

Handbuch für das VMware Cloud Director-Mandantenportal

Geändert am 4. April 2021
VMware Cloud Director 10.2

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 © 2017-2021 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Handbuch für das VMware Cloud Director™-Mandantenportal 11

1 Erste Schritte mit dem VMware Cloud Director-Mandantenportal 13

- Grundlegendes zu VMware Cloud Director™ 13
- Anmelden beim VMware Cloud Director-Mandantenportal 15
- Rollen und Rechte für das VMware Cloud Director-Mandantenportal 15
- Verwenden des VMware Cloud Director-Mandantenportals 16
- Verwenden der globalen VMware Cloud Director-Suche 17
- Verwenden der VMware Cloud Director-Schnellsuche 18
- Anzeigen von Aufgaben 19
- Beenden einer in Bearbeitung befindlichen Aufgabe 20
- Anzeigen von Ereignissen 21
- Festlegen der Benutzereinstellungen 22

2 Arbeiten mit virtuellen Maschinen 23

- Architektur von virtuellen Maschinen 24
- Verschlüsselung virtueller Maschinen 25
- Anzeigen von virtuellen Maschinen 26
- Erstellen einer neuen eigenständigen virtuellen Maschine 27
- Fast Provisioning virtueller Maschinen 29
- Öffnen der Konsole einer virtuellen Maschine 29
 - Installieren von VMware Remote Console auf einem Client 29
 - Öffnen einer Remote-Konsole für die virtuelle Maschine 30
 - Öffnen einer Webkonsole 31
- Ausführen von Energievorgängen auf virtuellen Maschinen 32
 - Einschalten einer virtuellen Maschine 32
 - Ausschalten einer virtuellen Maschine 33
 - Herunterfahren eines Gastbetriebssystems 33
 - Zurücksetzen einer virtuellen Maschine 34
 - Anhalten einer virtuellen Maschine 34
 - Verwerfen des Status „Angehalten“ einer virtuellen Maschine 35
 - Einschalten mehrerer VMs 35
 - Ausschalten mehrerer virtueller Maschinen 36
 - Verwerfen des Status „Angehalten“ mehrerer virtueller Maschinen 36
 - Zurücksetzen mehrerer virtueller Maschinen 36
- Installieren von VMware Tools in einer virtuellen Maschine 37
- Ausführen eines Upgrades der virtuellen Hardwareversion für eine virtuelle Maschine 38
- Bearbeiten der Eigenschaften von virtuellen Maschinen 39

Ändern der allgemeinen Eigenschaften einer virtuellen Maschine	39
Ändern der Hardwareeigenschaften einer virtuellen Maschine	40
Ändern der Eigenschaften für die Gastbetriebssystem-Anpassung einer virtuellen Maschine	43
Ändern der erweiterten Eigenschaften einer virtuellen Maschine	48
Medium einlegen	51
Medium auswerfen	51
Kopieren einer virtuellen Maschine in eine andere vApp	52
Verschieben einer virtuellen Maschine in eine andere vApp	53
Affinität und Anti-Affinität virtueller Maschinen	54
Anzeigen von Affinitäts- und Anti-Affinitätsregeln	54
Erstellen einer Affinitätsregel	55
Erstellen einer Anti-Affinitätsregel	56
Bearbeiten einer Affinitäts- oder Anti-Affinitätsregel	56
Löschen einer Affinitäts- oder Anti-Affinitätsregel	57
Überwachen von virtuellen Maschinen	57
Arbeiten mit Snapshots	59
Erstellen eines Snapshots einer virtuellen Maschine	59
Zurücksetzen einer virtuellen Maschine auf einen Snapshot	60
Entfernen eines Snapshots einer virtuellen Maschine	61
Verlängern des Lease einer virtuellen Maschine	61
Löschen einer virtuellen Maschine	62
Automatische Skalierungsgruppen	62
Erstellen einer Skalierungsgruppe	63
Hinzufügen einer Regel für die automatische Skalierung	64

3 Arbeiten mit vApps 66

Anzeigen von vApps	67
Erstellen einer neuen vApp	67
Erstellen einer vApp von einem OVF-Paket aus	70
Hinzufügen einer vApp aus einem Katalog	72
Erstellen einer vApp aus einer vApp-Vorlage	74
Importieren einer virtuellen Maschine aus vCenter Server als vApp	76
Ausführen von Energievorgängen auf vApps	77
Einschalten einer vApp	77
Ausschalten einer vApp	77
Zurücksetzen einer vApp	78
Anhalten einer vApp	78
Verwerfen des Zustands „Angehalten“ einer vApp	79
Einschalten mehrerer vApps	79
Ausschalten mehrerer vApps	80
Verwerfen des Zustands „Angehalten“ von mehreren vApps	80

Zurücksetzen mehrerer vApps	81
Anhalten mehrerer vApps	81
Öffnen einer vApp	82
vApp-Eigenschaften bearbeiten	82
Bearbeiten der allgemeinen Eigenschaften der vApp	82
Bearbeiten der Start- und Beendigungsreihenfolge von virtuellen Maschinen in einer vApp	83
Bearbeiten der Gasteigenschaften einer vApp	84
Freigeben einer vApp	85
Anzeigen eines vApp-Netzwerkdigramms	86
Arbeiten mit Netzwerken in einer vApp	87
Anzeigen von vApp-Netzwerken	88
Fencing eines vApp-Netzwerks	88
Hinzufügen eines Netzwerks zu einer vApp	89
Konfigurieren von Netzwerkdiensten für ein vApp-Netzwerk	90
Löschen eines vApp-Netzwerks	98
Arbeiten mit Snapshots	99
Erstellen eines Snapshots einer vApp	99
Zurücksetzen einer vApp auf einen Snapshot	100
Entfernen eines Snapshots einer vApp	101
Erstellen von Snapshots mehrerer vApps	101
Entfernen der Snapshots mehrerer vApps	102
Wiederherstellen von Snapshots mehrerer vApps	102
Ändern des Besitzers einer vApp	103
Verschieben einer vApp in ein anderes virtuelles Datacenter	103
Kopieren einer beendeten vApp in ein anderes virtuelles Datacenter	104
Kopieren einer eingeschalteten vApp	105
Hinzufügen einer virtuellen Maschine zu einer vApp	106
Speichern einer vApp als vApp-Vorlage in einem Katalog	107
Herunterladen einer vApp als OVF-Paket	108
Verlängern eines vApp-Lease	109
Löschen einer vApp	110
Löschen mehrerer vApps	110

4 Arbeiten mit Kubernetes-Clustern 112

Hinzufügen einer Kubernetes-Richtlinie des Organisations-VDC	113
Bearbeiten einer Kubernetes-Richtlinie des Organisations-VDC	115
Erstellen eines Tanzu Kubernetes-Clusters	116
Erstellen eines nativen Kubernetes-Clusters	118
Erstellen eines VMware Tanzu Kubernetes Grid Integrated Edition-Clusters	120
Konfigurieren des externen Zugriffs auf einen Dienst in einem Tanzu Kubernetes-Cluster	121

5 Arbeiten mit Netzwerken 124

Verwalten von VDC-Organisationsnetzwerken 127

- Anzeigen der verfügbaren VDC-Organisationsnetzwerke 129
- Hinzufügen eines isolierten VDC-Organisationsnetzwerks 129
- Hinzufügen eines VDC-Organisationsnetzwerks mit Routing 131
- Hinzufügen eines direkten VDC-Organisationsnetzwerks 134
- Hinzufügen eines VDC-Organisationsnetzwerks mit einem importierten logischen NSX-T Data Center-Switch 134
- Bearbeiten der allgemeinen Einstellungen eines VDC-Organisationsnetzwerks 135
- Verbinden eines VDC-Organisationsnetzwerks mit einem Edge-Gateway 136
- Trennen eines VDC-Organisationsnetzwerks von einem Edge-Gateway 137
- Konvertieren der Schnittstelle eines VDC-Organisationsnetzwerks mit Routing 137
- Anzeigen der für ein VDC-Organisationsnetzwerk verwendeten IP-Adressen 138
- Hinzufügen von IP-Adressen zum IP-Pool eines VDC-Organisationsnetzwerks 139
- Bearbeiten oder Entfernen von IP-Bereichen, die in einem VDC-Organisationsnetzwerk verwendet werden 140
- Bearbeiten der DNS-Einstellungen eines VDC-Organisationsnetzwerks 140
- Konfigurieren von DHCP-Einstellungen für ein isoliertes VDC-Organisationsnetzwerk 141
- Hinzufügen eines DHCP-Pools zu einem gerouteten VDC-Organisationsnetzwerk, das von NSX-T Data Center gestützt wird 142
- Bearbeiten oder Löschen eines vorhandenen DHCP-Pools für ein isoliertes VDC-Organisationsnetzwerk, das von NSX Data Center for vSphere gestützt wird 142
- Zurücksetzen eines VDC-Organisationsnetzwerks 143
- Löschen eines VDC-Organisationsnetzwerks 144

Verwalten von Datacenter-Gruppennetzwerken mit NSX-T Data Center 144

- Verwalten von Datacenter-Gruppen mit NSX-T Data Center als Typ des Netzanbieters 145
- Verwenden einer Distributed Firewall in einer Datacenter-Gruppe mit NSX-T Data Center als Typ des Netzanbieters 147
- Verwalten von Datacenter-Gruppennetzwerken mit NSX-T Data Center als Typ des Netzanbieters 153
- Verwalten von Egress-Punkten für Datacentergruppen mit dem NSX-T Data Center als Typ des Netzanbieters 159

Verwalten von Datacenter-Gruppennetzwerken mit NSX Data Center for vSphere 161

- Verwalten von Datacenter-Gruppen mit NSX Data Center for vSphere als Typ des Netzanbieters 163
- Verwalten der von NSX Data Center for vSphere-gestützten Datacenter-Gruppennetzwerke 178

Verwalten von NSX Data Center for vSphere-Edge-Gateways-Diensten 180

- Erste Schritte mit erweiterten VMware Cloud Director-Netzwerken mit NSX Data Center for vSphere 181
- Konfiguration der Mandanten-Firewall mit NSX Data Center for vSphere 181
- Verwalten von DHCP für NSX Data Center for vSphere-Edge-Gateways 194
- Verwalten der Netzwerkadressübersetzung auf einem NSX Data Center for vSphere-Edge-Gateway 199

Erweiterte Routing-Konfiguration für NSX Data Center for vSphere-Edge-Gateways	203
Lastenausgleich mit NSX Data Center for vSphere	213
Konfigurieren des sicheren Zugriffs mithilfe von VPN auf einem NSX Data Center for vSphere-Edge-Gateway	228
SSL-Zertifikatsverwaltung auf einem NSX Data Center for vSphere-Edge-Gateway	258
Benutzerdefinierte Gruppierungsobjekte für NSX Data Center for vSphere-Edge-Gateways	266
Statistiken und Protokolle für ein NSX Data Center for vSphere-Edge-Gateway	269
Aktivieren des SSH-Befehlszeilenzugriffs über ein NSX Data Center for vSphere-Edge-Gateway	271
Arbeiten mit Sicherheits-Tags für NSX Data Center for vSphere-Edge-Gateways	272
Arbeiten mit Sicherheitsgruppen für NSX Data Center for vSphere-Edge-Gateways	277
Verwalten von NSX-T Data Center-Edge-Gateways	281
Hinzufügen eines IP Set zu einem NSX-T Data Center-Edge-Gateway	281
Hinzufügen einer Firewallregel für NSX-T Data Center Edge-Gateways	282
Hinzufügen einer SNAT- oder DNAT-Regel zu einem NSX-T-Edge-Gateway	283
Konfigurieren eines DNS-Weiterleitungsdiensts auf einem NSX-T-Edge-Gateway	287
Erstellen von benutzerdefinierten Anwendungsportprofilen	287
Richtlinienbasiertes IPSec-VPN für NSX-T Data Center-Edge-Gateways	288
Konfigurieren dedizierter externer Netzwerkdienste	291
Arbeiten mit NSX Advanced Load Balancing	297
6 Verwenden benannter Festplatten und Überprüfen von Speicherrichtlinien	305
Erstellen und Verwenden benannter Festplatten	305
Erstellen einer benannten Festplatte	306
Bearbeiten einer benannten Festplatte	307
Anhängen einer benannten Festplatte an eine virtuelle Maschine	307
Löschen einer benannten Festplatte	308
Überprüfen der Eigenschaften von Speicherrichtlinien	308
7 Überprüfen und Bearbeiten der Eigenschaften von virtuellen Datencentern	310
Überprüfen der Eigenschaften von virtuellen Datencentern	310
Überprüfen der Metadaten des virtuellen Datencenters	311
Begrenzen des Zugriffs auf ein Organisations-VDC auf bestimmte Benutzer und Gruppen in Ihrer Organisation	311
8 Arbeiten mit dedizierten vCenter Server-Instanzen, -Endpoints und -Proxys	313
Verwenden von Chrome Browser Extension for VMware Cloud Director	314
Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen	314
Anmelden bei der Benutzeroberfläche einer Komponente mithilfe eines Endpoints	315
9 Arbeiten mit vApp-Vorlagen	317
Anzeigen einer vApp-Vorlage	317

	vApp-Vorlage aus einer OVF-Datei erstellen	318
	Importieren einer virtuellen Maschine aus vCenter Server als vApp-Vorlage	319
	Zuweisen einer VM-Platzierungsrichtlinie und einer VM-Größenrichtlinie zu einer vApp-Vorlage	320
	vApp-Vorlage herunterladen	321
	Löschen einer vApp-Vorlage	321
10	Arbeiten mit Mediendateien	323
	Hochladen von Mediendateien	323
	Löschen einer Mediendatei	324
	Herunterladen einer Mediendatei	324
11	Arbeiten mit Katalogen	326
	Anzeigen von Katalogen	327
	Erstellen eines Katalogs	327
	Freigeben eines Katalogs	328
	Löschen eines Katalogs	329
	Ändern des Besitzers eines Katalogs	330
	Verwalten von Metadaten für einen Katalog	330
	Veröffentlichen eines Katalogs	331
	Abonnieren eines externen Katalogs	332
	Aktualisieren der Speicherort-URL und des Kennworts für einen abonnierten Katalog	333
	Synchronisieren eines abonnierten Katalogs	333
12	Arbeiten mit VDC-Organisationsvorlagen	335
	Anzeigen verfügbarer Vorlagen für virtuelle Datacenter	335
	Instanzieren eines virtuellen Datacenters anhand einer Vorlage	336
13	Verwalten von Benutzern, Gruppen und Rollen	338
	Verwalten von Benutzern	338
	Erstellen eines Benutzers	338
	Benutzer importieren	340
	Ändern eines Benutzers	341
	Deaktivieren oder Aktivieren eines Benutzerkontos	342
	Löschen eines Benutzers	342
	Entsperren eines gesperrten Benutzerkontos	343
	Verwalten der Ressourcenkontingente eines Benutzers	343
	Verwalten von Gruppen	344
	Importieren einer Gruppe	344
	Löschen einer Gruppe	345
	Bearbeiten einer Gruppe	346
	Verwalten der Ressourcenkontingente einer Gruppe	346

Rollen und Rechte	347
Vordefinierte Rollen und ihre Rechte	347
Rechte in vordefinierten globalen Mandantenrollen	350
Erstellen einer benutzerdefinierten Mandantenrolle	355
Bearbeiten einer benutzerdefinierten Mandantenrolle	356
Löschen einer Rolle	357
14 Konfigurieren von Identitätsanbietern	358
Aktivieren der Verwendung eines SAML-Identitätsanbieter für die Organisation	358
Bearbeiten von LDAP-Einstellungen für Ihre Organisation	360
Konfigurieren, Testen und Synchronisieren einer LDAP-Verbindung	361
15 Verwalten von Zertifikaten	364
Importieren vertrauenswürdiger Zertifikate	364
Importieren von Zertifikaten in die Zertifikatsbibliothek	365
16 Verwalten Ihrer Organisation	367
Bearbeiten des Namens und der Beschreibung der Organisation	367
Ändern der E-Mail-Einstellungen	368
Testen der SMTP-Einstellungen	369
Ändern der Domäneneinstellungen für die virtuellen Maschinen in Ihrer Organisation	369
Arbeiten mit mehreren Sites	370
Konfigurieren und Verwalten von Multisite-Bereitstellungen	370
Wissenswertes über Leases	372
Ändern der Richtlinien für vApp- und vApp-Vorlage-Leases innerhalb der Organisation	372
Ändern des Kennworts und der Richtlinien für Benutzerkonten in Ihrer Organisation	373
Erstellen eines Dashboard für Sicherheitswarnungen	374
17 Arbeiten mit der Dienstbibliothek	376
Auffinden eines Diensts	376
Ausführen eines Diensts	377
18 Verwalten definierter Entitäten	378
Arbeiten mit benutzerdefinierten Entitätsdefinitionen	381
Auffinden einer benutzerdefinierten Entität	381
Bearbeiten einer benutzerdefinierten Entitätsdefinition	381
Hinzufügen einer benutzerdefinierten Entitätsdefinition	382
Benutzerdefinierte Entitätsinstanzen	383
Verknüpfen einer Aktion mit einer benutzerdefinierten Entität	384
Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entitätsdefinition	385
Veröffentlichen einer benutzerdefinierten Entität	385

[Löschen einer benutzerdefinierten Entität](#) 386

Handbuch für das VMware Cloud Director™-Mandantenportal

Das *VMware Cloud Director™-Mandantenportal-Handbuch* enthält Informationen zur Verwendung des VMware Cloud 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 VMware Cloud Director-Umgebung bereitgestellt werden. Mit dem VMware Cloud 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 VMware Cloud 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.

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>.

Nutzungsbedingungen

VMware berechtigt Sie dazu, dieses Mandanten-Benutzerhandbuch (das „Handbuch“) nach Bedarf zu ändern, um es an Ihre Betriebsvorgänge anzupassen, und das geänderte Handbuch zu vervielfältigen, um es dann an Ihre Kunden zu verteilen. Sie dürfen Ihren Kunden keine Gebühr für den Zugriff auf das geänderte Handbuch in Rechnung stellen. SIE ERKENNEN AN, DASS IHNEN DAS HANDBUCH KOSTENLOS, OHNE JEGliche GARANTIE UND NUR FÜR DEN OBEN BESCHRIEBENEN ZWECK ZUR VERFÜGUNG GESTELLT WIRD. DEMENTSPRECHEND DARF DIE GESAMTHAFTUNG VON VMWARE UND SEINER LIEFERANTEN, DIE SICH AUS DER BEREITSTELLUNG DES ZUGANGS ZUM HANDBUCH ERGIBT ODER DAMIT ZUSAMMENHÄNGT, 100 DOLLAR NICHT ÜBERSCHREITEN. IN KEINEM FALL HAFTEN VMWARE ODER SEINE LIEFERANTEN FÜR INDIREKTE, UNBEABSICHTIGTE, BESONDERE

SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN DURCH GEWINNAUSFÄLLE, BETRIEBSUNTERBRECHUNGEN ODER VERLUST VON GESCHÄFTSINFORMATIONEN), UNABHÄNGIG VON DER URSACHE UND BELIEBIGER THEORETISCHEN HAFTBARKEIT, AUCH WENN VMWARE ODER SEINE LIEFERANTEN AUF DIE MÖGLICHKEIT EINES SOLCHEN SCHADENS AUFMERKSAM GEMACHT WURDEN. DIESE BESCHRÄNKUNGEN GELTEN SELBST DANN, WENN EIN WESENTLICHER ZWECK DURCH EINGESCHRÄNKTE RECHTSMITTEL NICHT ERFÜLLT WIRD.

Erste Schritte mit dem VMware Cloud 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 Cloud Director™
- Anmelden beim VMware Cloud Director-Mandantenportal
- Rollen und Rechte für das VMware Cloud Director-Mandantenportal
- Verwenden des VMware Cloud Director-Mandantenportals
- Verwenden der globalen VMware Cloud Director-Suche
- Verwenden der VMware Cloud Director-Schnellsuche
- Anzeigen von Aufgaben
- Beenden einer in Bearbeitung befindlichen Aufgabe
- Anzeigen von Ereignissen
- Festlegen der Benutzereinstellungen

Grundlegendes zu VMware Cloud Director™

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.

Dedizierte vCenter Server-Instanzen (SDDCs) und -Proxys

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

Anmelden beim VMware Cloud Director-Mandantenportal

Sie können auf das VMware Cloud 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 *VMware Cloud Director-Versionshinweise*.

Verfahren

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

Rollen und Rechte für das VMware Cloud Director-Mandantenportal

VMware Cloud Director enthält einen vorkonfigurierten Satz an Benutzerrollen und deren Rechte. Die Rollen für den Zugriff auf das VMware Cloud 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 VMware Cloud Director-Mandantenportals

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

Der Dashboard-Bildschirm **Datencenter** ist Teil der Multisite-Funktion von VMware Cloud 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 VMware Cloud 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.

In der oberen Navigationsleiste können Sie zu den verschiedenen Menüelementen navigieren.

Menüelement	Beschreibung
Datencenter	Leitet Sie zu den Ressourcen Virtuelles Datencenter , Datencentergruppen und Dedizierte vSphere-Datencenter in Ihrer Organisation.
Virtuelles Datencenter	Leitet Sie zum Bildschirm Virtuelles Datencenter , in dem die virtuellen Datencenter innerhalb der Organisation angezeigt werden.
Dedizierte vSphere-Datencenter	Leitet Sie zu dem Bildschirm, auf dem die dedizierten vSphere-Datencenter angezeigt werden, die Ihr Dienstanbieter in Ihrer Organisation veröffentlicht hat.
Anwendungen	Leitet Sie zu den Ressourcen Virtuelle Anwendungen und Virtuelle Maschinen in Ihrer Organisation.
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.
Netzwerk	Leitet Sie zu den Netzwerken, Edge-Gateways und Datencenter-Gruppen in Ihrer Organisation.
Administration	Leitet Sie zu den Konfigurationsbildschirmen Zugriffssteuerung und Identitätsanbieter sowie zu den allgemeinen, E-Mail-, Gastpersonalisierungs-, Metadaten-, Multisite- und Richtlinienereinstellungen für Ihre Organisation.
Überwachen	Leitet Sie zu den Bildschirmen Aufgaben und Ereignisse . Im Bildschirm Aufgaben werden die von VMware Cloud Director gemeldeten Aufgaben und im Bildschirm Ereignisse die von VMware Cloud Director gemeldeten Ereignisse angezeigt.

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

Verwenden der globalen VMware Cloud Director-Suche

Mithilfe der globalen VMware Cloud 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 VMware Cloud 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.

Verwenden der VMware Cloud Director-Schnellsuche

Sie können die VMware Cloud Director-Schnellsuche verwenden, um nach Bildschirmen, Entitäten und Aktionen zu suchen. Die Ergebnisse richten sich nach Ihrer Position auf der Benutzeroberfläche.

Die Ergebnisse richten sich nach dem Kontext und den verfügbaren Aktionen für eine bestimmte Entität sowie danach, ob eine Entität ausgewählt wurde. Die Suchergebnisse werden in Abschnitten zusammengefasst.

- Globale Navigation: Die Ergebnisse in diesem Abschnitt beziehen sich nicht auf eine bestimmte Entität, z. B. Edge-Gateways, LDAP, Aufgaben, vertrauenswürdige Zertifikate, virtuelle Maschinen usw. Sie können diese Ergebnisse unabhängig von Ihrer Position auf der Benutzeroberfläche abrufen.

