
 - Der Speicherort des X.509-Zertifikats für den Dienst

Informationen zum Konfigurieren und Abrufen von Metadaten von einem SAML-Anbieter finden Sie in der Dokumentation zu Ihrem SAML-Identitätsanbieter.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie unter **Identitätsanbieter** auf **SAML**.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Geben Sie auf der Registerkarte **Dienstanbieter** die Entitäts-ID ein.

Die Entitäts-ID ist der einzige Bezeichner Ihrer Organisation für Ihren Identitätsanbieter. Sie können den Namen Ihrer Organisation oder eine beliebige andere Zeichenfolge verwenden, die den Anforderungen Ihres SAML-Identitätsanbieters entspricht.

Wichtig Nachdem Sie eine Element-ID angegeben haben, können Sie diese nicht mehr löschen. Um die Entitäts-ID zu ändern, müssen Sie eine vollständige SAML-Neukonfiguration für Ihre Organisation durchführen. Informationen zu Entitäts-IDs finden Sie im Dokument [Assertions and Protocols for the OASIS Security Assertion Markup Language \(SAML\) 2.0](#).

- 5 Klicken Sie auf den **Metadaten**-Link, um die SAML-Metadaten für Ihre Organisation herunterzuladen.

Die heruntergeladenen Metadaten müssen Ihrem Identitätsanbieter unverändert bereitgestellt werden.

- 6 Überprüfen Sie das Ablaufdatum des Zertifikats und klicken Sie optional auf **Neu generieren**, um das Zertifikat neu zu generieren, das zum Signieren von Verbundnachrichten verwendet wird.

Das Zertifikat ist in den SAML-Metadaten enthalten und wird für die Verschlüsselung und Signierung verwendet. Die Verschlüsselung oder die Signatur oder beide sind möglicherweise erforderlich, je nachdem, wie die Vertrauensstellung zwischen Ihrem SAML-Identitätsanbieter und Ihrer Organisation eingerichtet ist.

- 7 Aktivieren Sie auf der Registerkarte **Identitätsprovider** die Umschaltoption **SAML-Identitätsprovider verwenden**.

- 8 Kopieren Sie die SAML-Metadaten, die Sie von Ihrem Identitätsanbieter erhalten haben, und fügen Sie sie in das Textfeld ein oder klicken Sie auf **Hochladen**, um eine XML-Datei mit den Metadaten zu suchen und hochzuladen.
- 9 Klicken Sie auf **Speichern**.

Nächste Schritte

- Konfigurieren Sie Ihren SAML-Anbieter mit vCloud Director-Metadaten. Weitere Informationen finden Sie in der Dokumentation für Ihren SAML-Identitätsanbieter und im *vCloud Director Installations- und Upgrade-Handbuch*.
- Importieren Sie Benutzer und Gruppen von Ihrem SAML-Identitätsanbieter. Weitere Informationen finden Sie unter [Kapitel 14 Verwalten von Benutzern, Gruppen und Rollen](#)

Als **Organisationsadministrator** können Sie mehrere Einstellungen in Ihrer Organisation ändern, wie z. B. den Namen der Organisation, E-Mail-Einstellungen, Domäneneinstellungen, Metadaten, Richtlinien usw.

Dieses Kapitel enthält die folgenden Themen:

- Bearbeiten des Namens und der Beschreibung der Organisation
- Ändern der E-Mail-Einstellungen
- Testen der SMTP-Einstellungen
- Ändern der Domäneneinstellungen für die virtuellen Maschinen in Ihrer Organisation
- Arbeiten mit mehreren Sites
- Konfigurieren und Verwalten von Multisite-Bereitstellungen
- Wissenswertes über Leases
- Ändern der Richtlinien für vApp- und vApp-Vorlage-Leases innerhalb der Organisation
- Ändern der Standardkontingente für die virtuellen Maschinen in Ihrer Organisation
- Ändern des Kennworts und der Richtlinien für Benutzerkonten in Ihrer Organisation


Bearbeiten des Namens und der Beschreibung der Organisation

Sie können den vollständigen Namen und die Beschreibung der Organisation bearbeiten.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.

2 Klicken Sie unter **Einstellungen** auf **Allgemein**.

Die Liste der allgemeinen Einstellungen, wie z. B. Name der Organisation, Standard-URL, vollständiger Name und Beschreibung, wird angezeigt.