- **Kontextbezogene Navigation:** Die Ergebnisse in diesem Abschnitt richten sich nach der ausgewählten Entität auf der Benutzeroberfläche. Beispiel: vApp-spezifische Ansichten wie VMs, Netzwerkdiagramm usw. Wenn Sie eine Entität wie eine vApp auswählen, werden in der Suche sowohl die globale als auch die Kontextnavigation sowie alle Aktionen angezeigt, die unter Umständen auf die Entität angewendet werden können.
- **Kontextbezogene Aktionen:** Die Ergebnisse in diesem Abschnitt richten sich nach der ausgewählten Entität auf der Benutzeroberfläche. Abhängig von Ihrer Position auf der Benutzeroberfläche und der ausgewählten Entität können Sie mithilfe der Schnellsuche eine auf die Entität bezogene Aktion durchführen. Beispielsweise werden bei der Suche in der Detailansicht einer virtuellen Maschine Ergebnisse aus den globalen Ansichten, den Kontextansichten und den Aktionen angezeigt, die Sie für die ausgewählte VM durchführen können.
- **Entitätsuche nach Name:** Wenn Sie eine Liste der Entitäten anzeigen, können die Suchergebnisse auch Namen von Entitäten desselben Typs wie die in der Liste aufgeführten enthalten. Wenn Sie beispielsweise eine Liste mit VMs anzeigen, werden in den Suchergebnissen globale Navigationsübereinstimmungen und übereinstimmende Namen von VMs angezeigt. Enthält die angezeigte Liste mehr als eine Seite mit Entitäten, wird bei der Suche die vollständige Liste der Entitäten überprüft. Unter Umständen wird dabei ein Name ermittelt, der auf der aktuellen Seite nicht angezeigt wird.

Verfahren

1 Öffnen Sie das Fenster **Schnellsuche**.

- Klicken Sie in der oberen Navigationsleiste auf das Menü **Hilfe** und wählen Sie **Schnellsuche** aus.
- Drücken Sie je nach Betriebssystem STRG+. oder CMD+.

2 Geben Sie Suchkriterien ein.

3 Durchsuchen Sie die Ergebnisse und wählen Sie eine Option aus oder führen Sie durch Klicken oder Drücken der Eingabetaste eine Aktion aus.

Sie können die Pfeiltasten (nach oben und nach unten) verwenden, um die Suchergebnisse zu durchsuchen.

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 Klicken Sie in der oberen Navigationsleiste auf **Überwachung** und **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.cloud</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 Klicken Sie in der oberen Navigationsleiste auf **Überwachung** und **Ereignisse**.
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> .

Detail	Beschreibung
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“ starten vdcUpdateVapp</i> .
Status	Der Status des Ereignisses, z. B. „Erfolgreich“ oder „Fehlgeschlagen“
Dienst-Namespace	Der Dienstname, z. B. <i>com.vmware.cloud</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

Festlegen der Benutzereinstellungen

Sie können bestimmte Voreinstellungen für die Anzeige und für Systemwarnungen festlegen, die bei jeder Anmeldung beim System neu geladen werden.

Weitere Informationen über Leases finden Sie unter [Wissenswertes über Leases](#).

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf Ihren Benutzernamen und wählen Sie **Benutzereinstellungen** aus.
- 2 Wählen Sie die Seite aus, die beim Anmelden angezeigt werden soll.
 - a Aktivieren Sie die Optionsschaltfläche neben **Startseite** und klicken Sie auf **Bearbeiten**.
 - b Wählen Sie eine Option im Dropdown-Menü aus und klicken Sie auf **Speichern**.
- 3 Konfigurieren Sie eine E-Mail-Benachrichtigung für den Ablauf von Laufzeit-Leases.
 - a Aktivieren Sie das Optionsfeld neben **Warnzeit für Bereitstellungs-Lease** und klicken Sie auf **Bearbeiten**.
 - b Geben Sie einen Wert in Sekunden ein und klicken Sie auf **Speichern**.
- 4 Konfigurieren Sie eine E-Mail-Benachrichtigung für den Ablauf von Speicher-Leases.
 - a Aktivieren Sie das Optionsfeld neben **Warnzeit für Speicher-Lease** und klicken Sie auf **Bearbeiten**.
 - b Geben Sie einen Wert in Sekunden ein und klicken Sie auf **Speichern**.

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 VMware Cloud 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 VMware Cloud 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](#)
- [Verschlüsselung virtueller Maschinen](#)
- [Anzeigen von virtuellen Maschinen](#)
- [Erstellen einer neuen eigenständigen virtuellen Maschine](#)
- [Fast Provisioning virtueller Maschinen](#)
- [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](#)

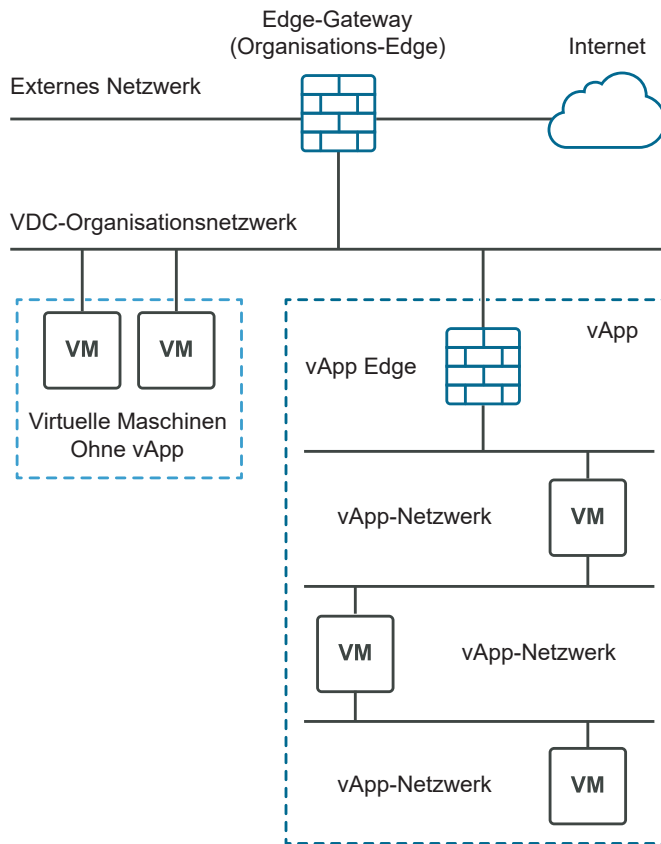
- [Medium einlegen](#)
- [Medium auswerfen](#)
- [Kopieren einer virtuellen Maschine in eine andere vApp](#)
- [Verschieben einer virtuellen Maschine in eine andere vApp](#)
- [Affinität und Anti-Affinität virtueller Maschinen](#)
- [Überwachen von virtuellen Maschinen](#)
- [Arbeiten mit Snapshots](#)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

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

Verschlüsselung virtueller Maschinen

Ab VMware Cloud Director 10.1 können Sie die Sicherheit Ihrer Daten mithilfe der VM-Verschlüsselung verbessern. Sie können VMs und Festplatten verschlüsseln, indem Sie sie Speicherrichtlinien zuordnen, die über die VM-Verschlüsselungsfunktion verfügen.

Bei der Verschlüsselung wird nicht nur Ihre virtuelle Maschine geschützt, sondern auch die Festplatten und andere Dateien der virtuellen Maschine. Sie können die Funktionen von Speicherrichtlinien und den Verschlüsselungsstatus von VMs und Festplatten in der API und der Benutzeroberfläche anzeigen. Sie können alle in der jeweiligen vCenter Server-Version unterstützten Vorgänge auf verschlüsselten VMs und Festplatten durchführen.

Wenn das Organisations-VDC über eine Speicherrichtlinie mit aktivierter VM-Verschlüsselung verfügt, können Sie VMs und Festplatten verschlüsseln. Weitere Informationen finden Sie im Abschnitt [Aktivieren der VM-Verschlüsselung für Speicherrichtlinien eines Organisations-VDC](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*. Um eine VM oder Festplatte zu verschlüsseln, ordnen Sie sie einer Speicherrichtlinie mit aktivierter VM-Verschlüsselung zu. Informationen zu virtuellen Maschinen finden Sie unter [Erstellen einer neuen eigenständigen virtuellen Maschine](#) oder [Ändern der allgemeinen Eigenschaften einer virtuellen Maschine](#).

Informationen zu benannten Festplatten finden Sie unter [Erstellen einer benannten Festplatte](#) oder [Bearbeiten einer benannten Festplatte](#). Um eine VM oder Festplatte zu entschlüsseln, ordnen Sie diese VM oder Festplatte einer Speicherrichtlinie zu, für die die Verschlüsselung nicht aktiviert ist.

Einschränkungen bei der VM-Verschlüsselung

Die folgenden Aktionen werden in VMware Cloud Director nicht unterstützt.

- Verschlüsseln oder Entschlüsseln einer eingeschalteten VM oder ihrer Festplatten
- Exportieren einer OVF-Datei einer verschlüsselten VM
- Verschlüsseln und Entschlüsseln der Festplatten einer VM mit einem Snapshot, wenn die Festplatten Teil des Snapshots sind
- Entschlüsseln einer VM, wenn ihre Festplatte einer verschlüsselten Richtlinie unterliegt
- Hinzufügen einer verschlüsselten Festplatte zu einer nicht verschlüsselten VM
- Verschlüsseln einer vorhandenen Festplatte auf einer nicht verschlüsselten VM
- Hinzufügen einer verschlüsselten benannten Festplatte zu einer nicht verschlüsselten VM
- Erstellen eines verschlüsselten Linked Clone
- Verschlüsseln einer Linked Clone-VM oder ihrer Festplatten
- Instanzieren, Verschieben oder Klonen von VMs über vCenter Server-Instanzen hinweg, wenn die Quell-VM verschlüsselt ist

Hinweis Wenn in einem schnell bereitgestellten Organisations-VDC die Quell- oder Ziel-VM verschlüsselt ist und Sie einen Klon erstellen möchten, erstellt VMware Cloud Director immer einen vollständigen Klon.

Identifizieren einer VM-Verschlüsselungsspeicherfunktion


Standardmäßig verfügen **Systemadministratoren** und **Organisationsadministratoren** über die erforderlichen Rechte zum Anzeigen der Speicherfunktionen des Organisations-VDC und des Verschlüsselungsstatus von VMs und Festplatten. **vApp-Autoren** können den Verschlüsselungsstatus einer virtuellen Maschine und ihrer Festplatten auf der Seite **Details** der virtuellen Maschine anzeigen. Weitere Informationen zu diesen Rollen und Rechten finden Sie unter [Vordefinierte Rollen und ihre Rechte](#).

Anzeigen 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Wählen Sie aus folgenden Optionen aus.

- Um die virtuellen Maschinen in einer Rasteransicht anzuzeigen, klicken Sie auf .

- Um die virtuellen Maschinen in einer Kartenansicht anzuzeigen, klicken Sie auf .

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

- 3 (Optional) Ordnen Sie die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 4 (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.

- 5 Um auf die Schnittstelle für das Gastbetriebssystem der virtuellen Maschine zuzugreifen, klicken Sie in der oberen rechten Ecke der Kartenansicht auf das Desktopsymbol:
- 6 Um die Details für eine virtuelle Maschine anzuzeigen und zu bearbeiten, klicken Sie auf **Details**.

Erstellen einer neuen eigenständigen virtuellen Maschine

Sie können eine neue eigenständige virtuelle Maschine erstellen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 3 Klicken Sie auf **Neue VM**.
- 4 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.

- 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> <ol style="list-style-type: none"> a Wählen Sie eine Betriebssystemfamilie und ein Betriebssystem aus. b (Optional) Wählen Sie ein Boot-Image aus. c (Optional) Wählen Sie eine VM-Platzierungsrichtlinie und eine VM-Größenrichtlinie aus. <p>Die Dropdown-Menüs für VM-Platzierungs- und -Größenrichtlinien werden nur angezeigt, wenn der Dienstanbieter solche Richtlinien für das Organisations-VDC veröffentlicht hat.</p> <ol style="list-style-type: none"> d (Optional) Wählen Sie die Größe der virtuellen Maschine aus den vordefinierten Größenoptionen aus oder klicken Sie auf Benutzerdefinierte Größenänderungsoptionen, um die Anzahl der virtuellen CPUs, Kerne pro Socket und Arbeitsspeichereinstellungen manuell einzugeben. <p>Wenn Sie eine VM-Größenrichtlinie auswählen, die die VM-Größe definiert, ist diese Option nicht sichtbar.</p> <p>Die vordefinierten Größen der virtuellen Maschinen sind: Klein, Mittel und Groß.</p> <ol 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> <ol style="list-style-type: none"> a Wählen Sie eine VM-Vorlage aus der Liste der verfügbaren Vorlagen aus. b (Optional) Wählen Sie eine VM-Platzierungsrichtlinie und eine VM-Größenrichtlinie aus. <p>Die Dropdown-Menüs für VM-Platzierungs- und -Größenrichtlinien werden nur angezeigt, wenn der Dienstanbieter solche Richtlinien für das Organisations-VDC veröffentlicht hat. Wenn der ausgewählten Vorlage Richtlinien zugewiesen wurden, sind Sie möglicherweise auf die vordefinierten Vorlagenrichtlinien beschränkt.</p> <ol style="list-style-type: none"> c (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. d 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.

Fast Provisioning virtueller Maschinen

Fast Provisioning spart Zeit, da verknüpfte Klone für Bereitstellungsvorgänge von virtuellen Maschinen verwendet werden.

Ein Linked Clone ist ein Duplikat einer virtuellen Maschine, das dieselbe virtuelle Festplatte wie das Original verwendet, wobei jedoch eine Kette von Delta-Festplatten erstellt und verwaltet wird, über die Änderungen zwischen dem Original und dem Klon verfolgt werden. Wenn Sie Fast Provisioning deaktivieren, resultieren alle Bereitstellungsvorgänge in vollständigen Klonen.

Ein Linked Clone darf nicht auf einem anderen vCenter Server-Datencenter oder -Datenspeicher als die ursprüngliche virtuelle Maschine vorhanden sein.

Wenn Sie eine VM mit Fast Provisioning bereitstellen, erstellt VMware Cloud Director eine virtuelle Schattenmaschine, um die Linked Clone-Erstellung über vCenter Server-Datencenter und -Datenspeicher hinweg für die virtuellen Maschinen zu unterstützen, die einer bestimmten vApp-Vorlage zugeordnet sind.

Eine virtuelle Schattenmaschine ist eine exakte Kopie der ursprünglichen virtuellen Maschine. Die virtuelle Schattenmaschine wird auf dem Datencenter und dem Datenspeicher erstellt, in dem der Linked Clone erstellt wird.

Wichtig Eine Vor-Ort-Konsolidierung einer schnell bereitgestellten VM wird auf Speichercontainern, die native Snapshots einsetzen, nicht unterstützt. VVOLs und VAAI-fähige Datenspeicher verwenden native Snapshots. Das heißt, schnell bereitgestellte VMs, die auf einem dieser Speichercontainer bereitgestellt werden, können nicht konsolidiert werden. Wenn Sie eine schnell bereitgestellte VM konsolidieren müssen, die auf einem VVOL oder einem VAAI-fähigen Datenspeicher bereitgestellt wurde, müssen Sie sie auf einen anderen Speichercontainer verschieben.

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 VMware Cloud 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 **Virtuelles Datencenter** im VMware Cloud Director Tenant Portal auf die Karte des virtuellen Datencenters, das Sie erkunden möchten. Wählen Sie eine virtuelle Maschine aus und wählen Sie im Menü **Aktionen** die Option **VMRC herunterladen** aus.

2 Führen Sie Ihre Plattforminstallation aus.

- Wenn Sie Windows verwenden, doppelklicken Sie auf das `.msi`-Installationsprogramm und folgen Sie den Bildschirmanweisungen.
- Wenn Sie Linux verwenden, melden Sie sich mit **root**-Rechten an, führen Sie das `.bundle`-Installationsprogramm aus und folgen Sie den Bildschirmanweisungen.
- Wenn Sie Mac OS verwenden, 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 VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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.

Einschalten mehrerer VMs

Sie können mehrere VMs gleichzeitig einschalten.

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.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die VMs aus, die Sie einschalten möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Einschalten** aus.
- 5 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Ausschalten mehrerer virtueller Maschinen

Sie können mehrere VMs gleichzeitig ausschalten.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die VMs aus, die Sie ausschalten möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Ausschalten** aus.
- 5 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Verwerfen des Status „Angehalten“ mehrerer virtueller Maschinen

Wenn sich mehrere VMs im Zustand „Angehalten“ befinden und Sie deren Nutzung nicht mehr fortsetzen müssen, können Sie den Zustand „Angehalten“ der VMs gleichzeitig verwerfen. Durch Verwerfen des Zustands „Angehalten“ wird der Speicher entfernt, und die VMs werden ausgeschaltet.

Voraussetzungen

Stellen Sie sicher, dass sich die VMs im angehaltenen Zustand befinden.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die VMs aus, für die Sie den Zustand „Angehalten“ verwerfen möchten.
- 4 Wählen Sie im Menü **Aktionen** den Befehl **Zustand „Angehalten“ verwerfen** aus.
- 5 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Zurücksetzen mehrerer virtueller Maschinen

Durch das gleichzeitige Zurücksetzen mehrerer VMs wird ihr Zustand (Arbeitsspeicher, Cache usw.) gelöscht, die VMs werden jedoch 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

Stellen Sie sicher, dass die VMs eingeschaltet sind.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die VMs aus, die Sie zurücksetzen möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Zurücksetzen** aus.
- 5 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Installieren von VMware Tools in einer virtuellen Maschine


VMware Cloud 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

- Stellen Sie sicher, dass die virtuelle Maschine eingeschaltet ist.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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.

VMware Cloud 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 VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.

- 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 **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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.

Option	Aktion
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.
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.

Verfahren

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

- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach an**.
- 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	<p>Bearbeiten Sie die Anzahl der CPUs.</p> <p>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.</p>
Kerne pro Socket	<p>Bearbeiten Sie die Kerne pro Socket.</p> <p>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.</p>
Offenlegen der hardwaregestützten CPU-Virtualisierung für ein Gastbetriebssystem	<p>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.</p>
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	<p>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.</p>
Hot-Add der virtuellen CPU	<p>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.</p>
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	<p>Zeigt die verfügbaren Wechselmedien an, beispielsweise angeschlossene CD/DVD- und Diskettenlaufwerke.</p>

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>
IOPS (E/A-Vorgänge pro Sekunde)	<p>Wählen Sie einen bestimmten IOPS-Wert für die Festplatte aus.</p> <p>Verwenden Sie diese Option, um die E/A-Vorgänge pro Festplatte pro Sekunde einzuschränken.</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>
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>. VMware Cloud Director unterstützt das Ändern von Netzwerkkarten virtueller Maschinen, während die virtuelle Maschine ausgeführt wird. Informationen zu unterstützten Netzwerkadapertypen finden Sie unter <http://kb.vmware.com/kb/1001805>.

Option	Beschreibung
Primärer Netzwerkadapter	<p>Wenn die primäre Netzwerkkarte ausgewählt ist, wird ein entsprechendes Kennzeichen angezeigt.</p> <p>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.</p>
Netzwerkadapter	Anzahl der Netzwerkadapter.
Verbunden	Aktivieren Sie das Kontrollkästchen, um einen Netzwerkadapter anzuschließen.
Netzwerk	Wählen Sie ein Netzwerk aus dem Dropdown-Menü.
IP-Modus	<p>Wählen Sie einen IP-Modus aus.</p> <p>Vorsicht Legen Sie den IP-Modus nicht auf Keine fest, wenn Sie ein Netzwerk ausgewählt haben, mit dem die Netzwerkkarte verbunden werden soll.</p> <ul style="list-style-type: none"> ■ Statisch – IP-Pool <p>Ruft eine statische IP-Adresse aus dem IP-Pool des Netzwerks ab.</p> ■ Statisch – Manuell <p>Ermöglicht Ihnen, eine bestimmte IP-Adresse manuell anzugeben. Wenn Sie diese Option auswählen, müssen Sie eine IP-Adresse in der Spalte IP-Adresse eingeben.</p> ■ DHCP <p>Ruft eine IP-Adresse aus einem DHCP-Server ab.</p>
MAC-Adresse	Wählen Sie im Dropdown-Menü aus, ob die MAC-Adresse beibehalten oder zurückgesetzt werden soll.

7 Klicken Sie auf **Speichern**.

Ändern der Eigenschaften für die Gastbetriebssystem-Anpassung einer virtuellen Maschine


Die Gastbetriebssystem-Anpassung in VMware Cloud 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 VMware Cloud Director-Servergruppe installieren. Weitere Informationen dazu finden Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.
- Das Anpassen von Linux-Gastbetriebssystemen setzt voraus, dass Perl auf dem Gastbetriebssystem installiert ist.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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. VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 3 Klicken Sie in der Karte der zu bearbeitenden virtuellen Maschine auf **Details**.
- 4 Klicken Sie auf **Erweitert** und **Bearbeiten**.
- 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 Arbeitsspeicherressource.
Maximum	Geben Sie eine Obergrenze für die Arbeitsspeicherreservierung an, die einer virtuellen Maschine zugewiesen werden kann.

- 9 Klicken Sie auf **Speichern**.


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 **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 Computername 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 VM verschieben, entfernt VMware Cloud Director die ursprüngliche VM aus der Quell-vApp.

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

Das Verschieben von VMs in verschiedene vApps basiert 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 derselben Organisation gehört. Das Organisations-VDC kann sich innerhalb desselben oder eines anderen Provider-VDC befinden.

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

- Stellen Sie sicher, dass Sie über die Rechte der Rolle **vApp-Autor** oder entsprechende Rechte verfügen.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 VM 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 ESXi-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.

Wenn die Affinitäts- oder Anti-Affinitätsregeln nicht erfüllt werden können, verhindert dies das Einschalten der virtuellen Maschinen, die der Regel hinzugefügt wurden.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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, die virtuellen 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 Lassen Sie das Kontrollkästchen **Erfordert** aktiviert.
Standardmäßig ist jede Affinitätsregel erforderlich. Dies bedeutet, dass die der Regel hinzugefügten virtuellen Maschinen nicht eingeschaltet werden, wenn die Regel nicht erfüllt werden kann.
- 6 Wählen Sie die virtuellen Maschinen aus, die Sie der Affinitätsregel hinzufügen möchten.
- 7 Klicken Sie auf **Speichern**.

Ergebnisse

VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 Lassen Sie das Kontrollkästchen **Erfordert** aktiviert.
Standardmäßig ist jede Anti-Affinitätsregel erforderlich. Dies bedeutet, dass die der Regel hinzugefügten virtuellen Maschinen nicht eingeschaltet werden, wenn die Regel nicht erfüllt werden kann.
- 6 Wählen Sie die virtuellen Maschinen aus, die der Anti-Affinitäts-Regel hinzugefügt werden sollen.
- 7 Klicken Sie auf **Speichern**.

Ergebnisse

VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 Lassen Sie das Kontrollkästchen **Erfordert** aktiviert.
 - 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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

VMware Cloud Director löscht die Affinitäts- oder Anti-Affinitätsregel.

Überwachen von virtuellen Maschinen


Wenn Ihr VMware Cloud 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 VMware Cloud Director-Administrator aktiviert wurde.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach an**.
- 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 Maschine 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 VMware Cloud 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

Sicherstellen, dass die virtuelle Maschine nicht mit einer benannten Festplatte verbunden ist.

Hinweis Snapshots erfassen keine NIC-Konfigurationen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.

- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 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.

Automatische Skalierungsgruppen

Ab VMware Cloud Director 10.2.2 können Sie Anwendungen in Abhängigkeit von der aktuellen CPU- und Speichernutzung automatisch skalieren.

Informationen zur Konfiguration der Lösung für die automatische Skalierung finden Sie unter [Automatische Skalierungsgruppen](#) im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

Je nach den vordefinierten Kriterien für die CPU- und Arbeitsspeichernutzung kann VMware Cloud Director die Anzahl der VMs in einer ausgewählten Skalierungsgruppe automatisch hoch- oder herunterskalieren. Zum Ausgleichen der Serverlast, die Sie zum Ausführen derselben Anwendung konfigurieren, können Sie VMware NSX Advanced Load Balancer (Avi Networks) verwenden.

Die Rollen **Systemadministrator** und **Organisationsadministrator** haben vollständige Kontrolle über die VMs in den Skalierungsgruppen. Die anderen globalen Mandantenrollen können die VMs anzeigen und auf die Web-Konsole der VM zugreifen. Betriebsvorgänge können jedoch weder gelöscht, bearbeitet noch durchgeführt werden.

Wenn Sie eine Skalierungsgruppe entfernen, löscht VMware Cloud Director keine der vorhandenen VMs in der Skalierungsgruppe.

Erstellen einer Skalierungsgruppe

Ab VMware Cloud Director 10.2.2 kann Ihnen Ihr Dienstleister Berechtigungen zum Erstellen von Skalierungsgruppen gewähren. Die Anzahl der VMs in einer Skalierungsgruppe ändert sich je nach den von Ihnen festgelegten Bedingungen automatisch.

Sie können auch auf Skalierungsgruppen aus einem ausgewählten Organisations-VDC (Virtual Data Center) zugreifen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Anwendungen** aus und klicken Sie auf die Registerkarte **Skalierungsgruppen**.
- 2 Klicken Sie auf **Neue Skalierungsgruppe**.
- 3 Wählen Sie ein Organisations-VDC aus, in dem die Skalierungsgruppe erstellt werden soll.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die neue Skalierungsgruppe ein.
- 5 Wählen Sie die Mindest- und Höchstzahl an VMs aus, auf die die Gruppe skaliert werden soll, und klicken Sie auf **Weiter**.
- 6 Wählen Sie eine VM-Vorlage für die VMs in der Skalierungsgruppe sowie eine Speicherrichtlinie aus und klicken Sie auf **Weiter**.
- 7 Wählen Sie ein Netzwerk für die Skalierungsgruppe aus.
 - Wenn Ihr VDC von NSX-T Data Center gestützt wird, wählen Sie einen Lastausgleichsdienst aus.
 - Wenn Sie den Lastausgleichsdienst selbst verwalten möchten oder kein Lastausgleichsdienst benötigt wird, wählen Sie **Ich habe ein vollständig eingerichtetes Netzwerk** aus.

8 Klicken Sie auf **Gruppe erstellen und Regeln hinzufügen**.

Ergebnisse

VMware Cloud Director beginnt mit der anfänglichen Erweiterung der Skalierungsgruppe, um die Mindestanzahl an VMs zu erreichen.

Nächste Schritte

- [Hinzufügen einer Regel für die automatische Skalierung](#)
- Wenn Sie in der Detailansicht einer Skalierungsgruppe die Option **Überwachen** auswählen, werden alle Aufgaben im Zusammenhang mit dieser Skalierungsgruppe angezeigt. Sie können beispielsweise den Zeitpunkt der Erstellung der Skalierungsgruppe, alle Vergrößerungs- oder Verkleinerungsaufgaben für die Gruppe, die Regeln, die die Aufgaben initiiert haben, usw. anzeigen.
- Löschen Sie eine Skalierungsgruppe. Wenn Sie eine Skalierungsgruppe entfernen, löscht VMware Cloud Director keine der vorhandenen VMs in der Skalierungsgruppe. Wenn Sie die Anzahl der VMs verringern möchten, müssen Sie sie manuell löschen.

Hinzufügen einer Regel für die automatische Skalierung

Ab VMware Cloud Director 10.2.2 kann Ihnen Ihr Dienstleister Berechtigungen zum Erstellen und Verwalten von Skalierungsgruppen gewähren. Sie können Regeln hinzufügen, mit denen die Vergrößerung oder Verkleinerung von Skalierungsgruppen ausgelöst wird.

Voraussetzungen

[Erstellen einer Skalierungsgruppe](#)

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Anwendungen** aus und klicken Sie auf die Registerkarte **Skalierungsgruppen**.
- 2 Wählen Sie eine Skalierungsgruppe und dann **Regeln** aus.
- 3 Klicken Sie auf **Regel hinzufügen**.
- 4 Geben Sie einen Namen für die Regel ein.
- 5 Geben Sie an, ob die Skalierungsgruppe vergrößert oder verkleinert werden muss, wenn die Regel wirksam wird.
- 6 Wählen Sie die Anzahl der VMs aus, um die die Gruppe vergrößert oder verkleinert werden soll, wenn die Regel wirksam wird.
- 7 Geben Sie nach jeder automatischen Skalierung in der Gruppe eine Abkühldauer in Minuten ein.

Die Bedingungen können eine weitere Skalierung erst auslösen, wenn die Abkühldauer abgelaufen ist. Die Abkühldauer wird zurückgesetzt, wenn eine der Regeln der Skalierungsgruppe wirksam wird.

- 8 Fügen Sie eine Bedingung hinzu, die die Regel auslöst.

Die Abkühldauer ist der Zeitraum, während dem die Bedingung zum Auslösen der Regel gültig sein muss. Zum Auslösen der Regel müssen alle Bedingungen erfüllt sein.

- 9 (Optional) Zum Hinzufügen einer weiteren Bedingung klicken Sie auf **Bedingung hinzufügen**.
- 10 Klicken Sie auf **Hinzufügen**.

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 VMware Cloud 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](#)
- [Hinzufügen einer vApp aus einem Katalog](#)
- [Erstellen einer vApp aus einer vApp-Vorlage](#)
- [Importieren einer virtuellen Maschine aus vCenter Server als vApp](#)
- [Ausführen von Energievorgängen auf vApps](#)
- [Öffnen einer vApp](#)
- [vApp-Eigenschaften bearbeiten](#)
- [Anzeigen eines vApp-Netzwerkdiagramms](#)
- [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
- Löschen mehrerer vApps

Anzeigen von vApps

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

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.
 - c Klicken Sie zum Speichern der Änderungen auf **OK**. 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 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Wählen Sie **Neue vApp** aus.
- 3 Geben Sie einen Namen und optional eine Beschreibung für die vApp ein.
- 4 (Optional) Wenn Sie möchten, dass die vApp bei der Bereitstellung eingeschaltet wird, aktivieren Sie das Kontrollkästchen **Einschalten**.

Hinweis Die vApp kann nur eingeschaltet werden, wenn sie virtuelle Maschinen enthält.

- 5 (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 (Optional) Wählen Sie eine VM-Platzierungsrichtlinie und eine VM-Größenrichtlinie aus. <p>Die Dropdown-Menüs für VM-Platzierungs- und -Größenrichtlinien werden nur angezeigt, wenn der Dienstanbieter solche Richtlinien für das Organisations-VDC veröffentlicht hat.</p> <ol style="list-style-type: none"> 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) Wählen Sie eine VM-Platzierungsrichtlinie und eine VM-Größenrichtlinie aus. <p>Die Dropdown-Menüs für VM-Platzierungs- und -Größenrichtlinien werden nur angezeigt, wenn der Dienstanbieter solche Richtlinien für das Organisations-VDC veröffentlicht hat. Wenn der ausgewählten Vorlage Richtlinien zugewiesen wurden, sind Sie möglicherweise auf die vordefinierten Vorlagenrichtlinien beschränkt.</p> <ol style="list-style-type: none"> 3 (Optional) Geben Sie an, dass eine benutzerdefinierte Speicherrichtlinie verwendet werden soll, und wählen Sie die Richtlinie unter Zu verwendende benutzerdefinierte Speicherrichtlinie aus. 4 Wenn eine Endbenutzerlizenzvereinbarung verfügbar ist, müssen Sie diese überprüfen und akzeptieren.

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

Die hinzugefügte virtuelle Maschine wird im Katalog angezeigt.

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

Ergebnisse

Die vApp wird erstellt. Wenn die vApp eingeschaltet wird, 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.

VMware Cloud Director weist eigene Einschränkungen für OVF-Bereitstellungen auf, die sich von den Einschränkungen in vCenter Server unterscheiden. Es ist daher möglich, dass eine OVF-Bereitstellung, die in vCenter Server erfolgreich ist, in VMware Cloud Director fehlschlägt.

VMware Cloud Director unterstützt OVF 1.1, aber nicht alle Abschnitte des OVF 1.1-Schemas. Beispielsweise wird der Abschnitt `DeploymentOptions` in OVF nicht unterstützt.

Eine OVF-Bereitstellung in VMware Cloud Director umfasst viele Komponenten, wie z. B. `TransferService`, Spool-Bereich auf NFS-Mount, NFC-Verbindung zu vCenter Server, Prüfsummenvalidierung usw. Wenn eine dieser Komponenten fehlschlägt, führt dies zu einem OVF-Uploadfehler.

Wenn Sie ein OVF-Paket mit einer Manifestdatei hochladen, validiert VMware Cloud Director den SHA-1-Hash der OVF-Deskriptordatei und aller VMDK-Dateien auf die Werte in der `manifest.mf`-Datei. Wenn ein Hash nicht übereinstimmt, schlägt der Upload fehl. Ein **Systemadministrator** kann diese Prüfung deaktivieren, indem er die `CONFIG`-Eigenschaft auf `ovf.manifest.check.disabled` festlegt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein OVF-Paket zum Hochladen sowie über die Berechtigung verfügen, OVF-Pakete hochzuladen und vApps bereitzustellen.
- Stellen Sie sicher, dass die OVF-Version in der OVF-Deskriptordatei nicht 0.9 ist.
- Die maximal unterstützte Standardgröße einer OVF-Deskriptordatei in VMware Cloud Director beträgt 12 MB. Sie können diesen Wert überschreiben, indem Sie die `CONFIG`-Eigenschaft `ovf.descriptor.size.max` bearbeiten.
- Stellen Sie sicher, dass die maximal zulässige Standardgröße der Manifestdatei (.mf-Erweiterung) 1 MB beträgt.
- Stellen Sie sicher, dass das OVF-Paket mit dem OVF-XSD-Schema übereinstimmt.
- Wenn im `VirtualSystemType`-Element der OVF-Deskriptordatei eine Hardwareversion bereitgestellt wird, stellen Sie sicher, dass sie niedriger als die höchste Hardwareversion ist, die in dem VDC, in das Sie die OVF-Datei hochladen, unterstützt wird.
- Wenn die OVF-Deskriptordatei `ExtraConfig`-Elemente enthält, stellen Sie sicher, dass Ihr **Systemadministrator** diese Elemente in die `AllowedList` der `extraConfigs`-Elemente aufgenommen hat. Elemente, die nicht in der `AllowedList` enthalten sind, führen zum Fehlschlagen des OVF-Uploads mit einem Validierungsfehler.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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**, navigieren Sie zu einem Speicherort, 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, Netzwerkadaptertyp, 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.

Hinzufügen einer vApp aus einem Katalog

Wenn Sie Zugriff auf einen Katalog haben, können Sie die vApp-Vorlagen im Katalog verwenden, um vApps zu erstellen.

Eine vApp-Vorlagen kann auf einer OVF-Datei mit Eigenschaften zum Anpassen der virtuellen Maschinen der vApp basieren. Die vApp erbt diese Eigenschaften. Sofern diese Eigenschaften vom Benutzer konfigurierbar sind, können Sie deren Werte angeben.

Voraussetzungen

- Vergewissern Sie sich für den Zugriff auf vApp-Vorlagen in öffentlichen Katalogen, dass Sie ein **Organisationsadministrator** oder **vApp-Autor** sind.
- Vergewissern Sie sich für den Zugriff auf vApp-Vorlagen in Organisationskatalogen, die für Sie freigegeben sind, dass Sie mindestens ein **vApp-Benutzer** sind.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf **Neu** und wählen Sie **vApp aus Katalog hinzufügen** aus.
- 3 Wählen Sie eine zu importierende Vorlage aus und klicken Sie auf **Weiter**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die vApp ein.
- 5 Geben Sie eine Laufzeit-Lease sowie eine Speicher-Lease für die vApp ein und klicken Sie auf **Weiter**.
- 6 Wählen Sie im Dropdown-Menü **Speicherrichtlinie** eine Speicherrichtlinie für jede der virtuellen Maschinen in der vApp aus und klicken Sie auf **Weiter**.
- 7 Wenn die Platzierungsrichtlinien und die Größenrichtlinien für die virtuellen Maschinen in der vApp konfigurierbar sind, wählen Sie im Dropdown-Menü eine Richtlinie für jede virtuelle Maschine aus.
- 8 Sofern die Computing-Eigenschaften für die virtuellen Maschinen in der vApp konfigurierbar sind, passen Sie sie an und klicken Sie auf **Weiter**.

Option	Beschreibung
Virtuelle 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	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.

- 9 Wenn die Hardwareeigenschaften der virtuellen Maschinen in der vApp konfigurierbar sind, passen Sie die Größe der Festplatten der virtuellen Maschine an und klicken Sie auf **Weiter**.
- 10 Sofern die Netzwerkeigenschaften der virtuellen Maschinen in der vApp konfigurierbar sind, passen Sie sie an und klicken Sie auf **Weiter**.
 - a Wählen Sie auf der Seite **Netzwerk konfigurieren** die Netzwerke aus, zu denen die einzelnen virtuellen Maschinen eine Verbindung herstellen sollen.
 - b (Optional) Aktivieren Sie das Kontrollkästchen, um zum Workflow für erweiterte Netzwerke zu wechseln, und konfigurieren Sie zusätzliche Netzwerkeinstellungen für die virtuellen Maschinen in der vApp.
- 11 Überprüfen Sie die vApp-Einstellungen und klicken Sie auf **Fertigstellen**.

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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **vApp-Vorlagen** aus.
Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf das Optionsfeld neben der zu verwendenden vApp-Vorlage und dann auf **vApp erstellen**.
- 3 Geben Sie einen Namen und optional eine Beschreibung der vApp ein.
- 4 Geben Sie in Stunden oder Tagen an, wie lange diese vApp ausgeführt werden kann, bevor sie automatisch beendet wird.
- 5 Geben Sie in Stunden oder Tagen an, wie lange die beendete vApp verfügbar bleibt, bevor sie automatisch gelöscht wird.
- 6 Klicken Sie auf **Weiter**.
- 7 Wählen Sie das virtuelle Datacenter aus, in dem Sie die vApp erstellen möchten.

8 Wählen Sie eine Speicherrichtlinie aus.

9 Klicken Sie auf **Weiter**.

10 Konfigurieren Sie für VMware Cloud Director 10.2.2 und höher die Platzierungs- und Größenrichtlinien der VM.

Ab Version 10.2.2 sind Platzierungsrichtlinien global und können in mehreren Provider-VDCs veröffentlicht werden. vApp-Vorlagen enthalten Informationen zur Größen- und Platzierungsrichtlinie.

11 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.

12 Klicken Sie auf **Weiter**.

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

Option	Beschreibung
Anzahl der virtuellen CPUs	<p>Geben Sie die Anzahl virtueller CPUs für jede virtuelle Maschine in der vApp ein.</p> <p>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.</p>
Kerne pro Socket	<p>Geben Sie die Anzahl der Kerne pro Socket für jede virtuelle Maschine in der vApp ein.</p> <p>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.</p>
Anzahl der Kerne	<p>Zeigen Sie die Anzahl der Kerne für jede virtuelle Maschine in der vApp an.</p> <p>Die Anzahl ändert sich, wenn Sie die Anzahl der virtuellen CPUs aktualisieren.</p>

Option	Beschreibung
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.

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

Ergebnisse

Die neue vApp wird in der Kartenansicht angezeigt.

Importieren einer virtuellen Maschine aus vCenter Server als vApp

Wenn Sie **Systemadministrator**-Rechte haben, können Sie vCenter Server-VMs als vApps in VMware Cloud Director importieren.

Beim Import einer virtuellen Maschine werden die in vCenter Server konfigurierten Einstellungen für Reservierungen, Grenzwerte und Anteile der virtuellen Maschine nicht beibehalten. Importierte virtuelle Maschinen erhalten ihre Einstellungen für die Ressourcenzuweisung aus dem virtuellen Organisations-Datencenter, in dem sie sich befinden.

Voraussetzungen

Um virtuelle Maschinen von vCenter Server anzuzeigen und zu importieren, stellen Sie sicher, dass Sie über **Systemadministrator**-Rechte verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf **Neu** und wählen Sie **Von vCenter importieren** aus.
- 3 Wählen Sie im Dropdown-Menü die vCenter Server-Instanz aus, aus der Sie eine virtuelle Maschine importieren möchten.
- 4 Wählen Sie eine virtuelle Maschine aus, die importiert werden soll.
- 5 Geben Sie einen Namen und optional eine Beschreibung für die vApp ein.
- 6 Wählen Sie im Dropdown-Menü ein virtuelles Datencenter aus, in dem die vApp gespeichert und ausgeführt werden soll.

- 7 (Optional) Wählen Sie im Dropdown-Menü eine Speicherrichtlinie für die vApp aus.
- 8 (Optional) Um die virtuelle Quellmaschine zu deaktivieren, aktivieren Sie die Option **Virtuelle Maschine verschieben**.
- 9 Klicken Sie auf **Importieren**.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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. Für bestimmte Aktionen müssen Sie vorab die vApp ausschalten. Dies gilt beispielsweise, wenn Sie eine vApp einem Katalog hinzufügen, kopieren oder in ein anderes VDC verschieben möchten.

Voraussetzungen

Die vApp muss gestartet sein.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.


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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.

Einschalten mehrerer vApps

Sie können mehrere vApps gleichzeitig einschalten. Durch diese Aktion werden alle noch nicht eingeschalteten VMs in der vApp eingeschaltet.

Voraussetzungen

Stellen Sie sicher, dass Sie mindestens über **vApp-Autor**-Rechte verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die vApps aus, die Sie einschalten möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Einschalten** aus.
- 5 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Ausschalten mehrerer vApps

Sie können mehrere vApps gleichzeitig ausschalten. Diese Aktion schaltet alle virtuellen Maschinen in den vApps aus. Für bestimmte Aktionen müssen Sie vorab die vApp ausschalten. Dies gilt beispielsweise, wenn Sie eine vApp einem Katalog hinzufügen, kopieren oder in ein anderes virtuelles Datacenter verschieben möchten.

Voraussetzungen

- Stellen Sie sicher, dass die vApps gestartet wurden.
- Stellen Sie sicher, dass Sie mindestens über **vApp-Autor**-Rechte verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die vApps aus, die Sie ausschalten möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Ausschalten** aus.
- 5 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Verwerfen des Zustands „Angehalten“ von mehreren vApps

Wenn sich mehrere vApps im Zustand „Angehalten“ befinden und Sie Ihre Nutzung nicht mehr fortsetzen müssen, können Sie den Zustand „Angehalten“ der vApps gleichzeitig verwerfen. Durch Verwerfen des Zustands „Angehalten“ wird der Speicher entfernt und die vApps werden ausgeschaltet.

Voraussetzungen

- Stellen Sie sicher, dass die vApps den Zustand „Angehalten“ aufweisen.
- Stellen Sie sicher, dass Sie mindestens über **vApp-Autor**-Rechte verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die angehaltenen vApps aus, die Sie ausschalten möchten.
- 4 Wählen Sie im Menü **Aktionen** den Befehl **Zustand „Angehalten“ verwerfen** aus.

Ergebnisse

Die vApps sind ausgeschaltet.

Zurücksetzen mehrerer vApps

Durch das gleichzeitige Zurücksetzen mehrerer vApps wird ihr Zustand (einschließlich Arbeitsspeicher und Cache) gelöscht, die vApps werden jedoch weiterhin ausgeführt.

Voraussetzungen

- Stellen Sie sicher, dass Ihre vApps gestartet wurden und die darin enthaltenen virtuellen Maschinen eingeschaltet sind.
- Stellen Sie sicher, dass Sie mindestens über **vApp-Autor**-Rechte verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die vApps aus, die Sie zurücksetzen möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Zurücksetzen** aus und klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Ergebnisse

Der Zustand der einzelnen vApps wird gelöscht. Die vApps werden weiterhin ausgeführt.

Anhalten mehrerer vApps

Beim gleichzeitigen Anhalten mehrerer vApps wird deren aktueller Zustand beibehalten. Dazu wird der Arbeitsspeicher auf die Festplatte geschrieben.

Voraussetzungen

Stellen Sie sicher, dass die vApps ausgeführt werden.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die vApps aus, die Sie anhalten möchten.
- 4 Wählen Sie im Menü **Aktionen** der vApp, die Sie anhalten möchten, die Option **Anhalten** aus und klicken Sie auf **OK**.


Ergebnisse

Die vApps werden angehalten, und ihr Zustand wird beibehalten.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Klicken Sie auf , um die vApps in einer Kartenansicht anzuzeigen.
In der Kartenansicht werden allgemeine Informationen für jede vApp angezeigt, wie z. B. deren Name, Betriebszustand, Leaseinformationen, Erstellungsdatum, Besitzer, die Anzahl der virtuellen Maschinen, die der vApp zugeordnet sind, die Gesamtanzahl der CPUs, Gesamtspeicher und -arbeitspeicher sowie zugeordnete Netzwerke.
- 3 Um die detaillierten Einstellungen einer ausgewählten vApp anzuzeigen, klicken Sie auf der vApp-Karte auf **Details**.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.
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 Start- und Beendigungsreihenfolge von virtuellen Maschinen in einer vApp


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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Start- und Beendigungsreihenfolge** und dann auf **Bearbeiten**.
- 5 Bearbeiten Sie die Start- und Beendigungsreihenfolge für jede virtuelle Maschine und klicken Sie auf **OK**.

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 VMware Cloud 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 VMware Cloud Director die nächste virtuelle Maschine in der Reihenfolge herunterfährt.

Bearbeiten der Gasteigenschaften einer vApp


Wenn eine vApp vom Benutzer konfigurierbare OVF-Eigenschaften enthält, können Sie diese prüfen und ändern.

Wenn für eine virtuelle Maschine in der vApp ein Wert für eine vom Benutzer konfigurierbare Eigenschaft definiert ist und diese Eigenschaft denselben Namen wie eine der OVF-Umgebungseigenschaften aufweist, hat der Wert der virtuellen Maschine Vorrang.

Voraussetzungen

Stellen Sie sicher, dass die vApp beendet wurde und ihre Gasteigenschaften vom Benutzer konfiguriert werden können.


Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **Virtuelle Maschinen** aus.
- 2 Klicken Sie auf , um die Liste in einer Kartenansicht anzuzeigen, und ordnen Sie optional die Liste der virtuellen Maschinen über das Dropdown-Menü **Sortieren nach** an.
- 3 Klicken Sie in der Karte der zu bearbeitenden virtuellen Maschine auf **Details**.
- 4 Klicken Sie auf **Gasteigenschaften** und auf **Bearbeiten**.
- 5 Ändern Sie die Gasteigenschaften für die vApp und klicken Sie auf **OK**.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.

Hinweis Virtuelle Organisations-VDCs, die auf NSX Data Center for vSphere basieren, unterstützen geroutete, isolierte und direkte vApp-Netzwerke.

Organisations-VDCs, die auf NSX-T Data Center basieren, unterstützen isolierte und direkte vApp-Netzwerke.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 Umschalloption 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			


Hinweis Virtuelle Organisations-VDCs, die auf NSX Data Center for vSphere basieren, unterstützen geroutete, isolierte und direkte vApp-Netzwerke.

Organisations-VDCs, die auf NSX-T Data Center basieren, unterstützen isolierte und direkte vApp-Netzwerke.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 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 **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden 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 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 VMware Cloud Director der virtuellen Maschine beim Einschalten per DHCP eine IP-Adresse zu.

Voraussetzungen

- Vergewissern Sie sich, dass das vApp-Netzwerk entweder geroutet oder isoliert ist.
- Vergewissern Sie sich, dass die vApp sich in einem Organisations-VDC befindet, das von NSX Data Center for vSphere gestützt wird.


Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 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.
VMware Cloud 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 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.

Jede von Ihnen erstellte statische Route wird automatisch aktiviert.

Voraussetzungen

Ein vApp-Netzwerk mit Routing.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 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

Hinzufügen einer Portweiterleitungsregel zu einem vApp-Netzwerk

Sie können bestimmte vApp-Netzwerke durch Hinzufügen einer NAT-Zuordnungsregel für die Portweiterleitung konfigurieren.

Die Portweiterleitung ermöglicht den Zugriff von externer Seite auf Dienste, die auf virtuellen Maschinen im vApp-Netzwerk ausgeführt werden.


Wenn Sie die Portweiterleitung konfigurieren, ordnet VMware Cloud Director einem auf einer virtuellen Maschine ausgeführten Dienst für eingehenden Datenverkehr einen externen Port zu.