3 Klicken Sie zum Bearbeiten des vollständigen Namens und der Beschreibung der Organisation auf **Bearbeiten**.

4 Wenden Sie die erforderlichen Änderungen an und klicken Sie auf **Speichern**.

Ändern der E-Mail-Einstellungen

Sie können die Standardeinstellungen für E-Mails überprüfen und ändern, die vom Systemadministrator beim Erstellen Ihrer Organisation festgelegt wurden.

vCloud Director sendet Warnungs-E-Mails, wenn wichtige Informationen übermittelt werden müssen, wie z. B. bei Speicherplatzmangel in einem Datacenter. Standardmäßig sendet eine Organisation E-Mail-Warnungen an den Systemadministrator oder an eine Liste mit E-Mail-Adressen, die auf Systemebene angegeben sind. Dafür wird ein auf Systemebene angegebener SMTP-Server verwendet. Sie können die E-Mail-Einstellungen auf Organisationsebene ändern, wenn vCloud Director Warnungen für diese Organisation an einen anderen Satz von E-Mail-Adressen als den auf Systemebene angegebenen Satz senden soll oder wenn die Organisation einen anderen SMTP-Server als den auf Systemebene angegebenen Server zum Senden von Warnungen verwenden soll.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

1 Wählen Sie im Hauptmenü () die Option **Administration** aus.

2 Klicken Sie unter **Einstellungen** auf **E-Mail**.

Die E-Mail-Einstellungen für Ihre Organisation werden angezeigt.

3 Klicken Sie auf **Bearbeiten**.

4 Bearbeiten Sie die Einstellungen für den SMTP-Server auf der Registerkarte **SMTP-Server**.

a Geben Sie an, ob ein benutzerdefinierter Server oder der Standardserver verwendet werden soll.

b Wenn Sie sich für die Verwendung eines benutzerdefinierten SMTP-Servers entscheiden, geben Sie den DNS-Hostnamen oder die IP-Adresse des SMTP-Servers im Textfeld **SMTP-Servername** ein.

- c (Optional) Geben Sie den SMTP-Serverport ein.
 - d (Optional) Geben Sie an, ob Authentifizierung erforderlich ist, und geben Sie einen Namen und ein Kennwort ein.
- 5** Klicken Sie zum Ändern der Benachrichtigungseinstellungen auf die Registerkarte **Benachrichtigungseinstellungen**.
- a Geben Sie an, ob benutzerdefinierte Benachrichtigungseinstellungen verwendet werden sollen.
 - b Geben Sie die E-Mail-Adresse ein, die als Absender in Organisations-E-Mails angezeigt wird.
 - c (Optional) Geben Sie den Text ein, der als Präfix für den E-Mail-Betreff verwendet werden soll.
 - d (Optional) Geben Sie an, ob Benachrichtigungen an alle Organisationsadministratoren oder an bestimmte E-Mail-Adressen gesendet werden sollen.
 - e (Optional) Wenn Sie sich für das Senden von Benachrichtigungen an bestimmte E-Mail-Adressen entschieden haben, geben Sie die E-Mail-Adressen getrennt durch Kommas ein.
- 6** Klicken Sie auf **Speichern**.


Testen der SMTP-Einstellungen

Nachdem Sie die E-Mail-Einstellungen für Ihre Organisation geändert haben, können Sie die SMTP-Einstellungen testen.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1** Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2** Klicken Sie unter **Einstellungen** auf **E-Mail**.
Die E-Mail-Einstellungen für Ihre Organisation werden angezeigt.
- 3** Klicken Sie auf **Testen**.
- 4** Geben Sie eine Ziel-E-Mail-Adresse und das Kennwort für den SMTP-Server ein, um die SMTP-Einstellungen zu testen, und klicken Sie auf die Schaltfläche **Testen**.


Ändern der Domäneneinstellungen für die virtuellen Maschinen in Ihrer Organisation

Sie können eine Windows-Standarddomäne festlegen, der virtuelle Maschinen, die innerhalb Ihrer Organisation erstellt wurden, beitreten können. Virtuelle Maschinen können jederzeit einer Domäne beitreten, für die sie über Anmeldeinformationen verfügen. Dabei spielt es keine Rolle, ob eine Standarddomäne festgelegt wurde.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie unter **Einstellungen** auf **Gast-Anpassung**.
- 3 Wählen Sie diese Option aus, um den Domänenbeitritt für die virtuellen Maschinen in der Organisation zu aktivieren.
- 4 Geben Sie den Domännennamen, den Benutzernamen und das Kennwort ein.
Die eingegebenen Anmeldedaten gelten für einen normalen Domänenbenutzer, nicht aber für einen Domänenadministrator.
- 5 (Optional) Geben Sie eine Organisationseinheit für das Konto ein.
- 6 Klicken Sie auf **Speichern**.

Arbeiten mit mehreren Sites

Mithilfe der Multisite-Funktion von vCloud Director kann ein Dienstanbieter oder Mandant mehrerer geografisch verteilter vCloud Director-Installationen (Servergruppen) diese Installationen und die zugehörigen Organisationen als einzelne Elemente verwalten und überwachen.

Das vCloud Director-Mandantenportal bietet **Organisationsadministratoren** die Möglichkeit, Organisationen an zugehörigen Sites zuzuordnen.

Weitere Informationen zu Sitezuordnungen finden Sie im *vCloud Director-Administratorhandbuch*.

Konfigurieren und Verwalten von Multisite-Bereitstellungen

Nachdem ein **Systemadministrator** zwei Sites verknüpft hat, können **Organisationsadministratoren** an jeder Mitgliedssite mit der Zuordnung ihrer Organisationen beginnen.

Zum Erstellen einer Zuordnung zwischen zwei Organisationen (in diesem Beispiel Org-A und Org-B) müssen Sie als **Organisationsadministrator** für beide Organisationen fungieren, damit Sie sich bei jeder Organisation anmelden, deren lokale Zuordnungsdaten abrufen und die abgerufenen Daten an die andere Organisation senden können.

Wichtig Der Vorgang der Zuordnung von zwei Organisationen kann logisch in zwei einander ergänzende Kopplungsvorgänge aufgeteilt werden. Im ersten Vorgang (in diesem Beispiel) wird Org-A an Site-A mit Org-B an Site-B gekoppelt. Dann müssen Sie Org-B an Site-B mit Org-A an Site-A koppeln. Die Zuordnung ist so lange unvollständig, bis beide Kopplungen abgeschlossen sind.

Voraussetzungen

- Die Sites, die von den Organisationen belegt sind, müssen einander zugeordnet sein.
- Sie müssen **Systemadministrator** an beiden Sites oder **Organisationsadministrator** in beiden Organisationen sein.

Verfahren

- 1 Melden Sie sich beim vCloud Director-Mandantenportal von Org-A an Site-A an, um die lokalen Zuordnungsdaten abzurufen.
 - a Klicken Sie auf **Administration**.
 - b Klicken Sie unter **Einstellungen** auf **Multisite**.
 - c Klicken Sie zum Herunterladen der Daten im XML-Format auf **Lokale Zuordnungsdaten exportieren**.

Der Browser speichert die Daten in einer Datei im Ordner „Downloads“.

- 2 Melden Sie sich beim vCloud Director-Mandantenportal von Org-B an Site-B an, um die lokalen Zuordnungsdaten aus Org-A an Site-A zu senden.
 - a Klicken Sie auf **Administration**.
 - b Klicken Sie unter **Einstellungen** auf **Multisite**.
 - c Klicken Sie auf **Neue Organisationszuordnung erstellen**.

Senden Sie die in [Schritt 1](#) heruntergeladenen Zuordnungsdaten an Org-B, indem Sie auf den Pfeil zum Hochladen unter dem Fenster **Neues Zuordnungs-XML** klicken und die lokalen Zuordnungsdaten auswählen, die Sie in [Schritt 1](#) heruntergeladen haben.

- d Klicken Sie auf **Weiter**, um die Daten zu überprüfen und abzusenden.

Das System koppelt Org-A an Site-A mit Org-B an Site-B.
- e Klicken Sie auf **Fertigstellen**, um die zugeordnete Organisation anzuzeigen.
- f Um Details der zugeordneten Organisation anzuzeigen oder die Zuordnung zu löschen, klicken Sie auf die Karte **Name der Organisation**.