Wenn Sie einem vApp-Netzwerk eine Portweiterleitungsregel hinzufügen, wird sie am Ende der Liste der NAT-Zuordnungsregeln angezeigt. Informationen darüber, wie Sie die Reihenfolge festlegen, in der die Portweiterleitungsregeln erzwungen werden, finden Sie unter

Voraussetzungen

- Stellen Sie sicher, dass das vApp-Netzwerk geroutet ist.
- Stellen Sie sicher, dass die Firewall im vApp-Netzwerk aktiviert ist. Wenn Sie die Firewall deaktivieren, werden die NAT-Zuordnungsregeln nicht mehr auf das vApp-Netzwerk angewendet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Klicken Sie auf **Dienste** und anschließend auf **Bearbeiten**.
- 6 Zum Aktivieren von NAT wählen Sie die Option „NAT“ aus.
- 7 Wählen Sie im Dropdown-Menü **NAT-Typ** die Option **Portweiterleitung** aus und klicken Sie auf **Hinzufügen**.
- 8 (Optional) Aktivieren Sie das Kontrollkästchen, um die IP-Maskierung zu aktivieren.
- 9 Konfigurieren Sie die Portweiterleitungsregel.
 - a Wählen Sie einen externen Port aus.
 - b Wählen Sie einen Port für die Weiterleitung aus.
 - c Wählen Sie eine VM-Schnittstelle aus.
 - d Wählen Sie ein Protokoll für den Typ des weiterzuleitenden Datenverkehrs aus.
- 10 Klicken Sie auf **Speichern**.

Nächste Schritte

Ordnen Sie ggf. die Portweiterleitungsregeln neu an, indem Sie die Schaltflächen **Nach oben verschieben** oder **Nach unten verschieben** verwenden.

Hinzufügen einer IP-Übersetzungsregel zu einem vApp-Netzwerk

Sie können bestimmte vApp-Netzwerke durch Hinzufügen einer NAT-Zuordnungsregel für die Bereitstellung einer IP-Übersetzung konfigurieren.


Wenn Sie eine IP-Übersetzungsregel für ein Netzwerk erstellen, fügt vCloud Director dem mit der Portgruppe des Netzwerks verknüpften Edge-Gateway eine DNAT- und eine SNAT-Regel hinzu. Die DNAT-Regel steuert die Umsetzung einer externen IP-Adresse in eine interne IP-Adresse für eingehenden Datenverkehr. Die SNAT-Regel steuert die Umsetzung einer internen IP-Adresse in eine externe IP-Adresse für ausgehenden Datenverkehr.

Voraussetzungen

- Stellen Sie sicher, dass das vApp-Netzwerk geroutet ist.
- Stellen Sie sicher, dass die Firewall im vApp-Netzwerk aktiviert ist. Wenn Sie die Firewall deaktivieren, werden die NAT-Zuordnungsregeln nicht mehr auf das vApp-Netzwerk angewendet.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden 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 der Registerkarte **Netzwerke** auf ein Netzwerk, um die Netzwerkdetails anzuzeigen.
- 5 Klicken Sie auf **Dienste** und anschließend auf **Bearbeiten**.
- 6 Zum Aktivieren von NAT wählen Sie die Option „NAT“ aus.
- 7 Wählen Sie im Dropdown-Menü **NAT-Typ** die Option **IP-Übersetzung** aus und klicken Sie auf **Hinzufügen**.
- 8 Wählen Sie eine VM-Schnittstelle aus und klicken Sie auf **Beibehalten**.
- 9 Wählen Sie den Zuordnungsmodus aus.
- 10 Wenn Sie den Zuordnungsmodus **Manuell** auswählen, geben Sie eine externe IP-Adresse ein.
- 11 Klicken Sie auf **Speichern**.

Nächste Schritte

Ordnen Sie bei Bedarf die IP-Übersetzungsregeln neu an, indem Sie die Schaltflächen **Nach oben verschieben** oder **Nach unten verschieben** verwenden.


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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 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 einer benannten Festplatte verbunden ist, können Sie keinen vApp-Snapshot erstellen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.

Erstellen von Snapshots mehrerer vApps

Indem Sie Snapshots mehrerer vApps erstellen, erstellen Sie Snapshots von allen virtuellen Maschinen in den vApps. Nachdem Sie die Snapshots erstellt haben, können Sie alle virtuellen Maschinen in den vApps auf die Snapshots zurücksetzen oder die Snapshots entfernen, wenn Sie sie nicht benötigen.

Für vApp-Snapshots gelten einige Einschränkungen.

- vApp-Snapshots erfassen keine NIC-Konfigurationen.
- Wenn eine virtuelle Maschine in einer vApp mit einer benannten Festplatte verbunden ist, können Sie keinen vApp-Snapshot erstellen.

- Durch das Erstellen von Snapshots mehrerer vApps wird keine Snapshots des Arbeitsspeichers der vApps erstellt und das Gastdateisystem der vApps wird nicht stillgelegt. Wenn Sie einen Snapshot des Arbeitsspeichers Ihrer vApps erstellen möchten oder das Gastdateisystem stilllegen möchten, müssen Sie für jede vApp einzelne Snapshots erstellen. Weitere Informationen finden Sie im [Erstellen eines Snapshots einer vApp](#).

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die vApps aus, für die Sie Snapshots erstellen möchten.
- 4 Wählen Sie im Menü **Aktionen** den Befehl **Snapshot erstellen** aus und klicken Sie zum Bestätigen auf **OK**.

Nächste Schritte

- Sie können alle virtuellen Maschinen in den vApps auf die neuesten Snapshots wiederherstellen. Weitere Informationen finden Sie im [Wiederherstellen von Snapshots mehrerer vApps](#).
- Sie können die Snapshots der vApps entfernen. Weitere Informationen finden Sie im [Entfernen der Snapshots mehrerer vApps](#).

Entfernen der Snapshots mehrerer vApps

Wenn Sie die Snapshots mehrerer vApps nicht mehr benötigen, können Sie sie gleichzeitig 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.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die vApps aus, deren Snapshots Sie entfernen möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Snapshot entfernen** aus.

Wiederherstellen von Snapshots mehrerer vApps

Sie können für alle virtuellen Maschinen in mehreren vApps den Zustand wiederherstellen, den sie hatten, als die vApp-Snapshots erstellt wurden.

Voraussetzungen

Stellen Sie sicher, dass die wiederherzustellenden vApps über vorhandene Snapshots verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die vApps aus, die Sie auf die neuesten Snapshots zurücksetzen möchten.
- 4 Wählen Sie im Menü **Aktionen** die Option **Snapshot wiederherstellen** aus.
- 5 Klicken Sie auf **OK**, um den Vorgang zu bestätigen.


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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 Datacenter 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 Datacenter 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 **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden 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 Datacenter 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 Computername darf nur alphanumerische Zeichen und Bindestriche enthalten. Ein Computername 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> <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 oder klicken Sie auf Benutzerdefinierte Größenänderungsoptionen, um die Computing-, Arbeitsspeicher- und Speichereinstellungen manuell einzugeben. <p>Die vordefinierten Größenänderungsoptionen sind klein, mittel oder groß.</p> <ul 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> <ul 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.


Ab VMware Cloud Director 10.2.2 enthält die vApp-Vorlage beim Hinzufügen einer vApp zu einem Katalog die Platzierungs- und Größenrichtlinien der Quell-vApp als nicht änderbare Tags.

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 **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden 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 beispielsweise eine neue Version einer vApp in den Katalog hochladen, sollten Sie die alte Version überschreiben.

- 7 Geben Sie an, wie die Vorlage verwendet werden muss.

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 Zum Abschließen der Erstellung der vApp-Vorlage klicken Sie auf **OK**.

Ergebnisse

Die vApp-Vorlage wird 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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

Vergewissern Sie sich, dass Ihnen die vordefinierte Rolle **vApp-Benutzer** oder dieser Rolle entsprechende Rechte zugewiesen sind.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.

4 Verlängern Sie die Laufzeit-Lease der vApp.

a Aktivieren Sie das Kontrollkästchen **Laufzeit-Lease**.

b Wählen Sie im Dropdown-Menü einen Wert für die Laufzeit-Lease aus.

Sie können einen Wert in Stunden oder Tagen auswählen bzw. die Lease auf **Läuft nie ab** festlegen. **Systemadministratoren** können die maximal auswählbare Dauer beschränken.

5 Verlängern Sie die Speicher-Lease der vApp.

a Aktivieren Sie das Kontrollkästchen **Speicher-Lease**.

b Wählen Sie im Dropdown-Menü einen Wert für die Speicher-Lease aus.

Sie können einen Wert in Stunden oder Tagen auswählen bzw. die Lease auf **Läuft nie ab** festlegen. **Systemadministratoren** können die maximal auswählbare Dauer beschränken.

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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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.

Löschen mehrerer vApps

Wenn Sie mehrere vApps aus Ihrer Organisation entfernen möchten, können Sie sie gleichzeitig löschen.

Voraussetzungen

- Stellen Sie sicher, dass Ihre vApps beendet wurden.
- Stellen Sie sicher, dass Sie mindestens über **vApp-Autor**-Rechte verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich die Option **vApps** aus.
- 2 Aktivieren Sie die Option **Mehrfachauswahl**.
- 3 Wählen Sie die zu löschenden vApps aus.
- 4 Wählen Sie im Menü **Aktionen** die Option **Löschen** aus.
- 5 Klicken Sie zur Bestätigung auf **Löschen**.

Arbeiten mit Kubernetes-Clustern

4

Sie können Kubernetes-Cluster unterschiedlicher Knotengröße anhand der vorhandenen Organisations-VDC-Richtlinien erstellen.

Kubernetes-Containercluster fungiert als Container Service Extension-Plug-In für VMware Cloud Director. Sie können das Plug-In Kubernetes-Containercluster im VMware Cloud Director Tenant Portal verwenden, um Cluster mit nativen und VMware Tanzu Kubernetes Grid Integrated Edition-Clustern (TKGI) bereitzustellen. Sie können Tanzu Kubernetes-Cluster ohne das Plug-In Kubernetes-Containercluster erstellen.

Bei Aktivierung auf einem vSphere-Cluster stellt VMware vSphere® with VMware Tanzu™ die Möglichkeit bereit, vorgelagerte Kubernetes-Cluster in dedizierten Ressourcenpools zu erstellen. Weitere Informationen finden Sie im Handbuch *Konfiguration und Verwaltung von vSphere with Kubernetes* in der Dokumentation zu vSphere.

Wenn ein Dienstanbieter eine Kubernetes-Richtlinie des Provider-VDC erstellt und die Richtlinie in einem Organisations-VDC veröffentlicht, wird eine Kubernetes-Richtlinie des Organisations-VDC erstellt. Sie können das Plug-In Kubernetes-Containercluster zum Erstellen von Tanzu Kubernetes-Clustern verwenden, indem Sie eine der Kubernetes-Richtlinien des Organisations-VDC anwenden.

Laufzeitoptionen für Kubernetes

- Tanzu Kubernetes-Cluster: Sie können die Laufzeitoption „vSphere Kubernetes“ verwenden, um vSphere with VMware Tanzu-verwaltete Tanzu Kubernetes-Cluster zu erstellen. Diese Option bietet eine größere Anzahl an Funktionen, ist aber möglicherweise teurer. Weitere Informationen finden Sie im Handbuch *Konfiguration und Verwaltung von vSphere with Kubernetes* in der Dokumentation zu vSphere.
- Native Cluster: Das Plug-In Kubernetes-Containercluster verwaltet die Cluster mit nativer Kubernetes-Laufzeit. Diese Cluster weisen eine verringerte Hochverfügbarkeitsfunktion mit einem einzelnen Steuerungsebenen-Knoten auf. Es stehen weniger dauerhafte Volumes zur Auswahl, und Netzwerkautomatisierung ist nicht vorhanden. Diese Cluster verursachen unter Umständen jedoch geringere Kosten.
- TKGI-Cluster: Bei der VMware Tanzu Kubernetes Grid Integrated Edition handelt es sich um eine speziell entwickelte Container-Lösung zum Operationalisieren von Kubernetes für Unternehmen und Dienstanbieter mit mehreren Clouds. Zu den Funktionen dieser Edition

gehören unter anderem Hochverfügbarkeit, automatische Skalierung, Integritätsprüfungen sowie Selbstreparatur und parallele Upgrades für Kubernetes-Cluster. Weitere Informationen zu TKGI-Clustern finden Sie in der Dokumentation zu *VMware Tanzu Kubernetes Grid Integrated Edition*.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen einer Kubernetes-Richtlinie des Organisations-VDC](#)
- [Bearbeiten einer Kubernetes-Richtlinie des Organisations-VDC](#)
- [Erstellen eines Tanzu Kubernetes-Clusters](#)
- [Erstellen eines nativen Kubernetes-Clusters](#)
- [Erstellen eines VMware Tanzu Kubernetes Grid Integrated Edition-Clusters](#)
- [Konfigurieren des externen Zugriffs auf einen Dienst in einem Tanzu Kubernetes-Cluster](#)

Hinzufügen einer Kubernetes-Richtlinie des Organisations-VDC

Wenn Sie über **Systemadministrator**rechte verfügen, können Sie eine Kubernetes-Richtlinie des Organisations-VDC hinzufügen, indem Sie die Kubernetes-Richtlinie eines Provider-VDC verwenden. Sie können die Kubernetes-Richtlinie des Organisations-VDC zum Erstellen von Tanzu Kubernetes-Clustern verwenden.

Wenn Sie die Kubernetes-Richtlinie eines Provider-VDC zu einem Organisations-VDC hinzufügen oder darin veröffentlichen, stellen Sie die Richtlinie Mandanten bereit, indem Sie eine VDC-Organisationsrichtlinie erstellen. Mandanten können die verfügbaren Kubernetes-Richtlinien des Organisations-VDC verwenden, um die Kubernetes-Kapazität beim Erstellen von Tanzu Kubernetes-Clustern zu nutzen. Eine Kubernetes-Richtlinie schließt Platzierung, Infrastrukturqualität und Speicherklassen für dauerhafte Volumes ein. Kubernetes-Richtlinien können unterschiedliche Berechnungsgrenzen aufweisen.

Sie können einem einzelnen Organisations-VDC mehrere Kubernetes-Richtlinien eines Organisations-VDC hinzufügen. Sie können mithilfe einer einzelnen Kubernetes-Richtlinie des Provider-VDC mehrere Kubernetes-Richtlinien für das Organisations-VDC erstellen. Sie können die Kubernetes-Richtlinien des Organisations-VDC als Indikator für die Dienstqualität verwenden. Sie können beispielsweise eine Richtlinie vom Typ „Gold Kubernetes“, die die Auswahl der garantierten Maschinenklassen und einer schnellen Speicherklasse ermöglicht, oder eine Richtlinie vom Typ „Silver Kubernetes“ veröffentlichen, die die Auswahl der bestmöglichen Maschinenklassen und eine langsame Speicherklasse ermöglicht.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Rolle **Systemadministrator** oder eine Rolle verfügen, die einen entsprechenden Satz an Regeln enthält. Alle anderen Rollen können nur die Kubernetes-Regeln des Organisations-VDC anzeigen.

- Stellen Sie sicher, dass Ihre Umgebung mindestens ein von einem Supervisor-Cluster gestütztes Provider-VDC aufweist. Die von einem Supervisor-Cluster gestützten Provider-VDCs werden mit einem Kubernetes-Symbol auf der Registerkarte **Provider-VDCs** des Service Provider Admin Portal gekennzeichnet. Weitere Informationen zu vSphere with VMware Tanzu in VMware Cloud Director finden Sie unter [Verwenden von vSphere with Kubernetes in VMware Cloud Director](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.
- Stellen Sie sicher, dass Sie bei einem Flex-Organisations-VDC angemeldet sind.
- Machen Sie sich mit den VM-Klassentypen für Tanzu Kubernetes-Cluster vertraut. Weitere Informationen finden Sie im Handbuch *Konfiguration und Verwaltung von vSphere with Kubernetes* in der Dokumentation zu vSphere.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Datencenter** und dann auf **Virtuelles Datencenter**.
- 2 Wählen Sie ein Organisations-VDC aus.
- 3 Wählen Sie im linken Fensterbereich unter **Einstellungen** die Option **Kubernetes-Richtlinien** aus und klicken Sie auf **Hinzufügen**.
Der Assistent **Für Organisations-VDC veröffentlichen** wird angezeigt.
- 4 Geben Sie einen für Mandanten sichtbaren Namen und eine Beschreibung für die Kubernetes-Richtlinie des Organisations-VDC ein und klicken Sie auf **Weiter**.
- 5 Wählen Sie die zu verwendende Kubernetes-Richtlinie des Provider-VDC aus und klicken Sie auf **Weiter**.
- 6 Wählen Sie CPU- und Arbeitsspeichergrenzwerte für die Tanzu Kubernetes-Cluster aus, die unter dieser Richtlinie erstellt wurden.

Die maximalen Grenzwerte richten sich nach den CPU- und Arbeitsspeicherzuteilungen des Organisations-VDC. Wenn Sie die Richtlinie hinzufügen, gelten die ausgewählten Grenzwerte als Maximalwerte für die Mandanten.

- 7 Geben Sie an, ob CPU und Arbeitsspeicher für die in dieser Richtlinie erstellten Tanzu Kubernetes-Clusterknoten reserviert werden sollen, und klicken Sie auf **Weiter**.

Für jeden Klassentyp gibt es zwei Editionen: garantiert und bestmöglich. Bei einer garantierten Klassenedition werden die zugehörigen konfigurierten Ressourcen vollständig reserviert, während eine bestmögliche Edition eine Überbelegung der Ressourcen zulässt. Je nach Auswahl können Sie auf der nächsten Seite des Assistenten zwischen VM-Klassentypen der garantierten und bestmöglichen Edition auswählen.

- Wählen Sie **Ja** für VM-Klassentypen der garantierten Edition mit vollständigen CPU- und Arbeitsspeicherreservierungen aus.
- Wählen Sie **Nein** für VM-Klassentypen der bestmöglichen Edition ohne CPU- und Arbeitsspeicherreservierungen aus.

- 8 Wählen Sie auf der Seite **Maschinenklassen** des Assistenten mindestens einen für diese Richtlinie verfügbaren VM-Klassentyp aus.

Bei den ausgewählten Maschinenklassen handelt es sich um die einzigen Klassentypen, die Mandanten zur Verfügung stehen, wenn Sie die Richtlinie zum Organisations-VDC hinzufügen.

- 9 Wählen Sie eine oder mehrere Speicherrichtlinien aus.
- 10 Überprüfen Sie Ihre Auswahl und klicken Sie auf **Veröffentlichen**.

Ergebnisse

Die Informationen zur veröffentlichten Richtlinie werden in der Liste der Kubernetes-Richtlinien angezeigt. Die veröffentlichte Richtlinie erstellt einen Supervisor-Namespace im Supervisor-Cluster mit den angegebenen Ressourcengrenzwerten aus der Richtlinie.

Die Mandanten können mit der Verwendung der Kubernetes-Richtlinie beginnen, um Tanzu Kubernetes-Cluster zu erstellen. VMware Cloud Director platziert jeden Tanzu Kubernetes-Cluster, der unter dieser Kubernetes-Richtlinie erstellt wurde, im selben Supervisor-Namespace. Die Ressourcengrenzwerte der Richtlinie werden zu Ressourcengrenzwerten des Supervisor-Namespace. Alle vom Mandanten erstellten Tanzu Kubernetes-Cluster im Supervisor-Namespace konkurrieren um die Ressourcen innerhalb dieser Grenzwerte.

Nächste Schritte

- Löschen Sie die Kubernetes-Richtlinie eines Organisations-VDC.
- Mithilfe des Service Provider Admin Portal können Sie Ressourcenkontingente der Organisation verwalten. Weitere Informationen finden Sie unter [Verwalten von Kontingenten für den Ressourcenverbrauch einer Organisation](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.
- [Verwalten der Ressourcenkontingente einer Gruppe](#) oder [Verwalten der Ressourcenkontingente eines Benutzers](#)

Bearbeiten einer Kubernetes-Richtlinie des Organisations-VDC

Wenn Sie über **Systemadministrator**rechte verfügen, können Sie die Kubernetes-Richtlinie eines Organisations-VDC bearbeiten, um deren Beschreibung und die CPU- und Arbeitsspeichergrenzwerte zu ändern.

Voraussetzungen

Stellen Sie sicher, dass Sie über die Rolle **Systemadministrator** oder eine Rolle verfügen, die einen entsprechenden Satz an Regeln enthält. Alle anderen Rollen können nur die Kubernetes-Regeln des Organisations-VDC anzeigen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Datencenter** und dann auf **Virtuelles Datencenter**.
- 2 Wählen Sie ein Organisations-VDC aus.
- 3 Klicken Sie im linken Bereich unter **Einstellungen** auf **Kubernetes-Richtlinie**.
- 4 Wählen Sie die zu bearbeitende Kubernetes-Richtlinie des Organisations-VDC aus und klicken Sie auf **Bearbeiten**.

Der Assistent **VDC-Kubernetes-Richtlinie bearbeiten** wird angezeigt.

- 5 Bearbeiten Sie die Beschreibung für die Kubernetes-Richtlinie des Organisations-VDC und klicken Sie auf **Weiter**.

Der Richtlinienname ist mit dem Supervisor-Namespace verknüpft, der während der Veröffentlichung der Richtlinie erstellt wurde, und kann nicht geändert werden.

- 6 Bearbeiten Sie den CPU- und Arbeitsspeichergrenzwert für die Kubernetes-Richtlinie des Organisations-VDC und klicken Sie auf **Weiter**.

Die CPU- und Arbeitsspeicherreservierung kann nicht bearbeitet werden.

- 7 Überprüfen Sie die Details der neuen Richtlinie und klicken Sie auf **Speichern**.

Nächste Schritte

- Löschen Sie die Kubernetes-Richtlinie eines Organisations-VDC.
- Mithilfe des Service Provider Admin Portal können Sie Ressourcenkontingente der Organisation ändern. Weitere Informationen finden Sie unter [Verwalten von Kontingenten für den Ressourcenverbrauch einer Organisation](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.
- Ändern Sie Gruppen- und Benutzerkontingente. Siehe [Verwalten der Ressourcenkontingente einer Gruppe](#) oder [Verwalten der Ressourcenkontingente eines Benutzers](#).

Erstellen eines Tanzu Kubernetes-Clusters

Sie können Tanzu Kubernetes-Cluster mithilfe des Plug-Ins Kubernetes-Containercluster erstellen.

Weitere Informationen zu den verschiedenen Kubernetes-Laufzeitoptionen für die Clustererstellung finden Sie unter [Kapitel 4 Arbeiten mit Kubernetes-Clustern](#).

Sie können Kubernetes-Cluster auch mithilfe der Container Service Extension-Befehlszeilenschnittstelle verwalten. Informationen hierzu finden Sie in der Dokumentation zu [Container Service Extension](#).

VMware Cloud Director stellt Tanzu Kubernetes-Cluster mit aktiviertem PodSecurityPolicy-Zugangskontroller bereit. Zum Bereitstellen von Arbeitslasten müssen Sie eine Pod-Sicherheitsrichtlinie erstellen. Weitere Informationen zum Implementieren der Nutzung von Pod-Sicherheitsrichtlinien in Kubernetes finden Sie im Thema *Verwenden von Pod-Sicherheitsrichtlinien mit Tanzu Kubernetes-Clustern* im Handbuch *Konfiguration und Verwaltung von vSphere with Kubernetes*.