- 3 Schließen Sie die Zuordnung ab, indem Sie Schritt 1 und 2 wiederholen, um die lokalen Zuordnungsdaten aus Org-B abzurufen und an Org-A zu senden.

Wissenswertes über Leases

Beim Erstellen von Organisationen müssen u. a. Leases angegeben werden. Leases ermöglichen eine grundlegende Steuerung der Speicher- und Rechenressourcen, indem festgelegt wird, wie lange vApps maximal ausgeführt und wie lange vApps und vApp-Vorlagen gespeichert werden dürfen.

Der Zweck von Laufzeit-Leases besteht darin, zu verhindern, dass inaktive vApps Rechenressourcen verbrauchen. Wenn beispielsweise ein Benutzer eine vApp startet und anschließend verreist, ohne sie anzuhalten, verbraucht die vApp fortlaufend Ressourcen.

Eine Laufzeit-Lease beginnt zu dem Zeitpunkt, an dem der Benutzer eine vApp startet. Wenn die Laufzeit-Lease abläuft, hält vCloud Director die vApp an.

Der Zweck von Speicher-Leases besteht darin, zu verhindern, dass nicht verwendete vApps und vApp-Vorlagen Speicherressourcen verbrauchen. Eine vApp-Speicher-Lease beginnt zu dem Zeitpunkt, an dem der Benutzer eine vApp anhält. Speicher-Leases haben keine Auswirkungen auf ausgeführte vApps. Eine vApp-Vorlagen-Speicher-Lease beginnt, wenn der Benutzer die vApp-Vorlage einer vApp oder einem Arbeitsbereich hinzufügt oder sie herunterlädt, kopiert oder verschiebt.

Bei Ablauf der Speicher-Lease kennzeichnet vCloud Director die vApp bzw. vApp-Vorlage als abgelaufen oder löscht sie entsprechend den festgelegten Organisationsrichtlinien.


Ändern der Richtlinien für vApp- und vApp-Vorlage-Leases innerhalb der Organisation

Sie können die Standardrichtlinien prüfen und ändern, die der Systemadministrator beim Erstellen der Organisation festgelegt hat.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie unter **Einstellungen** auf **Richtlinien**.

Sie können die Standardrichtlinien anzeigen, die Ihr Systemadministrator eingestellt hat.

- 3 Klicken Sie auf **Bearbeiten**.

4 Bearbeiten Sie die vApp-Leases.

vApp-Leases ermöglichen eine grundlegende Steuerung der Speicher- und Rechenressourcen der Organisation, indem festgelegt wird, wie lange vApps maximal ausgeführt und gespeichert werden dürfen. Darüber hinaus können Sie festlegen, was mit den vApps geschieht, wenn deren Speicher-Lease abläuft.

- a Geben Sie die maximale Laufzeit-Lease an, um festzulegen, wie lange vApps ausgeführt werden können, bevor sie automatisch beendet werden.
- b Wählen Sie eine Aktion aus, die bei Ablauf der Laufzeit durchgeführt werden soll, wie z. B. Ausschalten oder Anhalten.
- c Geben Sie die maximale Speicher-Lease ein, um festzulegen, wie lange vApps verfügbar bleiben, bevor sie automatisch bereinigt werden.
- d Wählen Sie eine Aktion zur Bereinigung des Speichers aus, wie z. B. permanentes Löschen der vApps oder Verschieben der vApps in die abgelaufenen Objekte.

5 Bearbeiten Sie die vApp-Vorlagen-Lease.

vApp-Vorlagen-Leases ermöglichen eine grundlegende Steuerung der Speicher- und Rechenressourcen der Organisation, indem festgelegt wird, wie lange vApp-Vorlagen maximal ausgeführt und gespeichert werden dürfen. Darüber hinaus können Sie festlegen, was mit den vApp-Vorlagen geschieht, wenn deren Speicher-Lease abläuft.

- a Geben Sie die maximale Speicher-Lease ein, um festzulegen, wie lange die vApp-Vorlagen verfügbar bleiben, bevor sie automatisch bereinigt werden.
- b Wählen Sie eine Aktion zur Bereinigung des Speichers aus, wie z. B. permanentes Löschen der vApp-Vorlagen oder Verschieben der vApp-Vorlagen in die abgelaufenen Objekte.

6 Klicken Sie auf **OK**.

Ändern der Standardkontingente für die virtuellen Maschinen in Ihrer Organisation


Sie können die Richtlinien für Standardkontingente überprüfen und ändern, die vom Systemadministrator beim Erstellen der Organisation festgelegt wurden.

Mit den Kontingenten wird die Anzahl der virtuellen Maschinen festgelegt, die pro Benutzer in den Organisations-VDCs gespeichert und eingeschaltet werden können. Die festgelegten Kontingente werden für alle der Organisation neu hinzugefügten Benutzer als Standardwerte übernommen. Auf Benutzerebene festgelegte Kontingente haben Vorrang vor Kontingenten, die auf der Organisationsebene festgelegt sind.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie unter **Einstellungen** auf **Richtlinien**.
Sie können die Standardrichtlinien anzeigen, die Ihr Systemadministrator eingestellt hat.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie zwischen einer unbegrenzten Anzahl an virtuellen Maschinen und einer von Ihnen festgelegten Anzahl.
- 5 Wählen Sie zwischen einer unbegrenzten Anzahl an eingeschalteten virtuellen Maschinen und einer von Ihnen festgelegten Anzahl.
- 6 Klicken Sie auf **OK**.

Ändern des Kennworts und der Richtlinien für Benutzerkonten in Ihrer Organisation


Sie können die Standardrichtlinien für Kennwörter und Benutzerkonten überprüfen und ändern, die vom Systemadministrator beim Erstellen der Organisation festgelegt wurden.

Mit den Richtlinien für Kennwörter und Benutzerkonten wird das Verhalten von vCloud Director festgelegt, wenn ein Benutzer ein ungültiges Kennwort eingibt.

Voraussetzungen

Dieser Vorgang erfordert die in der vordefinierten Rolle **Organisationsadministrator** enthaltenen Rechte oder entsprechende Rechte.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie unter **Einstellungen** auf **Richtlinien**.
Sie können die Standardrichtlinien anzeigen, die Ihr Systemadministrator eingestellt hat.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Sperrung eines Benutzerkontos nach einer Reihe von ungültigen Anmeldeversuchen aktivieren.
- 5 Geben Sie die Anzahl der ungültigen Anmeldeversuche bis zur Sperrung des Benutzerkontos ein.
- 6 Geben Sie das Zeitintervall in Minuten ein, während dessen der Benutzer des gesperrten Kontos keinen weiteren Anmeldeversuch durchführen kann.
- 7 Klicken Sie auf **OK**.

Bei den Elementen der Dienstbibliothek in vCloud Director handelt es sich um vRealize Orchestrator-Workflows, die die Cloud-Verwaltungsfunktionen erweitern und es Administratoren anderer Anbieter oder Mandanten ermöglichen, verschiedene Dienste zu überwachen und zu bearbeiten.

Dieses Kapitel enthält die folgenden Themen:

- [Auffinden eines Diensts](#)
- [Ausführen eines Diensts](#)

Auffinden eines Diensts

Auf der Seite **Dienstbibliothek** im vCloud Director-Mandantenportal werden die vRealize Orchestrator-Workflows aufgelistet, die in vCloud Director importiert und für Ihre Organisation veröffentlicht werden.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Dienstbibliothek“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Dienstbibliothek** aus.

Die Liste der Dienstelemente wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die vRealize Orchestrator importiert wird.

- 2 Geben Sie oben auf der Seite im Textfeld **Suchen** das erste Wort des Namens des Diensts oder der Kategorie ein, zu dem bzw. der der Dienst gehört.

a Geben Sie an, ob Sie die Dienstnamen oder die Kategorien durchsuchen möchten.

Die Suchergebnisse werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind.

Ausführen eines Diensts

Sie können einen Dienst über die Seite „Dienstbibliothek“ im Mandantenportal von vCloud Director ausführen.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Dienstbibliothek“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Dienstbibliothek** aus.

Die Liste der Dienstelemente wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die vRealize Orchestrator importiert wird.

- 2 Suchen Sie nach dem Dienst, den Sie ausführen möchten.

- 3 Klicken Sie auf der Karte des Diensts auf **Ausführen**.

Ein neues Dialogfeld wird geöffnet. Sie müssen Werte für die erforderlichen Eingabeparameter des Diensts eingeben.

- 4 Klicken Sie auf **Fertigstellen**, um die Ausführung des Diensts zu bestätigen.