Voraussetzungen

- Stellen Sie sicher, dass Ihr Dienstanbieter das Plug-In Kubernetes-Containercluster in Ihrer Organisation veröffentlicht hat. Das Plug-In steht auf der oberen Navigationsleiste unter **Mehr > Kubernetes-Containercluster** zur Verfügung.
- Stellen Sie sicher, dass mindestens eine Kubernetes-Richtlinie in Ihrem Organisations-VDC vorhanden ist. Informationen zum Hinzufügen einer Kubernetes-Richtlinie für das Organisations-VDC finden Sie unter [Hinzufügen einer Kubernetes-Richtlinie des Organisations-VDC](#).
- Stellen Sie sicher, dass der Dienstanbieter das Recht paket **Berechtigung vmware:tkgcluster** in Ihrer Organisation veröffentlicht und Ihnen die Berechtigung **Bearbeiten: Tanzu Kubernetes-Gastcluster** zum Erstellen und Ändern von Tanzu Kubernetes-Clustern erteilt hat. Sie müssen über die Berechtigung **Vollständige Kontrolle: Tanzu Kubernetes-Gastcluster** verfügen, um Cluster löschen zu können.
- Stellen Sie sicher, dass der Dienstanbieter einen Eintrag für die Zugriffssteuerungsliste (Access Control List, ACL) mit Informationen zu Ihrer Zugriffsebene erstellt hat.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Mehr > Kubernetes-Containercluster** aus.
- 2 (Optional) Wenn das Organisations-VDC für die Erstellung von TKGI-Clustern aktiviert ist, wählen Sie auf der Seite **Kubernetes-Containercluster** die Registerkarte **vSphere with Tanzu & Nativ** aus.
- 3 Klicken Sie auf **Neu**.
- 4 Wählen Sie die Laufzeioption **vSphere with Tanzu** aus und klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen für den neuen Kubernetes-Cluster ein und klicken Sie auf **Weiter**.
- 6 Wählen Sie das Organisations-VDC aus, dem ein Tanzu Kubernetes-Cluster bereitgestellt werden soll, und klicken Sie auf **Weiter**.
- 7 Wählen Sie eine Kubernetes-Richtlinie und eine Kubernetes-Version für das Organisations-VDC aus und klicken Sie auf **Weiter**.

VMware Cloud Director zeigt einen Standardsatz an Kubernetes-Versionen an, die weder an ein Organisations-VDC noch an eine Kubernetes-Richtlinie gebunden sind. Bei diesen

Versionen handelt es sich um eine globale Einstellung. Verwenden Sie zum Ändern der Liste der verfügbaren Versionen das Zellenverwaltungstool und führen Sie den Befehl `./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v version_numbers` mit kommagetrennten Versionsnummern aus.

- 8 Wählen Sie die Anzahl der Steuerungsebenen- und Worker-Knoten im neuen Cluster aus.
- 9 Wählen Sie Maschinenklassen für Steuerungsebenen- und Worker-Knoten aus und klicken Sie auf **Weiter**.
- 10 Wählen Sie eine Kubernetes-Richtlinienspeicherklasse für die Steuerungsebenen- und Worker-Knoten aus und klicken Sie auf **Weiter**.
- 11 (Optional) Geben Sie für VMware Cloud Director 10.2.2 und höher einen Bereich von IP-Adressen für Kubernetes-Dienste und einen Bereich für Kubernetes-Pods an und klicken Sie auf **Weiter**.

CIDR (Classless Inter-Domain Routing) ist eine Methode für IP-Routing und IP-Adresszuweisung.

Option	Beschreibung
<code>Pods CIDR</code>	Gibt einen IP-Adressbereich an, der für Kubernetes-Pods verwendet werden soll. Der Standardwert ist 192.168.0.0/16. Die Subnetzgröße der Pods muss größer oder gleich /24 sein. Dieser Wert darf sich nicht mit den Einstellungen des Supervisor-Clusters überschneiden. Sie können einen IP-Bereich eingeben.
<code>Services CIDR</code>	Gibt einen Bereich von IP-Adressen an, die für Kubernetes-Dienste verwendet werden sollen. Der Standardwert ist 10.96.0.0/12. Dieser Wert darf sich nicht mit den Einstellungen des Supervisor-Clusters überschneiden. Sie können einen IP-Bereich eingeben.

- 12 Überprüfen Sie die Clustereinstellungen und klicken Sie auf **Fertigstellen**.

Nächste Schritte

- Passen Sie die Größe des Kubernetes-Clusters an, um die Anzahl der Worker-Knoten zu ändern.
- Laden Sie die Datei „kubeconfig“ herunter. Das Befehlszeilenprogramm `kubectl` verwendet kubeconfig-Dateien, um Informationen zu Clustern, Benutzern, Namespaces und Authentifizierungsmechanismen abzurufen.
- Löschen Sie ein Kubernetes-Cluster.

Erstellen eines nativen Kubernetes-Clusters

Sie können mit Container Service Extension 3.0 verwaltete Kubernetes-Cluster erstellen, indem Sie das Plug-In Kubernetes-Containercluster verwenden.

Weitere Informationen zu den verschiedenen Kubernetes-Laufzeitoptionen für die Clustererstellung finden Sie unter [Kapitel 4 Arbeiten mit Kubernetes-Clustern](#).

Sie können Kubernetes-Cluster auch mithilfe der Container Service Extension-Befehlszeilenschnittstelle verwalten. Informationen hierzu finden Sie in der Dokumentation zu [Container Service Extension](#).

Voraussetzungen

- Stellen Sie sicher, dass Ihr Dienstanbieter das Plug-In Kubernetes-Containercluster in Ihrer Organisation veröffentlicht hat. Kubernetes-Containercluster fungiert als Container Service Extension-Plug-In für VMware Cloud Director. Das Plug-In steht auf der oberen Navigationsleiste unter **Mehr > Kubernetes-Containercluster** zur Verfügung.
- Stellen Sie sicher, dass Ihr Dienstanbieter die Einrichtung des Container Service Extension 3.0-Servers abgeschlossen und eine native Container Service Extension-Platzierungsrichtlinie im Organisations-VDC veröffentlicht hat.
- Stellen Sie sicher, dass der Dienstanbieter das Rechtepaket **Berechtigung cse:nativeCluster** in Ihrer Organisation veröffentlicht und Ihnen die Berechtigung **Bearbeiten CSE:NATIVECLUSTER** zum Erstellen und Ändern der nativen Kubernetes-Cluster erteilt hat. Sie müssen über die Berechtigung **Vollständige Kontrolle CSE:NATIVECLUSTER** verfügen, um Cluster löschen zu können.
- Stellen Sie sicher, dass der Dienstanbieter einen Eintrag für die Zugriffssteuerungsliste (Access Control List, ACL) mit Informationen zu Ihrer Zugriffsebene erstellt hat.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Mehr > Kubernetes-Containercluster** aus.
- 2 (Optional) Wenn das Organisations-VDC für die Erstellung von TKGI-Clustern aktiviert ist, wählen Sie auf der Seite **Kubernetes-Containercluster** die Registerkarte **vSphere with Tanzu & Nativ** aus.
- 3 Klicken Sie auf **Neu**.
- 4 Wählen Sie die Kubernetes-Laufzeitoption **Nativ** aus.
- 5 Geben Sie einen Namen ein und wählen Sie eine Kubernetes-Vorlage in der Liste aus.
- 6 (Optional) Geben Sie eine Beschreibung für den neuen Kubernetes-Cluster und einen öffentlichen SSH-Schlüssel ein.
- 7 Klicken Sie auf **Weiter**.
- 8 Wählen Sie das Organisations-VDC aus, dem ein nativer Cluster bereitgestellt werden soll, und klicken Sie auf **Weiter**.
- 9 Wählen Sie die Anzahl der Steuerungsebenen- und Worker-Knoten und optional Größenrichtlinien für die Knoten aus.
- 10 Klicken Sie auf **Weiter**.

- 11 Wenn Sie eine zusätzliche VM mit NFS-Software bereitstellen möchten, schalten Sie die Option **NFS aktivieren** ein.
- 12 (Optional) Wählen Sie Speicherrichtlinien für die Steuerungsebenen- und Worker-Knoten aus.
- 13 Klicken Sie auf **Weiter**.
- 14 Wählen Sie ein Netzwerk für den Kubernetes-Cluster aus und klicken Sie auf **Weiter**.
- 15 Überprüfen Sie die Clustereinstellungen und klicken Sie auf **Fertigstellen**.

Nächste Schritte

- Passen Sie die Größe des Kubernetes-Clusters an, um die Anzahl der Worker-Knoten zu ändern.
- Laden Sie die Datei „kubecfg“ herunter. Das Befehlszeilenprogramm kubectl verwendet kubecfg-Dateien, um Informationen zu Clustern, Benutzern, Namespaces und Authentifizierungsmechanismen abzurufen.
- Löschen Sie ein Kubernetes-Cluster.

Erstellen eines VMware Tanzu Kubernetes Grid Integrated Edition-Clusters

Sie können VMware Tanzu Kubernetes Grid Integrated Edition-Cluster (TKGI) mithilfe von Container Service Extension erstellen.

Weitere Informationen zu den verschiedenen Kubernetes-Laufzeitoptionen für die Clustererstellung finden Sie unter [Kapitel 4 Arbeiten mit Kubernetes-Clustern](#).

Sie können Kubernetes-Cluster auch mithilfe der Container Service Extension-Befehlszeilenschnittstelle verwalten. Informationen hierzu finden Sie in der Dokumentation zu [Container Service Extension](#).

Voraussetzungen

- Stellen Sie sicher, dass Ihr Dienstanbieter das Plug-In Kubernetes-Containercluster in Ihrer Organisation veröffentlicht hat. Kubernetes-Containercluster fungiert als Container Service Extension-Plug-In für VMware Cloud Director. Das Plug-In steht auf der oberen Navigationsleiste unter **Mehr > Kubernetes-Containercluster** zur Verfügung.
- Stellen Sie sicher, dass Ihr Dienstanbieter die Einrichtung des Container Service Extension 3.0-Servers abgeschlossen und Container Service Extension-Metadaten für die TKGI-Aktivierung im Organisations-VDC veröffentlicht hat.
- Stellen Sie sicher, dass Sie über die Berechtigung **{cse}:PKS DEPLOY RIGHT** verfügen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Mehr > Kubernetes-Containercluster** aus.

- 2 Wählen Sie auf der Seite **Kubernetes-Containercluster** die Registerkarte **TKGI** aus und klicken Sie auf **Neu**.

Der Assistent **Neuen TKGI-Cluster erstellen** wird angezeigt.

- 3 Wählen Sie das Organisations-VDC aus, dem ein TKGI-Cluster bereitgestellt werden soll, und klicken Sie auf **Weiter**.

Das Laden der Liste kann unter Umständen etwas länger dauern, da VMware Cloud Director die Informationen vom CSE-Server abrufen.

- 4 Geben Sie einen Namen für den neuen TKGI-Cluster ein und wählen Sie die Anzahl der Worker-Knoten aus.

TKGI-Cluster müssen mindestens einen Worker-Knoten aufweisen.

- 5 Klicken Sie auf **Weiter**.

- 6 Überprüfen Sie die Clustereinstellungen und klicken Sie auf **Fertigstellen**.

- 7 (Optional) Klicken Sie auf die Schaltfläche **Aktualisieren** rechts auf der Seite für den neuen TKGI-Cluster, der in der Liste der Cluster angezeigt werden soll.

Nächste Schritte

- Passen Sie die Größe des Kubernetes-Clusters an, um die Anzahl der Worker-Knoten zu ändern.
- Laden Sie die Datei „kubecfg“ herunter. Das Befehlszeilenprogramm kubectl verwendet kubecfg-Dateien, um Informationen zu Clustern, Benutzern, Namespaces und Authentifizierungsmechanismen abzurufen.
- Löschen Sie ein Kubernetes-Cluster.

Konfigurieren des externen Zugriffs auf einen Dienst in einem Tanzu Kubernetes-Cluster

Ab VMware Cloud Director 10.2.2 sind Tanzu Kubernetes-Cluster standardmäßig nur über IP-Subnetze von Netzwerken innerhalb desselben Organisations-VDC erreichbar, in dem ein Cluster erstellt wird. Gegebenenfalls können Sie externen Zugriff auf bestimmte Dienste in einem Tanzu Kubernetes-Cluster manuell konfigurieren.

Bei der Veröffentlichung einer VDC-Kubernetes-Richtlinie in einem Organisations-VDC wird automatisch eine Firewallrichtlinie auf dem Cluster-Edge-Gateway bereitgestellt, um über autorisierte Quellen innerhalb des VDC Zugriff auf den Cluster zu gewähren. Darüber hinaus wird automatisch eine SNAT-Systemregel zu den NSX-T Data Center-Edge-Gateways innerhalb des Organisations-VDC hinzugefügt, um sicherzustellen, dass das Cluster-Edge-Gateway für die Arbeitslasten innerhalb des Organisations-VDC erreichbar ist.

Hinweis Wenn das Organisations-VDC zu einer NSX-T Data Center-Gruppe gehört, ist das Cluster-Edge-Gateway für die anderen VDCs in der Datencentergruppe nicht erreichbar.

Sowohl die Firewallrichtlinie, die auf dem Cluster-Edge-Gateway bereitgestellt wird, als auch die SNAT-Regel auf dem NSX-T Data Center-Edge-Gateway können nur entfernt werden, wenn ein **Systemadministrator** die Kubernetes-Richtlinie aus dem VDC löscht.

Bei Bedarf können Sie den Zugriff über ein externes Netzwerk auf einen bestimmten Dienst in einem Tanzu Kubernetes-Cluster konfigurieren. Hierzu müssen Sie eine DNAT-Regel auf dem NSX-T Data Center-Edge-Gateway erstellen, mit der sichergestellt wird, dass der von externen Standorten kommende Datenverkehr an das Cluster-Edge-Gateway weitergeleitet wird.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Cloud-Infrastruktur von vSphere 7.0 Update 1C, 7.0 Update 2 oder höher gestützt wird. Wenden Sie sich an Ihren **Systemadministrator**.
- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben.
- Stellen Sie sicher, dass Ihr **Systemadministrator** ein NSX-T Data Center-Edge-Gateway innerhalb des Organisations-VDC erstellt hat, in dem sich der Tanzu Kubernetes-Cluster befindet.
- Stellen Sie sicher, dass die für den Dienst zu veröffentlichende IP-Adresse der Edge-Gateway-Schnittstelle zugeteilt wurde, der Sie eine DNAT-Regel hinzufügen möchten.
- Verwenden Sie den Befehl `get services my-service` des `kubectl`-Befehlszeilentools, um die externe IP für den anzuzeigenden Dienst abzurufen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway und dann unter **Dienste** auf **NAT**.
- 3 Klicken Sie auf **Neu**, um eine Regel hinzuzufügen.
- 4 Konfigurieren Sie eine DNAT-Regel für den Dienst, den Sie mit einem externen Netzwerk verbinden möchten.

Option	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Regel ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.
Zustand	Um die Regel bei der Erstellung zu aktivieren, verwenden Sie die Umschaltoption Zustand .
Schnittstellentyp	Wählen Sie im Dropdown-Menü die Option „DNAT“ aus.
Externe IP	Geben Sie die öffentliche IP-Adresse des Diensts ein. Die eingegebenen IP-Adressen müssen zum unterzugewiesenen IP-Bereich des NSX-T Data Center-Edge-Gateways gehören.
Anwendung	Lassen Sie das Feld leer.
Interne IP	Geben Sie die IP-Adresse des Diensts ein, die über den Kubernetes-Ingress-Pool zugeteilt wurde.

Option	Beschreibung
Interner Port	(Optional) Geben Sie eine Portnummer ein, an die der eingehende Datenverkehr geleitet wird.
Protokollierung	(Optional) Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung .

5 Klicken Sie auf **Speichern**.

Nächste Schritte

Wenn Sie Zugriff auf andere Anwendungen bereitstellen möchten, die als Kubernetes-Dienste aus externen Netzwerken veröffentlicht werden, müssen Sie zusätzliche DNAT-Regeln für jede dieser Anwendungen konfigurieren.

Zum Bereitstellen einer hochflexiblen und sicheren Netzwerkinfrastruktur in einer Cloudumgebung für unterschiedliche Zwecke verwendet VMware Cloud Director eine Netzwerkarchitektur mit Layern, die vier Kategorien für Netzwerke aufweist. Die Netzwerkategorien lauten wie folgt: Externe Netzwerke, VDC-Organisationsnetzwerke, Datacenter-Gruppennetzwerke und vApp-Netzwerke. Die meisten VMware Cloud Director-Netzwerktypen erfordern zusätzliche Infrastrukturobjekte, wie z. B. Edge-Gateways und Netzwerkpools.

Externe Netzwerke

Ein externes Netzwerk stellt eine Uplink-Schnittstelle bereit, die Netzwerke und virtuelle Maschinen Ihrer VMware Cloud Director-Umgebung mit einem Netzwerk außerhalb des Systems verbindet, z. B. einem VPN, einem Unternehmensintranet oder dem öffentlichen Internet.

Ein externes Netzwerk wird entweder durch ein einzelnes vSphere-Netzwerk, durch mehrere vSphere-Netzwerke oder durch einen logischen NSX-T Data Center-Tier-0-Router gestützt.

Nur ein **Systemadministrator** kann ein externes Netzwerk erstellen. Informationen zu externen Netzwerken finden Sie unter *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Sammlung von isolierten Layer-2-Netzwerksegmenten, die Sie zum Erstellen von vApp-Netzwerken und bestimmten VDC-Organisationsnetzwerktypen nach Bedarf verwenden können.

Netzwerkpools müssen vor VDC-Organisationsnetzwerken und vApp-Netzwerken erstellt werden. Wenn sie nicht vorhanden sind, ist die einzige einer Organisation zur Verfügung stehende Netzwerkooption die direkte Verbindung mit einem externen Netzwerk.

Nur ein **Systemadministrator** kann einen Netzwerkpool erstellen.

Informationen zu externen Netzwerkpools finden Sie unter *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

VDC-Organisationsnetzwerke

VDC-Organisationsnetzwerke ermöglichen vApps die Kommunikation miteinander oder mit externen Netzwerken außerhalb der Organisation.

Je nach Verbindung des VDC-Organisationsnetzwerks mit einem externen Netzwerk gibt es verschiedene VDC-Organisationsnetzwerktypen.

Diese VDC-Organisationsnetzwerke stellen direkte oder weitergeleitete Verbindungen zu externen Netzwerken bereit. Sie können aber auch von externen Netzwerken und anderen Organisations-VDC-Netzwerken isoliert werden. Weitergeleitete Verbindungen erfordern ein Edge-Gateway und einen Netzwerkpool im Organisations-VDC.

Ein **Systemadministrator** oder **Organisationsadministrator** erstellt VDC-Organisationsnetzwerke und weist diese Ihrer Organisation zu.

Einem neu erstellten Organisations-VDC stehen keine Netzwerke zur Verfügung. Nachdem ein **Systemadministrator** die erforderliche Netzwerkinfrastruktur erstellt hat, kann ein **Organisationsadministrator** die meisten VDC-Organisationsnetzwerktypen erstellen und verwalten.

Von NSX Data Center for vSphere gestützte Datencenter-Gruppennetzwerke

Ein von NSX Data Center for vSphere gestütztes Netzwerk, das eine Datencenter-Gruppe umfasst. Eine Datencenter-Gruppe kann zwischen einem und 16 Organisations-VDCs in einer VMware Cloud Director-Bereitstellung mit einer einzigen oder mehreren Sites enthalten.

Von NSX-T Data Center gestützte Datencenter-Gruppennetzwerke

Datencenter-Gruppennetzwerke sind VDC-Organisationsnetzwerke, die von einem oder mehreren VDCs gemeinsam genutzt werden und mit denen vApps eine Verbindung herstellen können.

Ein **Systemadministrator** oder ein **Organisationsadministrator** erstellt Datencenter-Gruppennetzwerke und legt ihren Geltungsbereich auf eine einzelne VDC-Gruppe fest.

VMware Cloud Director unterstützt isolierte, importierte, direkte und geroutete Datencentergruppen-Netzwerke, die von NSX-T Data Center gestützt werden.

vApp-Netzwerke

Mit vApp-Netzwerken können virtuelle Maschinen miteinander kommunizieren. Sie können auch mit virtuellen Maschinen in anderen vApps kommunizieren, indem sie eine Verbindung mit einem VDC-Organisationsnetzwerk herstellen.

Ein vApp-Netzwerk ist in einer vApp enthalten. Ein vApp-Netzwerk kann von anderen Netzwerken isoliert oder mit einem VDC-Organisationsnetzwerk verbunden sein.

Jede vApp enthält ein vApp-Netzwerk. Das Netzwerk wird erstellt, wenn die vApp bereitgestellt wird. Es wird gelöscht, wenn die Bereitstellung der vApp aufgehoben wird.

Ein **Organisationsadministrator** richtet vApp-Netzwerke ein und steuert diese.

Netzwerktypen in einer vApp

Die virtuellen Maschinen in einer vApp können eine Verbindung zu vApp-Netzwerken, die isoliert, direkt oder geroutet werden können, sowie zu VDC-Organisationsnetzwerken herstellen.

Hinweis Virtuelle Organisations-VDCs, die auf NSX Data Center for vSphere basieren, unterstützen geroutete, isolierte und direkte vApp-Netzwerke.

Organisations-VDCs, die auf NSX-T Data Center basieren, unterstützen isolierte und direkte vApp-Netzwerke.

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 Netzwerk zuerst der vApp hinzufügen.

Eine vApp kann vApp-Netzwerke und VDC-Organisationsnetzwerke enthalten. 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 mit Fencing umgrenzen. Durch das Fencing der vApp können Sie die virtuellen Maschinen ohne Konflikt einschalten, indem Sie ihre MAC- und IP-Adressen isolieren.

Informationen hierzu finden Sie unter [Arbeiten mit Netzwerken in einer vApp](#).

Edge-Gateways

Ein Edge-Gateway stellt für ein VDC-Organisationsnetzwerk mit Routing die Konnektivität zu anderen Netzwerken her und kann Dienste wie Lastausgleich, Netzwerkadressübersetzung (NAT) und eine Firewall bereitstellen. VMware Cloud Director unterstützt IPv4- und IPv6-Edge-Gateways.

Für Edge-Gateways ist NSX Data Center for vSphere oder NSX-T Data Center erforderlich.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von VDC-Organisationsnetzwerken](#)

- [Verwalten von Datencenter-Gruppennetzwerken mit NSX-T Data Center](#)
- [Verwalten von Datencenter-Gruppennetzwerken mit NSX Data Center for vSphere](#)
- [Verwalten von NSX Data Center for vSphere-Edge-Gateways-Diensten](#)
- [Verwalten von NSX-T Data Center-Edge-Gateways](#)

Verwalten von VDC-Organisationsnetzwerken

Ein **Systemadministrator** oder **Organisationsadministrator** erstellt VDC-Organisationsnetzwerke und weist diese Ihrem Organisations-VDC oder einer Organisations-VDC-Gruppe zu. Ein **Organisationsadministrator** kann Informationen zu Netzwerken anzeigen, Netzwerkdienste konfigurieren usw.

Sie können direkte, geroutete, isolierte oder Datencenter-Gruppen-VDC-Organisationsnetzwerke verwenden, die von NSX Data Center for vSphere gestützt werden.

Sie können geroutete, isolierte, importierte und direkte VDC-Organisationsnetzwerke verwenden, die von NSX-T Data Center gestützt werden. Sie können auch geroutete, isolierte und importierte Datencenter-Gruppennetzwerke verwenden, die von NSX-T Data Center gestützt werden.