Nächste Schritte

Sie können in der Ansicht **Kürzlich bearbeitete Aufgaben** den Status der Ausführung überwachen. Weitere Informationen finden Sie unter [Anzeigen von Aufgaben](#).

Arbeiten mit benutzerdefinierten Entitätsdefinitionen

18

Bei den benutzerdefinierten Entitätsdefinitionen in vCloud Director handelt es sich um Objekttypen, die an vRealize Orchestrator-Objekttypen gebunden sind. Benutzer innerhalb einer vCloud Director-Organisation können diese Typen entsprechend ihrer Bedürfnisse besitzen, verwalten und ändern. Durch Ausführen von Diensten können Organisationsbenutzer die benutzerdefinierten Entitäten instanziierten und Aktionen auf die Instanzen der Objekte anwenden.

Dieses Kapitel enthält die folgenden Themen:

- [Auffinden einer benutzerdefinierten Entität](#)
- [Bearbeiten einer benutzerdefinierten Entitätsdefinition](#)
- [Hinzufügen einer benutzerdefinierten Entitätsdefinition](#)
- [Benutzerdefinierte Entitätsinstanzen](#)
- [Verknüpfen einer Aktion mit einer benutzerdefinierten Entität](#)
- [Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entitätsdefinition](#)
- [Veröffentlichen einer benutzerdefinierten Entität](#)
- [Löschen einer benutzerdefinierten Entität](#)

Auffinden einer benutzerdefinierten Entität

Sie können nach den benutzerdefinierten Entitäten suchen, die für Ihre Organisation veröffentlicht wurden.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Geben Sie im Textfeld **Suchen** oben auf der Seite ein Wort oder ein Zeichen des Namens der Entität ein, nach der Sie suchen.

Die Suchergebnisse werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind.

Bearbeiten einer benutzerdefinierten Entitätsdefinition

Sie können den Namen und die Beschreibung einer benutzerdefinierten Entität ändern. Sie können den Typ des Elements oder den vRealize Orchestrator-Objektyp, an den die Entität gebunden ist, nicht ändern. Hierbei handelt es sich um die Standardeigenschaften der benutzerdefinierten Entität. Wenn Sie beliebige Standardeigenschaften ändern möchten, müssen Sie die benutzerdefinierte Entitätsdefinition löschen und neu erstellen.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Bearbeiten** aus.

Ein neues Dialogfeld wird geöffnet.

- 3 Ändern Sie den Namen oder die Beschreibung der benutzerdefinierten Entitätsdefinition.
- 4 Klicken Sie auf **OK**, um die Änderung zu bestätigen.

Hinzufügen einer benutzerdefinierten Entitätsdefinition

Sie können eine benutzerdefinierte Entität erstellen und einem vorhandenen vRealize Orchestrator-Objektyp zuordnen.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Klicken Sie auf das Symbol , um eine neue benutzerdefinierte Entität hinzuzufügen.

Ein neues Dialogfeld wird geöffnet.

- 3 Führen Sie die im Assistenten **Benutzerdefinierte Entitätsdefinition** angezeigten Schritte durch.

Schritt	
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung für die neue Entität ein. Geben Sie einen Namen für den Entitätstyp ein, z. B. <code>sshHost</code> .
vRO	Wählen Sie im Dropdown-Menü den vRealize Orchestrator aus, den Sie zum Zuordnen der benutzerdefinierten Entitätsdefinition verwenden möchten. Hinweis Bei mehreren vRealize Orchestrator-Servern müssen Sie für jeden einzelnen Server eine benutzerdefinierte Entitätsdefinition erstellen.
Typ	Klicken Sie auf das Symbol für die Listenansicht () , um durch die verfügbaren nach Plug-Ins gruppierten vRealize Orchestrator-Objektypen zu navigieren. Beispielsweise SSH > Host . Wenn Sie den Namen des Typs kennen, können Sie ihn direkt im Textfeld eingeben. Beispiel: <code>SSH:Host</code> .
Überprüfen	Überprüfen Sie die von Ihnen angegebenen Details und klicken Sie auf Fertig , um den Erstellvorgang abzuschließen.

Ergebnisse

Die neue benutzerdefinierte Entitätsdefinition wird in der Kartenansicht angezeigt.