Tabelle 5-1. Typen von VDC-Organisationsnetzwerken

Netzwerk vom Typ „Datencenter“	Beschreibung
Direkt	<p>Ein VDC-Organisationsnetzwerk mit einer direkten Verbindung zu einem der externen Netzwerke, die vom Systemadministrator bereitgestellt und von vSphere-Ressourcen gestützt werden.</p> <p>Direkte Netzwerke werden für Organisations-VDCs unterstützt, die von NSX Data Center for vSphere gestützt werden, und ab VMware Cloud Director 10.2.2 für Organisations-VDCs, die von NSX-T Data Center gestützt werden.</p> <p>Auf direkte Netzwerke kann von mehreren Organisations-VDCs zugegriffen werden.</p> <p>Zu verschiedenen Organisations-VDCs gehörende virtuelle Maschinen können sich mit diesem Netzwerk verbinden und den Datenverkehr dieses Netzwerkes sehen.</p> <p>Ein direktes 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>Auf isolierte Netzwerke kann nur über dasselbe Organisations-VDC zugegriffen werden. Nur virtuelle Maschinen in diesem Organisations-VDC können sich mit dem internen VDC-Organisationsnetzwerk verbinden und den Datenverkehr im internen Netzwerk sehen.</p> <p>Isolierte Netzwerke werden für Organisations-VDCs unterstützt, die von NSX-T Data Center und Organisations-VDC NSX Data Center for vSphere gestützt werden.</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>
Weitergeleitet	<p>Auf geroutete Netzwerke kann nur über dasselbe Organisations-VDC zugegriffen werden. 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. 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>
Importierter logischer NSX-T Data Center-Switch	<p>Importierte NSX-T Data Center-Netzwerke sind logische Segmente, die in NSX-T Data Center erstellt werden und einen vorhandenen logischen NSX-T Data Center-Switch verwenden. Sie werden in einer bestimmten Organisation als VDC-Organisationsnetzwerk importiert.</p> <hr/> <p>Hinweis Nur ein Systemadministrator kann ein NSX-T Data Center-Netzwerk importieren.</p> <hr/>

Tabelle 5-1. Typen von VDC-Organisationsnetzwerken (Fortsetzung)

Netzwerk vom Typ „Datencenter“	Beschreibung
Von NSX Data Center for vSphere gestützte Datencenter-Gruppennetzwerke	<p>Dieses Netzwerk ist Teil eines Datencenter-Gruppennetzwerks, das sich über eine Datencenter-Gruppe erstreckt. Eine Datencenter-Gruppe kann zwischen einem und 16 Organisations-VDCs in einer VMware Cloud Director-Bereitstellung mit einer einzigen oder mehreren Sites enthalten.</p> <p>Die mit diesem Netzwerk verbundenen virtuellen Maschinen sind mit dem zugrunde liegenden ausgeweiteten Netzwerk verbunden.</p>
Von NSX-T Data Center gestützte Datencenter-Gruppennetzwerke	<p>Datencenter-Gruppennetzwerke sind von NSX-T Data Center gestützte VDC-Organisationsnetzwerke, die von einem oder mehreren VDCs gemeinsam genutzt werden und mit denen vApps eine Verbindung herstellen können.</p> <p>Datencenter-Gruppennetzwerke können isoliert, importiert oder geroutet werden und erfordern NSX-T Data Center.</p>

Alle Schritte zur Verwaltung Ihrer VDC-Organisationsnetzwerke werden unter der Annahme dokumentiert, dass Sie über mehrere VDCs verfügen.

Anzeigen der verfügbaren VDC-Organisationsnetzwerke

Sie können die verfügbaren VDC-Organisationsnetzwerke anzeigen.

Voraussetzungen

Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.

Verfahren

- ◆ Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.

Ergebnisse

Auf der Registerkarte **Netzwerke** sehen Sie eine Liste der verfügbaren Netzwerke, die Sie nach unterschiedlichen Kriterien filtern können.

Nächste Schritte

Sie können ein VDC-Organisationsnetzwerk hinzufügen. Sie können auch den Bereich bearbeiten oder vergrößern sowie ein vorhandenes VDC-Organisationsnetzwerk 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 Dienstleister 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 in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.
- 3 Wählen Sie auf der Seite **Bereich** die Option **Organisations-VDC** aus, wählen Sie ein VDC aus, in dem das Netzwerk erstellt werden soll, und klicken Sie auf **Weiter**.
- 4 Wählen Sie auf der Seite **Netzwerktyp auswählen** die Option **Isoliert** aus und klicken Sie auf **Weiter**.
- 5 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 6 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.
- 7 Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 8 (Optional) Wenn das VDC, in dem Sie das Netzwerk erstellen, von NSX Data Center for vSphere gestützt wird, aktivieren Sie die Option **Gemeinsam genutzt**, um das VDC-Organisationsnetzwerk anderen Organisations-VDCs in derselben Organisation zur Verfügung zu stellen.

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.

- 9 Klicken Sie auf **Weiter**.

10 (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**.

Um mehrere statische IP-Adressen oder -Bereiche hinzuzufügen, wiederholen Sie diesen Schritt.

- b (Optional) Um IP-Adressen und Bereiche zu ändern oder zu entfernen, klicken Sie auf **Ändern** oder **Entfernen**.

11 Klicken Sie auf **Weiter**.

12 (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.

13 Klicken Sie auf **Weiter**.

14 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Einstellungen 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 in der oberen Navigationsleiste auf **Netzwerk**.

- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.
- 3 Wählen Sie auf der Seite **Bereich** die Option **Organisations-VDC** aus, wählen Sie ein VDC aus, in dem das Netzwerk erstellt werden soll, und klicken Sie auf **Weiter**.
- 4 Wählen Sie auf der Seite **Netzwerktyp auswählen** die Option **Weitergeleitet** aus und klicken Sie auf **Weiter**.
- 5 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 6 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.
- 7 Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 8 (Optional) Wenn das VDC, in dem Sie das Netzwerk erstellen, von NSX Data Center for vSphere gestützt wird, aktivieren Sie die Option **Gemeinsam genutzt**, um das VDC-Organisationsnetzwerk anderen Organisations-VDCs in derselben Organisation zur Verfügung zu stellen.

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.

- 9 Klicken Sie auf **Weiter**.
- 10 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.

- 11 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. VMware Cloud Director identifiziert das zu verwendende Netzwerk zum Erweitern über L2 VPN. VMware Cloud Director erstellt mithilfe der NSX-Netzwerkvirtualisierung einen Trunk-Schnittstellentyp für dieses Netzwerk. Die maximal zulässige Anzahl Netzwerke ist 200.

- 12 (Optional) Um das Tagging von Gast-VLANs in diesem Netzwerk zu aktivieren, aktivieren Sie die Option **Gast-VLAN zulässig**.
- 13 Klicken Sie auf **Weiter**.
- 14 (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**.
- 15 Klicken Sie auf **Weiter**.
- 16 (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.

- 17 Klicken Sie auf **Weiter**.
- 18 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Einstellungen 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.

Ab VMware Cloud Director 10.2.2 wird direkte Netzwerkerstellung in Organisations-VDCs unterstützt, die von NSX-T Data Center und NSX Data Center for vSphere gestützt werden.

Wenn Sie sich beim VMware Cloud 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

Vergewissern Sie sich, dass Sie über **Systemadministrator**-Rechte verfügen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.
- 3 Wählen Sie auf der Seite **Bereich** die Option **Organisations-VDC** aus, wählen Sie ein VDC aus, in dem das Netzwerk erstellt werden soll, und klicken Sie auf **Weiter**.
- 4 Wählen Sie auf der Seite **Netzwerktyp** die Option **Direkt** aus und klicken Sie auf **Weiter**.
- 5 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 6 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**.
- 8 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**.
- 9 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Einstellungen und klicken Sie auf **Fertigstellen**.

Hinzufügen eines VDC-Organisationsnetzwerks mit einem importierten logischen NSX-T Data Center-Switch

Systemadministratoren können ein VDC-Organisationsnetzwerk erstellen, indem sie einen logischen Switch aus einer zugeordneten NSX-T Manager-Instanz importieren.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über **Systemadministrator**-Rechte verfügen.
- Vergewissern Sie sich, dass dem Provider-VDC, das das virtuelle Datacenter der Zielorganisation stützt, eine NSX-T Manager-Instanz zugeordnet ist.

- Sie müssen mindestens einen logischen NSX-T-Switch erstellen, der nicht von anderen VDC-Organisationsnetzwerken verwendet wird.

Informationen zum Erstellen und Konfigurieren von logischen NSX-T-Switches finden Sie im *NSX-T Data Center-Verwaltungshandbuch*.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.
- 3 Wählen Sie auf der Seite **Bereich** die Option **Organisations-VDC** aus, wählen Sie ein VDC aus, in dem das Netzwerk erstellt werden soll, und klicken Sie auf **Weiter**.
- 4 Wählen Sie auf der Seite **Netzwerktyp** die Option **Importiert** und dann **Logischer NSX-T-Switch** aus und klicken Sie anschließend auf **Weiter**.
- 5 Wählen Sie aus der Liste der verfügbaren logischen NSX-T-Switches den Ziel-Switch aus und klicken Sie auf **Weiter**.
- 6 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 7 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.
Wenn der Switch mit einem Subnetz konfiguriert ist, sind diese Informationen bereits vorausgefüllt.
- 8 Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 9 Klicken Sie auf **Weiter**.
- 10 (Optional) Konfigurieren Sie die DNS-Einstellungen und den statischen IP-Pool.
Sie können mehrere IP-Adressen und IP-Bereiche hinzufügen.
- 11 Klicken Sie auf **Weiter**.
- 12 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Einstellungen und klicken Sie auf **Fertigstellen**.

Bearbeiten der allgemeinen Einstellungen eines VDC-Organisationsnetzwerks

Sie können die Eigenschaften von VDC-Organisationsnetzwerken ändern.

Voraussetzungen

Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf den Namen des VDC-Organisationsnetzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie auf der Registerkarte **Allgemein** auf **Bearbeiten**.
 - a Bearbeiten Sie den Namen und die Beschreibung des Netzwerks.
 - b Wenn das VDC, in dem Sie das Netzwerk erstellt haben, von NSX Data Center for vSphere gestützt wird, aktivieren oder deaktivieren Sie die Option **Gemeinsam genutzt**, um das VDC-Organisationsnetzwerk anderen Organisations-VDCs in derselben Organisation zur Verfügung zu stellen.
- 4 Klicken Sie auf **Speichern**.

Verbinden eines VDC-Organisationsnetzwerks mit einem Edge-Gateway

Nachdem Sie ein VDC-Organisationsnetzwerk erstellt haben, können Sie das Netzwerk mit einem Edge-Gateway verbinden.

Ab Version 10.1 unterstützt VMware Cloud Director die Verbindung zu einem Edge-Gateway für VDC-Organisationsnetzwerke, die entweder von NSX Data Center for vSphere oder NSX-T Data Center gestützt werden.

Voraussetzungen

Für diesen Vorgang ist die vordefinierte Rolle **Organisationsadministrator** oder **Systemadministrator** bzw. eine Rolle erforderlich, die die für die Organisation veröffentlichten Rechte **VDC-Organisationsnetzwerk: Eigenschaften bearbeiten** und **VDC-Gruppe: Anzeigen** beinhaltet.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des VDC-Organisationsnetzwerks, das Sie mit einem Edge-Gateway verbinden möchten.
- 3 Klicken Sie auf der Registerkarte **Allgemein** auf **Bearbeiten**.
- 4 Klicken Sie auf **Verbindung**.
- 5 Verbinden Sie das Netzwerk mit einem Edge-Gateway.
 - a Aktivieren Sie die Option **Verbindung zu einem Edge-Gateway herstellen**.
 - b Wählen Sie in der Liste der verfügbaren Edge-Gateways das Edge-Gateway aus, mit dem eine Verbindung hergestellt werden soll.

- c Wählen Sie den Schnittstellentyp aus.
- d Um ein Gast-VLAN zuzulassen, aktivieren Sie die Option **Gast-VLAN zulässig**.

6 Klicken Sie auf **Speichern**.

Ergebnisse

Das VDC-Organisationsnetzwerk verbindet sich mit einem Edge-Gateway und konvertiert von isoliert nach geroutet.

Trennen eines VDC-Organisationsnetzwerks von einem Edge-Gateway

Indem Sie ein VDC-Organisationsnetzwerk von einem Edge-Gateway trennen, können Sie das Netzwerk von geroutet in isoliert konvertieren.

Ab Version 10.1 wird das Verbinden zu und Trennen von einem Edge-Gateway für VDC-Organisationsnetzwerke unterstützt, die entweder von NSX Data Center for vSphere oder NSX-T Data Center gestützt werden.

Voraussetzungen

Für diesen Vorgang ist die vordefinierte Rolle **Organisationsadministrator** oder **Systemadministrator** bzw. eine Rolle erforderlich, die das Recht **VDC-Organisationsnetzwerk: Eigenschaften bearbeiten** beinhaltet.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des VDC-Organisationsnetzwerks, das Sie trennen möchten.
- 3 Klicken Sie auf der Registerkarte **Allgemein** auf **Bearbeiten**.
- 4 Klicken Sie auf **Verbindung**.
- 5 Um das Netzwerk vom Edge-Gateway zu trennen, deaktivieren Sie die Option **Verbindung zu einem Edge-Gateway herstellen**.
- 6 Klicken Sie auf **Speichern**.

Ergebnisse

Sie haben das VDC-Organisationsnetzwerk von einem Edge-Gateway getrennt. Das VDC-Organisationsnetzwerk wird von geroutet in isoliert 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 in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des VDC-Organisationsnetzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie auf der Registerkarte **Allgemein** auf **Bearbeiten**.
- 4 Klicken Sie auf **Verbindung**.
- 5 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. VMware Cloud Director identifiziert das zu verwendende Netzwerk zum Erweitern über L2 VPN. VMware Cloud Director erstellt mithilfe der NSX-Netzwerkvirtualisierung einen Trunk-Schnittstellentyp für dieses Netzwerk. Die maximal zulässige Anzahl Netzwerke ist 200.

- 6 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

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.

- 2 Klicken Sie auf den Namen des Netzwerks, für das Sie die verwendeten IP-Adressen anzeigen möchten.
- 3 Klicken Sie im Abschnitt **IP-Verwaltung** auf **IP-Nutzung**, um zu sehen, 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

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie im Abschnitt **IP-Verwaltung** auf die Registerkarte **Statische IP-Pools**.
- 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

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie im Abschnitt **IP-Verwaltung** auf **Statische IP-Pools**.
- 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

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes oder geroutetes VDC-Organisationsnetzwerk handelt.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie im Abschnitt **IP-Verwaltung** auf **DNS**.

- 4 Klicken Sie auf der rechten Seite auf die Schaltfläche **Bearbeiten**.
- 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, das von NSX Data Center for vSphere gestützt wird. 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.

Ab Version 10.2 unterstützt VMware Cloud Director DHCP-Einstellungen sowohl für IPv4 als auch für IPv6. Sie können IPv6-Einstellungen mithilfe der VMware Cloud Director-API konfigurieren.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes VDC-Organisationsnetzwerk handelt.
- Stellen Sie sicher, dass Ihr Netzwerk von NSX Data Center for vSphere gestützt wird.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie im Abschnitt **IP-Verwaltung** auf **DHCP**.
- 4 Klicken Sie zum Aktivieren von DHCP rechts von **DHCP-Pool-Dienst** auf **Bearbeiten**.
- 5 Aktivieren Sie den **DHCP-Pool-Dienst** und klicken Sie auf **Speichern**.

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

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

- a Klicken Sie auf **Neu**.
- 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.

- 7 Klicken Sie auf **Speichern**.

Hinzufügen eines DHCP-Pools zu einem gerouteten VDC-Organisationsnetzwerk, das von NSX-T Data Center gestützt wird

Sie können DHCP-Pools zu einem gerouteten VDC-Organisationsnetzwerk hinzufügen, das von NSX-T Data Center gestützt wird.

Hinweis Das Löschen oder Aktualisieren von DHCP-Pools wird für VDC-Organisationsnetzwerke, die von NSX-T Data Center gestützt werden, nicht unterstützt.

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 VDC-Organisationsnetzwerk handelt.
- Stellen Sie sicher, dass Ihr Netzwerk von NSX-T Data Center gestützt wird.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie im Abschnitt **IP-Verwaltung** auf „DHCP“.
- 4 Klicken Sie auf **Neu**, um einen DHCP-Pool hinzuzufügen.
- 5 Geben Sie einen IPv4-Adressbereich für den Pool ein.
- 6 Klicken Sie auf **Speichern**.

Bearbeiten oder Löschen eines vorhandenen DHCP-Pools für ein isoliertes VDC-Organisationsnetzwerk, das von NSX Data Center for vSphere gestützt wird

Wenn Sie in Ihrem isolierten VDC-Organisationsnetzwerk keinen DHCP-Pool mehr benötigen, können Sie den von NSX Data Center for vSphere gestützten Pool entweder löschen oder bearbeiten.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass es sich bei Ihrem Netzwerk um ein isoliertes VDC-Organisationsnetzwerk handelt.
- Stellen Sie sicher, dass das VDC-Organisationsnetzwerk von NSX Data Center for vSphere gestützt wird.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf den Namen des Netzwerks, das Sie bearbeiten möchten.
- 3 Klicken Sie auf den Abschnitt **IP-Verwaltung** und dann auf **DHCP**.
- 4 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 in der oberen Navigationsleiste auf **Netzwerk**.
- 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 in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Netzwerks und dann auf **Löschen**.
- 3 Klicken Sie zur Bestätigung auf **OK**.

Verwalten von Datencenter-Gruppennetzwerken mit NSX-T Data Center

Ab Version 10.2 unterstützt VMware Cloud Director von NSX-T Data Center gestützte Datencenter-Gruppennetzwerke.

Um ein Netzwerk über mehrere Organisations-VDCs zu erstellen, gruppieren Sie zuerst die VDCs und erstellen dann ein Gruppennetzwerk, das von diesen gemeinsam genutzt wird.

Von NSX-T Data Center gestützte Datencenter-Gruppennetzwerke bieten die gemeinsame Nutzung von Netzwerken auf Ebene 2, die Konfiguration eines einzelnen aktiven Egress-Punkts sowie Distributed Firewall-Regeln (DFW), die auf eine Datencenter-Gruppe angewendet werden.

Datencenter-Gruppe

Eine Datencenter-Gruppe fungiert als ein VDC-übergreifender Router, der zentralisierte Netzwerkverwaltung, Egress-Punktkonfiguration und Ost-West-Datenverkehr zwischen allen Netzwerken innerhalb der Gruppe bereitstellt. Eine Datencenter-Gruppe kann zwischen einem und 16 VDCs enthalten, die zur gemeinsamen Nutzung eines aktiven Egress-Punkts konfiguriert sind.

Verfügbarkeitszone

Eine Verfügbarkeitszone stellt die Computing-Cluster oder -Fehlerdomänen dar, die für das Netzwerk verfügbar sind. Standardmäßig ist die Verfügbarkeitszone des Provider-VDC.

Wichtig Ihr **Systemadministrator** muss die Verfügbarkeitszonen für Gruppennetzwerke mit NSX-T Data Center konfigurieren, indem er einen Wert für den Computing-Anbieter-Geltungsbereich für die vCenter Server-Instanz und optional für die von der vCenter Server-Instanz gestützten Provider-VDCs festlegt. Standardmäßig wird der Computing-Anbieter-Geltungsbereich eines Provider-VDC von der vCenter Server-Instanz kopiert, die dieses VDC stützt. Ein **Systemadministrator** kann den Computing-Anbieter-Geltungsbereich für verschiedene Provider-VDCs, die von einer einzelnen vCenter Server-Instanz gestützt werden, differenzieren. Beispielsweise können Sie eine vCenter Server-Instanz mit dem Geltungsbereich **Deutschland** und ein Provider-VDC mit dem Bereich **München** haben.

Ihr **Systemadministrator** kann auch die Verfügbarkeitszone neu konfigurieren, sodass sie mit dem Geltungsbereich des Netzwerkanbieters identisch ist, der in der Regel die zugrunde liegende vCenter Server-Instanz mit dem zugeordneten NSX-T Manager darstellt.

Egress-Punkt

Ein vorhandenes NSX-T Data Center-Edge-Gateway, das Sie zur Herstellung einer Verbindung zwischen einer Datencenter-Gruppe und einem externen Netzwerk konfigurieren.

Datencenter-Gruppennetzwerk

Ein Layer-2-Netzwerk, das von allen VDCs in einer Datencenter-Gruppe gemeinsam genutzt wird.

Verwalten von Datencenter-Gruppen mit NSX-T Data Center als Typ des Netzwerkanbieters

Nach der Erstellung einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters können Sie Datencenter der Gruppe hinzufügen, daraus entfernen und die Gruppeneinstellungen bearbeiten.

Eine Datencenter-Gruppe kann maximal 16 virtuelle Datencenter enthalten.

VDCs, die Sie aus der Datencenter-Gruppe entfernen, dürfen keine Arbeitslasten aufweisen, die an zur Datencenter-Gruppe gehörende Netzwerke angehängt sind.

Erstellen einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters

Sie können zwischen 1 und 16 VDCs in einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters zusammenfassen.

Voraussetzungen

Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** oder **Systemadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.
- 2 Klicken Sie auf **Neu**.
- 3 Wählen Sie auf der Seite **Erstes VDC** ein von NSX-T Data Center gestütztes VDC aus, um die Gruppe zu starten.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die neue Datencenter-Gruppe ein.
- 5 Wählen Sie auf der Seite **Teilnehmende VDCs** weitere Datencenter für die neue Datencenter-Gruppe aus und klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die Details der Datencenter-Gruppe und klicken Sie auf **Fertigstellen**.

Ergebnisse

Die neu erstellte Gruppe wird in der Liste der Datencenter-Gruppen angezeigt.

Nächste Schritte

Erstellen Sie ein Netzwerk, das die Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters umfasst.

Anzeigen und Bearbeiten der allgemeinen Einstellungen einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters

Sie können die Datencenter-Gruppen mit NSX-T Data Center als Typ des Netzwerkanbieters in Ihrer Organisation anzeigen und bearbeiten.

Voraussetzungen

Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder über eine Rolle mit entsprechenden Rechten verfügen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.
Die Liste der Datencenter-Gruppen wird angezeigt.
- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie im Bereich **Allgemeine Einstellungen** auf **Bearbeiten**.
- 4 Bearbeiten Sie den Namen und optional die Beschreibung der Datencenter-Gruppe und klicken Sie zum Bestätigen des Vorgangs auf **Speichern**.

Verwalten der teilnehmenden VDCs in einer Datencenter-Gruppe

Sie können die VDCs auswählen, die an einer VDC-Gruppe teilnehmen und miteinander kommunizieren sollen.

Voraussetzungen

Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder über eine Rolle mit entsprechenden Rechten verfügen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.
Die Liste der Datencenter-Gruppen wird angezeigt.
- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie auf **Teilnehmende VDCs** und dann auf **Verwalten**.
- 4 Wählen Sie die in die Gruppe aufzunehmenden VDCs aus und klicken Sie zum Bestätigen des Vorgangs auf **Speichern**.

Synchronisieren einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters

Um sicherzustellen, dass alle VDCs, die zu einer Datencenter-Gruppe gehören, weiterhin vorhanden und ordnungsgemäß konfiguriert sind, können Sie die Datencenter-Gruppe synchronisieren.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.
Die Liste der Datencenter-Gruppen wird angezeigt.
- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie auf **Synchronisieren** und bestätigen Sie den Vorgang.

Verwenden einer Distributed Firewall in einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters

Ab Version 10.2 unterstützt VMware Cloud Director den Distributed Firewall-Dienst für Datencenter-Gruppen mit NSX-T Data Center als Typ des Netzwerkanbieters.

Wenn Sie eine Distributed Firewall für eine Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters aktivieren, erstellen Sie eine einzelne Standardsicherheitsrichtlinie, die auf die Datencenter-Gruppe angewendet wird.

Als **Organisationsadministrator** können Sie zusätzliche Distributed Firewall-Regeln erstellen und bearbeiten, die mit der Standardsicherheitsrichtlinie der Datencenter-Gruppe verknüpft sind.

Der Distributed Firewall-Dienst ist standardmäßig nicht aktiviert. Nach dem Aktivieren der Distributed Firewall können Sie IP Sets und Sicherheitsgruppen erstellen, um die Erstellung von Distributed Firewall-Regeln zu vereinfachen.

Hinweis Die von Ihnen erstellten Distributed Firewall-Regeln gelten nur für die Arbeitslasten, die an die Netzwerke der Datencenter-Gruppe angehängt wurden.

Aktivieren einer Distributed Firewall für eine Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzanbieters

Durch Verwendung einer Distributed Firewall können Sie einen Satz von Firewallregeln der Ebene 3 über eine einzelne Datencenter-Gruppe hinweg anwenden.

Distributed Firewalls sind standardmäßig nicht aktiviert. Wenn Sie diese Option aktivieren, erstellen Sie eine einzelne Standardsicherheitsrichtlinie.

Voraussetzungen

Vergewissern Sie sich, dass Sie die Rolle **Systemadministrator** haben.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie im Abschnitt **Distributed Firewall** auf **Aktivieren** und bestätigen Sie, dass Sie die Distributed Firewall aktivieren möchten.

Nächste Schritte

Erstellen Sie Distributed Firewall-Regeln.

Hinzufügen eines IP Sets zu einer Datencenter-Gruppe

Zum Erstellen von Distributed Firewall-Regeln und Hinzufügen dieser Regeln zu einer Datencenter-Gruppe müssen Sie zuerst IP Sets erstellen. IP Sets sind Gruppen von IP-Adressen und Netzwerken, auf die die Distributed Firewall-Regeln angewendet werden. Durch die Kombination mehrerer Objekte in IP Sets können Sie die Gesamtzahl der zu erstellenden Distributed Firewall-Regeln reduzieren.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie unter „Sicherheit“ auf **IP Sets**.

- 4 Klicken Sie auf **Neu**.
- 5 Geben Sie einen aussagekräftigen Namen und optional eine Beschreibung für das neue IP Set ein.
- 6 Geben Sie eine IPv4-, eine IPv6-Adresse oder einen Adressbereich im CIDR-Format ein und klicken Sie auf **Hinzufügen**.
- 7 Zum Ändern einer vorhandenen IP-Adresse oder eines vorhandenen Bereichs klicken Sie auf **Ändern** und bearbeiten Sie den Wert.
- 8 Klicken Sie zur Bestätigung auf **Speichern**.

Erstellen einer Sicherheitsgruppe in einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzerkanbieters

Bevor Sie Distributed Firewall-Regeln für eine Datencenter-Gruppe erstellen, können Sie Datencenter-Gruppennetzwerke in Sicherheitsgruppen zusammenfassen, für die die Regeln gelten.

Bei Sicherheitsgruppen handelt es sich um Datencenter-Gruppennetzwerke, für die Distributed Firewall-Regeln gelten. Durch das Zusammenfassen von Netzwerken können Sie die Gesamtzahl der zu erstellenden Distributed Firewall-Regeln reduzieren.

Voraussetzungen

Stellen Sie sicher, dass Sie über mindestens ein Datencenter-Gruppennetzwerk verfügen, das von NSX-T Data Center gestützt wird.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.
Die Liste der Datencenter-Gruppen wird angezeigt.
- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie unter „Sicherheit“ auf **Sicherheitsgruppen** und dann auf **Neu**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die Sicherheitsgruppe ein und klicken Sie auf **Speichern**.
Die neue Sicherheitsgruppe wird in der Liste angezeigt.
- 5 Wählen Sie die neu erstellte Sicherheitsgruppe aus und klicken Sie auf **Mitglieder verwalten**.
- 6 Wählen Sie die gewünschten Datencenter-Gruppennetzwerke aus, um sie zur Sicherheitsgruppe hinzuzufügen.
- 7 Klicken Sie auf **Speichern**.

Nächste Schritte

[Hinzufügen einer Distributed Firewall-Regel zu einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzerkanbieters](#)

Hinzufügen eines Anwendungsportprofils zu einer Datencenter-Gruppe

Zum Erstellen von Distributed Firewall-Regeln können Sie vorkonfigurierte und benutzerdefinierte Anwendungsportprofile verwenden.

Anwendungsportprofile enthalten eine Kombination aus einem Protokoll und einem Port oder einer Gruppe von Ports, die für Firewall-Dienste verwendet werden. Zusätzlich zu den vorkonfigurierten Standard-Portprofilen können Sie benutzerdefinierte Anwendungsportprofile erstellen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.
Die Liste der Datencenter-Gruppen wird angezeigt.
- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie unter „Sicherheit“ auf **Anwendungsportprofile**.
- 4 Klicken Sie im Bereich **Benutzerdefinierte Anwendungen** auf **Neu**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für das Anwendungsportprofil ein.
- 6 Wählen Sie im Dropdown-Menü **Protokoll** das Protokoll aus.
- 7 Geben Sie einen Port oder einen durch Kommas getrennten Portbereich ein und klicken Sie auf **Speichern**.
- 8 Wiederholen Sie die Schritte, um zusätzliche Portprofile zu konfigurieren.

Nächste Schritte

Verwenden Sie die Anwendungsportprofile, um Distributed Firewall-Regeln zu erstellen.

Hinzufügen einer Distributed Firewall-Regel zu einer Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzerkanbieters

Die von Ihnen erstellten Distributed Firewall-Regeln gelten nur für Arbeitslasten, die an die Netzwerke der Datencenter-Gruppe angehängt wurden.

Voraussetzungen

Stellen Sie sicher, dass der Distributed Firewall-Dienst für die Datencenter-Gruppe aktiviert ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie auf die Registerkarte **Distributed Firewall** auf der linken Seite.
- 4 Klicken Sie auf **Regeln bearbeiten**.
- 5 Klicken Sie zum Hinzufügen einer Firewallregel auf **Neue oben**.
- 6 Konfigurieren Sie die Regel.

Option	Beschreibung
Name	Geben Sie einen Namen für die Regel ein.
Zustand	Um die Regel bei der Erstellung zu aktivieren, aktivieren Sie die Umschaltoption Zustand .
Anwendungen	(Optional) Zur Auswahl eines bestimmten Portprofils, für das die Regel gilt, aktivieren Sie die Umschaltoption Anwendungen und klicken auf Speichern .
Kontext	(Optional) Wählen Sie ein NSX-T Data Center-Kontextprofil für die Regel aus.
Quelle	<p>Wählen Sie den Quelldatenverkehr aus und klicken Sie auf Behalten.</p> <ul style="list-style-type: none"> ■ Um Datenverkehr von einer beliebigen Quelladresse zuzulassen oder zu verweigern, aktivieren Sie die Umschaltoption Beliebige Quelle. ■ Um Datenverkehr aus bestimmten IP Sets oder Sicherheitsgruppen zuzulassen oder zu verweigern, wählen Sie die IP Sets und Sicherheitsgruppen in der Liste aus.
Ziel	<p>Wählen Sie den Zieldatenverkehr aus und klicken Sie auf Behalten.</p> <ul style="list-style-type: none"> ■ Um Datenverkehr zu einer beliebigen Zieladresse zuzulassen oder zu verweigern, aktivieren Sie die Umschaltoption Beliebiges Ziel. ■ Um Datenverkehr in bestimmte IP Sets und Sicherheitsgruppen zuzulassen oder zu verweigern, wählen Sie die IP Sets und Sicherheitsgruppen in der Liste aus.
Aktion	<p>Wählen Sie im Dropdown-Menü Aktion aus, ob Datenverkehr von oder zu bestimmten Quellen zugelassen oder verweigert werden soll.</p> <ul style="list-style-type: none"> ■ Wählen Sie Annehmen aus, um Datenverkehr von oder zu den angegebenen Quellen, Zielen und Diensten zuzulassen. ■ Wählen Sie Verweigern aus, um Datenverkehr von oder zu den angegebenen Quellen, Zielen und Diensten zu blockieren.
IP-Protokoll	Wählen Sie aus, ob die Regel auf IPv4- oder IPv6-Datenverkehr angewendet werden soll.
Protokollierung aktivieren	Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung aktivieren .

- 7 Klicken Sie auf **Speichern**.
- 8 Wiederholen Sie die Schritte, um zusätzliche Regeln zu konfigurieren.

Ergebnisse

Nachdem Sie die Firewallregeln erstellt haben, werden sie in der Liste der Distributed Firewall-Regeln angezeigt. Sie können die Regeln nach Bedarf nach oben oder unten verschieben, bearbeiten oder löschen.

Deaktivieren der Standardrichtlinie für die verteilte Firewall

Wenn Sie den Dienst für verteilte Firewalls deaktivieren möchten, müssen Sie zuerst die Standardrichtlinie für die verteilte Firewall deaktivieren.

Wenn Sie die Standardrichtlinie deaktivieren, können Sie die Regeln für verteilte Firewalls bearbeiten, aber die Regeln werden nicht mehr angewendet.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie auf die Registerkarte **Verteilte Firewall** auf der linken Seite.
- 4 Klicken Sie auf der Karte **Standardrichtlinie** oberhalb der Liste mit Regeln für verteilte Firewalls auf **Deaktivieren** und bestätigen Sie die Aktion.

Ergebnisse

Die Standardrichtlinie ist deaktiviert. Die restlichen Regeln für verteilte Firewalls können bearbeitet werden, aber sie werden nicht angewendet.

Deaktivieren des Diensts für verteilte Firewalls

Wenn Sie den Dienst für verteilte Firewalls nicht verwenden möchten, können Sie ihn deaktivieren.

Wenn Sie den Dienst für verteilte Firewalls für eine Datencenter-Gruppe deaktivieren, wird die Konfiguration der Sicherheitsregeln für diese Gruppe dauerhaft gelöscht und kann nicht wiederhergestellt werden.

Voraussetzungen

[Deaktivieren der Standardrichtlinie für die verteilte Firewall](#)

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

3 Klicken Sie auf **Allgemein**.

4 Klicken Sie im Bereich **Verteilte Firewall** auf der rechten Seite auf **Deaktivieren** und bestätigen Sie den Vorgang.

Ergebnisse

Der Dienst für verteilte Firewalls ist deaktiviert, und die Konfiguration der Sicherheitsregeln wird gelöscht.

Verwalten von Datacenter-Gruppennetzwerken mit NSX-T Data Center als Typ des Netzanbieters

Nachdem Sie eine Datacenter-Gruppe erstellt und konfiguriert haben, können Sie Datacenter-Gruppennetzwerke erstellen und verwalten, die die beteiligten VDCs umfassen.

Sie können geroutete, isolierte und importierte Datacenter-Gruppennetzwerke der Organisation verwenden, die von NSX-T Data Center gestützt werden.

Ein Datacenter-Gruppennetzwerk kann nur auf eine einzelne Datacenter-Gruppe beschränkt werden.

Sie können den Geltungsbereich eines vorhandenen Netzwerks von einem Organisations-VDC auf eine Datacenter-Gruppe erweitern.

Einer Datacenter-Gruppe können alle Netzwerktypen hinzugefügt werden.

Wichtig Die IP-Adressen in den Netzwerken, die Teil einer Datacenter-Gruppe sind, dürfen sich nicht überlappen, auch wenn die Netzwerke isoliert sind.

Tabelle 5-2. Typen von Datacenter-Gruppennetzwerken

Typ des Datacenter-Gruppennetzwerks	Beschreibung
Isoliert	Auf ein isoliertes Datacenter-Gruppennetzwerk kann nur von VDCs in derselben Datacenter-Gruppe zugegriffen werden. Nur virtuelle Maschinen in der Datacenter-Gruppe können eine Verbindung zu dem isolierten Datacenter-Gruppennetzwerk herstellen und den Datenverkehr dieses Netzwerks anzeigen.
Weitergeleitet	Ein geroutetes Datacenter-Gruppennetzwerks bietet kontrollierten Zugriff auf ein externes Netzwerk über ein NSX-T Data Center-Edge-Gateway, das Teil der Datacenter-Gruppe ist.
Importiert	Ein importiertes Datacenter-Gruppennetzwerk verwendet einen vorhandenen logischen NSX-T Data Center-Switch. Nur ein Systemadministrator kann ein Netzwerk importieren.

Erstellen eines von NSX-T Data Center gestützten isolierten Datacenter-Gruppennetzwerks

Sie können ein isoliertes Datacenter-Gruppennetzwerk hinzufügen, auf das nur VMs in der Datacenter-Gruppe zugreifen können. VMs außerhalb dieses Netzwerks haben keine

Konnektivität zu diesem Netzwerk. Dabei spielt es keine Rolle, ob die VMs mit anderen Netzwerken in derselben Datencenter-Gruppe verbunden sind.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben.
- Vergewissern Sie sich, dass Sie eine Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters erstellt haben.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.
- 3 Wählen Sie auf der Seite **Bereich** die Option **Datencenter-Gruppe** und dann eine Gruppe mit NSX-T Data Center-Netzwerkanbieter aus, in der das Netzwerk erstellt werden soll.
- 4 Wählen Sie auf der Seite **Netzwerktyp** die Option **Isoliert** aus und klicken Sie auf **Weiter**.
- 5 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 6 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.
- 7 Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 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**.
Um mehrere statische IP-Adressen oder -Bereiche hinzuzufügen, wiederholen Sie diesen Schritt.
 - b (Optional) Um IP-Adressen und Bereiche zu ändern oder zu entfernen, klicken Sie auf **Ändern** oder **Entfernen**.
- 10 (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.

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

Erstellen eines von NSX-T Data Center gestützten gerouteten Datencenter-Gruppennetzwerks

Um den Zugriff auf ein externes Netzwerk zu steuern, können Sie ein geroutetes Datencenter-Gruppennetzwerk hinzufügen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder über eine Rolle mit entsprechenden Rechten verfügen.
- Vergewissern Sie sich, dass Sie eine Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzwerkanbieters erstellt haben.
- Vergewissern Sie sich, dass Sie ein vorhandenes NSX-T Data Center-Edge-Gateway auf die Datencenter-Gruppe zugeschnitten haben, in der Sie ein geroutetes Netzwerk erstellen möchten.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.
- 3 Wählen Sie auf der Seite **Bereich** die Option **Datencenter-Gruppe** und dann eine Gruppe mit NSX-T Data Center-Netzwerkanbieter aus, in der das Netzwerk erstellt werden soll.
- 4 Wählen Sie auf der Seite **Netzwerktyp** die Option **Geroutet** aus und klicken Sie auf **Weiter**.
Wenn nur ein verfügbares Edge-Gateway auf die Datencenter-Gruppe zugeschnitten ist, wird es dem Netzwerk automatisch zugewiesen.
- 5 Wenn der Datencenter-Gruppe mehr als ein NSX-T Data Center zur Verfügung steht, wählen Sie ein Edge-Gateway in der Liste aus und klicken Sie auf **Weiter**.
- 6 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 7 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.
- 8 Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 9 Klicken Sie auf **Weiter**.

- 10 (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**.

Um mehrere statische IP-Adressen oder -Bereiche hinzuzufügen, wiederholen Sie diesen Schritt.

- b (Optional) Um IP-Adressen und Bereiche zu ändern oder zu entfernen, klicken Sie auf **Ändern** oder **Entfernen**.

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

Erstellen eines Datacenter-Gruppennetzwerks mit einem importierten logischen NSX-T-Switch

Systemadministratoren können ein VDC-Organisationsnetzwerk erstellen, indem sie ein Segment aus einer zugeordneten NSX-T Manager-Instanz importieren.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Systemadministrator** haben.
- Vergewissern Sie sich, dass Sie eine Datacenter-Gruppe mit NSX-T Data Center als Typ des Netzanbieters erstellt haben.
- Vergewissern Sie sich, dass dem Provider-VDC, das die VDC-Zielgruppe stützt, eine NSX-T Manager-Instanz zugeordnet ist.
- Vergewissern Sie sich, dass Sie mindestens einen logischen NSX-T-Switch erstellt haben, der nicht von anderen Netzwerken verwendet wird. Informationen zum Erstellen und Konfigurieren von logischen NSX-T-Switches finden Sie im *NSX-T Data Center-Verwaltungshandbuch*.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.

- 3 Wählen Sie auf der Seite **Bereich** die Option **Datencenter-Gruppe** und dann eine Gruppe mit NSX-T Data Center-Netzwerkanbieter aus, in der das Netzwerk erstellt werden soll.
- 4 Wählen Sie auf der Seite **Netzwerktyp** die Option **Importiert** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie aus der Liste der verfügbaren logischen NSX-T-Switches den Ziel-Switch aus und klicken Sie auf **Weiter**.
- 6 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 7 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.
- 8 Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 9 Klicken Sie auf **Weiter**.
- 10 (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**.

Um mehrere statische IP-Adressen oder -Bereiche hinzuzufügen, wiederholen Sie diesen Schritt.
 - b (Optional) Um IP-Adressen und Bereiche zu ändern oder zu entfernen, klicken Sie auf **Ändern** oder **Entfernen**.
- 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 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Einstellungen und klicken Sie auf **Fertigstellen**.

Erweitern des Bereichs eines von NSX-T Data Center gestützten VDC-Organisationsnetzwerks

Nach dem Erweitern des Bereichs eines VDC-Organisationsnetzwerks auf ein Datencenter-Gruppennetzwerk können Sie Arbeitslasten aus allen Datencentern verbinden, die zur Datencenter-Gruppe gehören.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder über eine Rolle mit entsprechenden Rechten verfügen.
- Vergewissern Sie sich, dass Sie eine Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzerkanbieters erstellt haben.
- Vergewissern Sie sich, dass Sie ein von NSX-T Data Center gestütztes VDC-Organisationsnetzwerk erstellt haben.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf das Optionsfeld neben dem VDC-Organisationsnetzwerk, dessen Bereich erweitert werden soll, und klicken Sie auf **Bereich erweitern**.
- 3 Wählen Sie in der Liste der Datencenter-Gruppen eine Datencenter-Gruppe aus und klicken Sie zum Bestätigen des Vorgangs auf **OK**.

Ergebnisse

Der Bereich des Netzwerks wird auf ein Datencenter-Gruppennetzwerk erweitert. In der Liste „Netzwerke“ wird das Netzwerk als Bereich für die ausgewählte Datencenter-Gruppe aufgelistet.

Reduzieren des Bereichs eines von NSX-T Data Center gestützten Datencenter-Gruppennetzwerks

Sie können den Bereich eines von NSX-T Data Center gestützten Datencenter-Gruppennetzwerks auf ein VDC-Organisationsnetzwerk reduzieren.

Wenn Sie den Bereich eines Datencenter-Gruppennetzwerks auf ein einzelnes VDC-Organisationsnetzwerk reduzieren, stellen Sie Netzwerkonnktivität für Arbeitslasten bereit, die ausschließlich dem Organisations-VDC angehören.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder über eine Rolle mit entsprechenden Rechten verfügen.
- Vergewissern Sie sich, dass Sie ein VDC-Netzwerk erstellt haben, das auf eine Datencenter-Gruppe mit NSX-T Data Center als Typ des Netzerkanbieters zugeschnitten ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf das Optionsfeld neben dem Datencenter-Gruppennetzwerk, dessen Bereich reduziert werden soll, und klicken Sie auf **Bereich reduzieren**.
- 3 Wählen Sie in der Liste der zum Gruppennetzwerk gehörenden VDCs das VDC aus, auf das das Netzwerk zugeschnitten werden soll, und klicken Sie auf **OK**.

Ergebnisse

Der Bereich des Netzwerks wird auf ein einzelnes VDC-Organisationsnetzwerk reduziert.

Verwalten von Egress-Punkten für Datencentergruppen mit dem NSX-T Data Center als Typ des Netzanbieters

Zum Weiterleiten von Datenverkehr in ein Datencentergruppen-Netzwerk und aus einem solchen Netzwerk in ein externes Netzwerk können Sie ein NSX-T Data Center-Edge-Gateway als Egress-Punkt für eine Datencentergruppe konfigurieren.

Wenn Sie ein Edge-Gateway als Egress-Punkt für eine Datencenter-Gruppe konfigurieren, erweitern Sie seinen Geltungsbereich auf die Datencenter-Gruppe. Das Edge-Gateway wird von allen Datencentern gemeinsam genutzt, die an der Gruppe beteiligt sind. Alle an das Edge-Gateway angehängten gerouteten Netzwerke werden mit der Datencentergruppe verbunden und auf diese zugeschnitten.

Alle Edge-Gateway-Dienste bleiben Teil der Edge-Gateway-Funktionen. Weitere Informationen finden Sie unter [Verwalten von NSX-T Data Center-Edge-Gateways](#).

Wenn ein VDC Mitglied der Datencenter-Gruppe ist und an keines der gerouteten Netzwerke, die Teil des gewünschten Geltungsbereichs sind, Arbeitslasten angehängt sind, können Sie ein Edge-Gateway aus einer Datencenter-Gruppe entfernen und seinen Geltungsbereich auf ein einzelnes VDC festlegen.

Sie können ein Edge-Gateway einem isolierten Datencenter-Gruppennetzwerk hinzufügen und dieses in ein geroutetes Datencenter-Netzwerk umwandeln. Sie können auch die Verbindung mit einem Edge-Gateway aus einem Datencenter-Gruppennetzwerk entfernen, indem Sie das geroutete Netzwerk in ein isoliertes Datencenter-Gruppennetzwerk umwandeln.

Hinzufügen eines NSX-T Data Center-Edge-Gateways zu einer Datencenter-Gruppe

Um ein NSX-T Data Center-Edge-Gateway als Egress-Punkt für eine Datencenter-Gruppe zu konfigurieren, erweitern Sie den Geltungsbereich des Edge-Gateways. Das Gateway wird dann von allen Datencentern gemeinsam genutzt, die an der Gruppe beteiligt sind.

Wenn Sie ein Edge-Gateway auf eine Datencentergruppe zuschneiden, werden alle an das Edge-Gateway angehängten gerouteten Netzwerke mit der Datencentergruppe verbunden und auf diese angewendet.

Alle neuen gerouteten Netzwerke, die Sie an das Edge-Gateway anhängen, gehören zur Datencentergruppe.

Ein geroutetes Netzwerk, das an ein auf ein VDC zugeschnittenes Edge-Gateway angehängt ist, kann nur dann an einer Datencentergruppe teilnehmen, wenn der Bereich des Edge auf diese Datencentergruppe erweitert wird.

Voraussetzungen

Stellen Sie sicher, dass Sie ein vorhandenes NSX-T Data Center-Edge-Gateway mit einem der VDCs verknüpft haben, die zur Datencentergruppe gehören.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie auf **Edge-Gateway** und dann auf **Edge hinzufügen**.
- 4 Wählen Sie eines der verfügbaren Edge-Gateways aus und klicken Sie auf **Speichern**.

Ergebnisse

Der Bereich des Edge-Gateways wird auf die Datencentergruppe erweitert. Eine Änderung des Bereichs hat keine Auswirkungen auf vorhandene zugrunde liegende Dienste oder Netzwerke.

Reduzieren des Bereichs eines NSX-T Data Center-Edge-Gateways auf ein VDC

Sie können den Bereich eines NSX-T Data Center-Edge-Gateways auf ein bestimmtes VDC reduzieren, indem Sie das Edge-Gateway aus der Datencentergruppe entfernen, auf das es zugeschnitten ist.

Wenn Sie den Bereich eines Edge-Gateways auf ein bestimmtes VDC reduzieren, verbleiben alle vom Edge-Gateway verwendeten Sicherheitsgruppenobjekte im Gateway. Sicherheitsgruppen, die ausschließlich von der verteilten Firewall verwendet werden, bleiben Teil der VDC-Gruppe.

Voraussetzungen

- Stellen Sie sicher, dass das VDC, auf das Sie den Bereich des Edge-Gateways reduzieren möchten, ein Mitglied der Datencentergruppe ist.
- Stellen Sie sicher, dass keine Arbeitslasten an geroutete Netzwerke angehängt sind, die nicht zum Zielbereich des Edge-Gateways gehören.
- Stellen Sie sicher, dass sich keine Sicherheitsgruppen oder IP Sets in der Datencentergruppe befinden, die sowohl vom Edge-Gateway als auch von der verteilten Firewall verwendet werden.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.
- 3 Klicken Sie auf **Edge-Gateway** und dann auf **Edge entfernen**.

- 4 Wählen Sie ein VDC aus, auf das der Bereich des Edge-Gateways reduziert werden soll, und klicken Sie auf **Speichern**.

Verwalten von Datacenter-Gruppennetzwerken mit NSX Data Center for vSphere

Um ein Netzwerk über mehrere Organisations-VDCs zu erstellen, gruppieren Sie zuerst die virtuellen Datacenter und erstellen dann ein VDC-Netzwerk, dessen Geltungsbereich auf die Datacenter-Gruppe beschränkt ist.