Benutzerdefinierte Entitätsinstanzen

Wenn Sie einen vRealize Orchestrator-Workflow mit einem Eingabeparameter ausführen, der einen Objekttyp darstellt, der bereits als benutzerdefinierte Entitätsdefinition in vCloud Director definiert ist, wird der Ausgabeparameter als Instanz einer benutzerdefinierten Entität angezeigt.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Klicken Sie auf der Karte der ausgewählten benutzerdefinierten Entität auf **Instanzen**.

Die verfügbaren Instanzen werden in einer Rasteransicht angezeigt.

- 3 Klicken Sie auf die Listenleiste () auf der linken Seite jeder Entität, um die verknüpften Workflows anzuzeigen.

Durch Klicken auf einen Workflow wird eine Workflowausführung gestartet, die die Entitätsinstanz als Eingabeparameter verwendet.

Verknüpfen einer Aktion mit einer benutzerdefinierten Entität

Durch Verknüpfen einer Aktion mit einer benutzerdefinierten Entitätsdefinition können Sie mehrere vRealize Orchestrator-Workflows in den Instanzen einer bestimmten benutzerdefinierten Entität ausführen.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Aktion verknüpfen** aus.

Ein neues Dialogfeld wird geöffnet.

- 3 Führen Sie die im Assistenten **Benutzerdefinierte Entität mit VRO-Workflow verknüpfen** angezeigten Schritte durch.

Schritt	Details
VRO-Workflow auswählen	Wählen Sie einen der aufgelisteten Workflows aus. Hierbei handelt es sich um die Workflows, die auf der Seite Dienstbibliothek verfügbar sind.
Workflow-Eingabeparameter auswählen	Wählen Sie einen verfügbaren Eingabeparameter in der Liste aus. Sie verknüpfen den Typ des vRealize Orchestrator-Workflows mit dem Typ der benutzerdefinierten Entitätsdefinition.
Zuordnung überprüfen	Überprüfen Sie die von Ihnen angegebenen Details und klicken Sie auf Fertig , um die Zuordnung abzuschließen.

Beispiel

Wenn Sie beispielsweise über eine benutzerdefinierte Entität vom Typ `SSH:Host` verfügen, können Sie sie mit dem Workflow `Add a Root Folder to SSH Host` verknüpfen, indem Sie den `sshHost`-Eingabeparameter auswählen, der dem Typ der benutzerdefinierten Entität entspricht.

Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entitätsdefinition

Sie können einen vRealize Orchestrator-Workflow aus der Liste der verknüpften Aktionen entfernen.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Verknüpfung der Aktion aufheben** aus.

Ein neues Dialogfeld wird geöffnet.

- 3 Wählen Sie den zu entfernenden Workflow aus und klicken Sie auf **Verknüpfung der Aktion aufheben**.

Der vRealize Orchestrator-Workflow ist nicht mehr mit der benutzerdefinierten Entität verknüpft.


Veröffentlichen einer benutzerdefinierten Entität

Sie müssen eine benutzerdefinierte Entität veröffentlichen, damit Benutzer aus anderen Mandanten oder Diensteanbietern Workflows mithilfe der benutzerdefinierten Entitätsinstanzen als Eingabeparameter ausführen können.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Veröffentlichen** aus.

Ein neues Dialogfeld wird geöffnet.

- 3 Geben Sie an, ob die benutzerdefinierte Entitätsdefinition für Diensteanbieter, alle Mandanten oder nur für ausgewählte Mandanten veröffentlicht werden soll.

- 4 Klicken Sie auf **Speichern**, um die Änderung zu bestätigen.

Die benutzerdefinierte Entitätsdefinition steht den ausgewählten Gruppen nun zur Verfügung.

Löschen einer benutzerdefinierten Entität

Sie können eine benutzerdefinierte Entitätsdefinition löschen, wenn die benutzerdefinierte Entität nicht mehr verwendet wird, nicht ordnungsgemäß konfiguriert wurde oder der vRealize Orchestrator-Typ einer anderen benutzerdefinierten Entität zugeordnet werden soll.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Benutzerdefinierte Entität“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Bibliotheken** und wählen Sie dann unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Löschen** aus.
- 3 Bestätigen Sie den Löschvorgang.

Die benutzerdefinierte Entität wird aus der Kartenansicht entfernt.