VMware Cloud Director unterstützt Datacenter-Gruppennetzwerke für Organisations-VDCs, die von NSX Data Center for vSphere gestützt werden, sowohl mit einem aktiven und als auch mit einem Standby-Egress-Punkt für eine einzelne Netzwerk-Fehlerdomäne.

Eine von NSX Data Center for vSphere gestützte Datacenter-Gruppe kann entweder eine gemeinsame Egress-Punktkonfiguration, eine Egress-Punktkonfiguration für jede Netzwerk-Fehlerdomäne oder eine Konfiguration der lokalen Gruppe aufweisen.

Datacenter-Gruppe

Eine Datacenter-Gruppe fungiert als ein VDC-Gruppen-Router, der zentralisierte Netzwerkverwaltung, Konfiguration für mehrere Egress-Punkte in mehreren virtuellen Datacentern und Ost-West-Datenverkehr zwischen allen Netzwerken innerhalb der Gruppe bereitstellt. Eine Datacenter-Gruppe kann zwischen einem und 16 virtuellen Datacentern enthalten, die zur gemeinsamen Nutzung mehrerer Egress-Punkte konfiguriert sind. Eine Datacenter-Gruppe kann eine der folgenden Egress-Punktekfigurationen aufweisen:

Tabelle 5-3. Arten der Egress-Punktekfiguration für Datencenter, die von NSX Data Center for vSphere gestützt werden

Egress-Punkte-Konfigurationstyp	Beschreibung
Konfiguration gemeinsamer Egress-Punkte	<p>Sie können die Datencenter-Gruppe mit einem aktiven und einem Standby-Egress-Punkt konfigurieren. Die beiden Egress-Punkte werden von allen beteiligten virtuellen Datencentern in allen Netzwerk-Fehlerdomänen in der Datencenter-Gruppe gemeinsam verwendet.</p> <p>Eine Datencenter-Gruppe mit dieser Konfiguration kann Datencenter mit bis zu vier Netzwerk-Fehlerdomänen enthalten.</p>
Egress-Punktekfiguration pro Fehlerdomäne	<p>Sie können die Datencenter-Gruppe mit einem aktiven und einem Standby-Egress-Punkt für jede Netzwerk-Fehlerdomäne in der Datencenter-Gruppe konfigurieren.</p> <p>Eine Datencenter-Gruppe mit dieser Konfiguration kann Datencenter mit bis zu vier Netzwerk-Fehlerdomänen enthalten.</p>
Konfiguration der lokalen Gruppe	<p>Die Organisations-VDCs in einer lokalen Datencenter-Gruppe werden von einer einzelnen vCenter Server-Instanz gestützt. Sie können die lokale Datencenter-Gruppe mit einem aktiven und einem Standby-Egress-Punkt für eine einzelne Netzwerk-Fehlerdomäne konfigurieren.</p>

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

Die teilnehmenden virtuellen Organisations-Datencenter können zu unterschiedlichen VMware Cloud 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.

Verwalten von Datacenter-Gruppen mit NSX Data Center for vSphere als Typ des Netzanbieters

Nachdem Sie eine von NSX Data Center for vSphere gestützte Datacenter-Gruppe erstellt haben, können Sie die Netzwerktopologie einer Datacenter-Gruppe bearbeiten. Sie können virtuelle Datacenter 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 von NSX Data Center for vSphere gestützten Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration

Sie können eine von NSX Data Center for vSphere gestützte virtuelle Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration erstellen, bei der Sie ein Edge-Gateway-Paar aus aktivem und Standby-Egress-Punkt für alle beteiligten virtuellen Datacenter 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.
- Ihr **Systemadministrator** muss die gewünschten virtuellen Datacenter für VDC-übergreifende Netzwerke aktivieren.

Verfahren

1 Erstellen einer von NSX Data Center for vSphere gestützten Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration

Sie können 1 bis 16 virtuelle Datacenter in einer Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration zusammenfassen.

2 Hinzufügen eines aktiven Egress-Punkts zu einer Datacenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzanbieters

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

3 Hinzufügen eines Standby-Egress-Punkts zu einer Datacenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzanbieters

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

Erstellen einer von NSX Data Center for vSphere gestützten Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration

Sie können 1 bis 16 virtuelle Datacenter in einer Datacenter-Gruppe mit einer gemeinsamen Egress-Konfiguration zusammenfassen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf **Neu**.
- 3 Wählen Sie auf der Seite **Erstes VDC** ein VDC als das erste für die neue VDC-Gruppe aus.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die neue Datencenter-Gruppe ein.
- 5 Wählen Sie **Gemeinsame Egress-Punkte** aus und klicken Sie auf **Weiter**.
- 6 Wählen Sie auf der Seite **Teilnehmende VDCs** weitere Datencenter für die neue Datencenter-Gruppe aus und klicken Sie auf **Weiter**.

Die Seite **Datencenter** enthält eine Liste mit VDCs, die der **Systemadministrator** für die virtuelle Vernetzung von Datencentern aktiviert hat.

- 7 Überprüfen Sie die Details der Datencenter-Gruppe und klicken Sie auf **Fertigstellen**.

Ergebnisse

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

Hinzufügen eines aktiven Egress-Punkts zu einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzwerkanbieters

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 Datacentern gehören.

4 Wählen Sie das Edge-Gateway aus, das als aktiver Egress-Punkt für diese Datacenter-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 Datacenter-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 Datacentern zum Internet ist durch eine durchgezogene blaue Linie dargestellt.

Hinzufügen eines Standby-Egress-Punkts zu einer Datacenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzanbieters

In virtuellen Datacenter-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 Datacenter vorhanden sein, die Teil der Gruppe sind.

Verfahren

1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datacenter-Gruppen**.

Die Liste der Datacenter-Gruppen wird angezeigt.

2 Klicken Sie auf die Ziel-Datacenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datacenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 Datacentern gehören. Das Edge-Gateway, das vom aktiven Egress-Punkt in dieser virtuellen Datacenter-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 Netzwerk-Fehlerdomäne konfiguriert. Die Konfiguration wirkt sich nicht auf die vorhandenen Routen auf dem Edge Gateway aus.

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 von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration

Sie können eine von NSX Data Center for vSphere gestützte 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 von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration](#)

Sie können 1 bis 16 virtuelle Datencenter in einer von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit einer Egress-Konfiguration für Fehlerdomänen zusammenfassen.

- 2 [Hinzufügen eines Egress-Punkts für eine Fehlerdomäne](#)

Wenn Sie die virtuellen Datencenter aus einer Netzwerk-Fehlerdomäne in einer von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit dem Internet verbinden möchten, müssen Sie dieser Netzwerk-Fehlerdomäne einen Egress-Punkt hinzufügen. Sie können jeder Netzwerk-Fehlerdomäne in der Datencenter-Gruppe einen Egress-Punkt hinzufügen. Standby-Egress-Punkte werden in einer Datencenter-Gruppe mit einer Egress-Konfiguration für Fehlerdomänen nicht unterstützt.

Erstellen einer von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit einer Fehlerdomänen-Egress-Konfiguration

Sie können 1 bis 16 virtuelle Datencenter in einer von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit einer Egress-Konfiguration für Fehlerdomänen zusammenfassen.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datacenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf **Neu**.

- 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 **Teilnehmende VDCs** weitere Datacenter für die neue Datacenter-Gruppe aus und klicken Sie auf **Weiter**.

Die Seite **Datencenter** enthält eine Liste mit VDCs, die der **Systemadministrator** für die virtuelle Vernetzung von Datacentern aktiviert hat.

- 6 Überprüfen Sie die Details der Datacenter-Gruppe und klicken Sie auf **Fertigstellen**.

Ergebnisse

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

Hinzufügen eines Egress-Punkts für eine Fehlerdomäne

Wenn Sie die virtuellen Datacenter aus einer Netzwerk-Fehlerdomäne in einer von NSX Data Center for vSphere gestützten 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 Datacenter-Gruppe als Egress-Punkte verwendet werden, muss mindestens ein nicht verwendetes Edge-Gateway in einem der teilnehmenden virtuellen Datacenter vorhanden sein.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datacenter-Gruppen wird angezeigt.

2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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.

Erstellen und Konfigurieren einer lokalen virtuellen Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzanbieters

Ab Version 10.1 unterstützt VMware Cloud Director von NSX Data Center for vSphere gestützte Datencenter-Gruppen mit einem aktiven und einem Standby-Egress-Punkt für eine einzelne Netzwerk-Fehlerdomäne.

Die Organisations-VDCs in einer lokalen Gruppe werden von einer einzelnen vCenter Server-Instanz gestützt.

In einer lokalen Datencenter-Gruppe können Sie zwei Edge-Gateways festlegen – einen aktiven Egress-Punkt und einen Standby-Egress-Punkt zur Unterstützung von Hochverfügbarkeits- und Notfallwiederherstellungsszenarien innerhalb derselben Netzwerk-Fehlerdomäne.

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 lokalen Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzwerkanbieters

Sie können 1 bis 16 virtuelle Datencenter (VDCs) in einer von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit einer Egress-Konfiguration für Fehlerdomänen zusammenfassen.

2 Hinzufügen eines aktiven Egress-Punkts für eine lokale Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzwerkanbieters

Zum Verbinden der Datencenter aus der von NSX Data Center for vSphere gestützten lokalen Datencenter-Gruppe mit dem Internet müssen Sie der Netzwerk-Fehlerdomäne einen aktiven Egress-Punkt hinzufügen.

3 Hinzufügen eines Standby-Egress-Punkts für eine lokale Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzwerkanbieters

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

Erstellen einer lokalen Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzwerkanbieters

Sie können 1 bis 16 virtuelle Datencenter (VDCs) in einer von NSX Data Center for vSphere gestützten Datencenter-Gruppe mit einer Egress-Konfiguration für Fehlerdomänen zusammenfassen.

Voraussetzungen

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

Verfahren

1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

2 Klicken Sie auf **Neu**.

3 Wählen Sie auf der Seite **Erstes VDC** ein VDC als das erste für die neue VDC-Gruppe aus.

4 Geben Sie einen Namen und optional eine Beschreibung für die neue Datencenter-Gruppe ein.

5 Zum Erstellen einer Gruppe, die nur virtuelle Datencenter aus einer einzelnen Netzwerk-Fehlerdomäne enthält, aktivieren Sie die Option **Lokale Gruppe erstellen**.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite **Teilnehmende VDCs** weitere Datacenter für die neue Datacenter-Gruppe aus und klicken Sie auf **Weiter**.

Die Seite **Datacenter** enthält eine Liste mit VDCs, die der **Systemadministrator** für die virtuelle Vernetzung von Datacentern aktiviert hat.

8 Überprüfen Sie die Details der Datacenter-Gruppe und klicken Sie auf **Fertigstellen**.

Ergebnisse

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

Hinzufügen eines aktiven Egress-Punkts für eine lokale Datacenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzwerkanbieters

Zum Verbinden der Datacenter aus der von NSX Data Center for vSphere gestützten lokalen Datacenter-Gruppe mit dem Internet müssen Sie der Netzwerk-Fehlerdomäne einen aktiven Egress-Punkt hinzufügen.

Verfahren

1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datacenter-Gruppen**.

Die Liste der Datacenter-Gruppen wird angezeigt.

2 Klicken Sie auf die Ziel-Datacenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datacenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.

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

4 Wählen Sie in der Liste der Edge-Gateways, die zu den teilnehmenden virtuellen Datacentern gehören, ein Edge-Gateway aus, das als aktiver Egress-Punkt für die Datacenter-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 Netzwerk-Fehlerdomäne konfiguriert. Die Konfiguration wirkt sich nicht auf die vorhandenen Routen auf dem Edge Gateway aus.

Der neu hinzugefügte aktive Egress-Punkt wird im Diagramm der Netzwerktopologie angezeigt. Eine kontinuierliche blaue Linie stellt den Datenverkehr von den virtuellen Datacentern in der Netzwerk-Fehlerdomäne zum Internet dar.

Nächste Schritte

Um Fault Tolerance für Egress-Punkte zuzulassen, fügen Sie einen Standby-Egress-Punkt für die lokale Datacenter-Gruppe hinzu.

Hinzufügen eines Standby-Egress-Punkts für eine lokale Datacenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzanbieters

In Konfigurationen für lokale Datacenter-Gruppen 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 Datacenter vorhanden sein, die Teil der lokalen Datacenter-Gruppe sind.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datacenter-Gruppen**.

Die Liste der Datacenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datacenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datacenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 Datacentern gehören. Das Edge-Gateway, das vom aktiven Egress-Punkt in dieser virtuellen Datacenter-Gruppe verwendet wird, ist abgeblendet.

- 4 Wählen Sie das Edge-Gateway aus, das als Standby-Egress-Punkt für diese Datacenter-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 Netzwerk-Fehlerdomäne konfiguriert. Die Konfiguration wirkt sich nicht auf die vorhandenen Routen auf dem Edge Gateway aus.

Der neu hinzugefügte Egress-Punkt wird im Netzwerktopologiediagramm angezeigt. Eine gestrichelte blaue Linie stellt den Datenverkehr von den teilnehmenden virtuellen Datacentern zum Internet in den Fault Tolerance-Szenarien dar.

Anzeigen einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzerkanbieters

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.

Hinzufügen eines virtuellen Datencenters zu einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzerkanbieters

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 Datencenters aus einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzwerkanbieters

Sie können ein virtuelles Datencenter aus einer Datencenter-Gruppe entfernen. Die vorhandenen Netzwerke aus diesem virtuellen Datencenter 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 Datencenter-Gruppe muss mindestens drei virtuelle Datencenter enthalten.
- Das virtuelle Datencenter, das Sie entfernen möchten, darf keinen Egress-Punkt für die Datencenter-Gruppe bereitstellen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 Datencenters auf die drei Punkte und anschließend auf **Entfernen**.
- 4 Klicken Sie zur Bestätigung auf **Entfernen**.

Ergebnisse

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

Synchronisieren einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzerkanbieters

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

Hinweis Während des Synchronisierungsvorgangs der Datencenter-Gruppe ist die Datencenter-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs mit ihren Netzwerk-Fehlerdomänen, den Egress-Punkten (sofern konfiguriert) und den Datenverkehrsrouten dargestellt.

- 3 Klicken Sie auf **Datencentergruppe synchronisieren**.

- 4 Klicken Sie zur Bestätigung auf **OK**.

Tauschen der Egress-Punkte in einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzerkanbieters und 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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-Gateways eines Egress-Punkts eines Datencenters mit NSX Data Center for vSphere als Typ des Netzanbieters

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 aktiven Egress-Punkts aus einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzanbieters

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 einer Datencenter-Gruppe mit NSX Data Center for vSphere als Typ des Netzerkanbieters

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Datencenter-Gruppen**.

Die Liste der Datencenter-Gruppen wird angezeigt.

- 2 Klicken Sie auf die Ziel-Datencenter-Gruppe.

Die Ansicht **Netzwerktopologie** für diese Datencenter-Gruppe wird geöffnet. Im Diagramm der aktuellen Netzwerktopologie werden die beteiligten VDCs 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 Datacenter-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 der von NSX Data Center for vSphere-gestützten Datacenter-Gruppennetzwerke

Nachdem Sie eine Datacenter-Gruppe erstellt und konfiguriert haben, können Sie VDC-Gruppen-Layer-2-Netzwerke erstellen und verwalten, die die beteiligten virtuellen Datacenter umfassen.

Hinzufügen eines von NSX Data Center for vSphere gestützten VDC-Gruppennetzwerks

Sie können ein VDC-Gruppennetzwerk für alle virtuellen Datacenter erstellen, die Teil einer Datacentergruppe sind.

Sie können nur ein von NSX Data Center for vSphere gestütztes IPv4-Datacentergruppen-Netzwerk hinzufügen.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Neu**.
- 3 Wählen Sie auf der Seite **Bereich** die Option **Datacentergruppe** und dann eine von NSX Data Center for vSphere gestützte Datacentergruppe aus, in der das Netzwerk erstellt werden soll, und klicken Sie auf **Weiter**.
- 4 Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- 5 Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
Verwenden Sie das Format *Netzwerk-Gateway-IP-Adresse/Subnetz-Präfixlänge*, z. B. **192.167.1.1/24**.
- 6 Geben Sie eine Beschreibung des VDC-Organisationsnetzwerks ein.
- 7 Klicken Sie auf **Weiter**.
- 8 Überprüfen Sie die Einstellungen und klicken Sie auf **Fertigstellen**.

Ergebnisse

Das neu erstellte Datacentergruppen-Netzwerk wird in der Liste der Netzwerke für die Organisation angezeigt.

Der Netzwerktyp wird als „VDC-übergreifend“ aufgelistet.

Für jedes teilnehmende virtuelle Datacenter wird ein VDC-Organisationsnetzwerk mit VDC-übergreifendem Routing erstellt. Sie können die VDC-Gruppennetzwerke der teilnehmenden virtuellen Datacenter anzeigen, indem Sie auf die Karte eines teilnehmenden virtuellen Datacenters und dann 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 VDC-Gruppennetzwerk 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 VDC-Gruppennetzwerk angehängt sind, können Sie VMware Cloud Director OpenAPI verwenden. Wenn Sie sich die Dokumentation zu VMware Cloud Director OpenAPI ansehen möchten, wechseln Sie zu https://Cloud_Director_IP_address_or_host_name/docs. Um sich Codebeispiele anzusehen und VMware Cloud Director OpenAPI-Aufrufe zu testen, wechseln Sie zu https://Cloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name.

Anzeigen oder Bearbeiten eines von NSX Data Center for vSphere gestützten Datacentergruppen-Netzwerks

Sie können den Namen, die Beschreibung und die CIDR-Einstellungen eines von NSX Data Center for vSphere gestützten Datacentergruppen-Netzwerks anzeigen. Sie können nur den Namen und die Beschreibung eines von NSX Data Center for vSphere gestützten Datacentergruppen-Netzwerks bearbeiten.

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

Voraussetzungen

Vergewissern Sie sich, dass Ihnen die vordefinierte Rolle **Organisationsadministrator** oder eine Rolle, die die Rechte **VDC-Organisationsnetzwerk: Eigenschaften anzeigen** und **VDC-Organisationsnetzwerk: Eigenschaften bearbeiten** umfasst, zugewiesen ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Klicken Sie auf das Zielnetzwerk, um die Details dafür anzuzeigen.
- 3 Um den Namen und die Beschreibung des Netzwerks zu bearbeiten, klicken Sie auf **Bearbeiten**.
- 4 Bearbeiten Sie die Netzwerkdetails und klicken Sie auf **Speichern**.

Synchronisieren eines von NSX Data Center for vSphere gestützten Datencenter-Gruppennetzwerks

Um sicherzustellen, dass alle teilnehmenden virtuellen Datencenter auf ihr von NSX Data Center for vSphere gestütztes Datencenter-Gruppennetzwerk zugreifen können, können Sie das Datencenter-Gruppennetzwerk synchronisieren.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk**.
- 2 Aktivieren Sie auf der Registerkarte „Netzwerke“ das Optionsfeld neben dem Namen des Zielnetzwerks und klicken Sie anschließend auf **Synchronisieren**.
- 3 Klicken Sie zur Bestätigung auf **OK**.

Verwalten von NSX Data Center for vSphere-Edge-Gateways-Diensten

VMware Cloud Director stellt die von der NSX Data Center for vSphere-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 Data Center for vSphere-Funktionen in Ihrer VMware Cloud 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 einer in der Cloud gehosteten Anwendungsbereitstellung Redundanz und Kontinuität bereitzustellen.
- **Differenzierte Netzwerksicherheit und Isolierung:** Die NSX Data Center for vSphere-Funktionen in der VMware Cloud 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 VMware Cloud Director-Umgebung befinden, und um das Zero-Trust-Sicherheitsmodell für portierbare Sicherheit unabhängig vom Bereitstellungsort einer Anwendung zu erweitern.

- Weitere Funktionen, die von NSX Data Center for vSphere 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 [Konfiguration der Mandanten-Firewall mit NSX Data Center for vSphere](#).

Sie können auf diese erweiterten Netzwerkfunktionen über das VMware Cloud Director-Mandantenportal oder das VMware Cloud Director Service Provider Admin Portal zugreifen. Das Edge-Gateway muss zuerst in ein erweitertes Edge-Gateway konvertiert werden. Weitere Informationen finden Sie im [Konvertieren eines NSX Data Center for vSphere-Edge-Gateways in ein erweitertes Edge-Gateway](#).

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

Erste Schritte mit erweiterten VMware Cloud Director-Netzwerken mit NSX Data Center for vSphere

Sie verwenden erweiterte VMware Cloud Director-Netzwerke, um Verwaltungsaufgaben für eine Organisation in einem VMware Cloud Director-System auszuführen. Sie können verteilte Firewalls und andere erweiterte Netzwerkfunktionen verwalten, die von NSX Data Center for vSphere bereitgestellt werden, die der Organisation von einem VMware Cloud Director-Systemadministrator zur Verfügung gestellt werden.

Die typischen Benutzer des von NSX Data Center for vSphere bereitgestellten erweiterten Netzwerks sind:

- VMware Cloud Director **-Systemadministratoren**, die das Mandantenportal verwenden, um die verteilte Firewall und andere erweiterte Netzwerkfunktionen für eine Organisation zu konfigurieren.
- **Organisationsadministratoren**, die das Mandantenportal zum Verwalten der verteilten Firewall und anderer erweiterter Netzwerkfunktionen nutzen, die der **Systemadministrator** dieser Organisation zur Verfügung gestellt hat.

Konfiguration der Mandanten-Firewall mit NSX Data Center for vSphere

Im Mandantenportal können Sie die Firewallfunktionen konfigurieren, die von NSX Data Center for vSphere in Ihrem VMware Cloud Director-Organisations-VDC zur Verfügung gestellt werden. Sie können Firewallregeln für verteilte 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 verteilte Firewalls konfiguriert werden.

Die NSX Data Center for vSphere-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 verteilte Firewall auf die horizontale Zugriffssteuerung konzentriert.

Wichtige Unterschiede zwischen Edge-Gateway-Firewalls und verteilten 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 verteilte Firewall bietet die Möglichkeit, jede virtuelle Maschine und jede Anwendung bis zur Ebene 2 (L2) zu isolieren und zu sichern. Durch die Konfiguration von verteilten 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 Datencentern verschoben werden.

Firewallregeln

Wie in der NSX Data Center for vSphere-Produktdokumentation beschrieben, werden die auf zentraler Ebene definierten Firewallregeln 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 Regel für die verteilte Firewall

Weitere Informationen dazu, wie die NSX Data Center for vSphere-Software Firewallregeln erzwingt, finden Sie unter *Ändern der Reihenfolge einer Firewallregel* in der NSX Data Center for vSphere-Dokumentation.

Edge-Gateway-Firewall von NSX Data Center for vSphere

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 VMware Cloud Director-Umgebung wird von NSX Data Center for vSphere zur Verfügung gestellt. In NSX Data Center for vSphere 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 Funktionen, die von der Edge-Gateway-Firewall von NSX Data Center for vSphere zur Verfügung gestellt werden, finden Sie in der NSX Data Center for vSphere-Dokumentation.

Verwalten einer NSX Data Center for vSphere-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 NSX Data Center for vSphere-Regeln für verteilte Firewalls mithilfe des Mandantenportals](#).

Auf dem Bildschirm „Verteilte 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 NSX Data Center for vSphere-Edge-Gateways in ein erweitertes Edge-Gateway

Um mit einem NSX Data Center for vSphere-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 NSX Data Center for vSphere für diese erweiterten Edge-Gateways bereitgestellt werden.

Voraussetzungen

Sie haben ein vorhandenes Edge-Gateway.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 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** klicken.

Hinzufügen einer Firewallregel für NSX Data Center for vSphere Edge-Gateways

Sie können die Registerkarte **Firewall** des Edge-Gateways verwenden, um Firewallregeln für das betreffende 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-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.

- 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:

- Wählen Sie das Dienstprotokoll aus.
- Geben Sie die Portnummern für die Quell- und Zielports oder **Beliebig** an.
- 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 NSX Data Center for vSphere-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 NSX Data Center for vSphere Edge-Gateways](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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**.

NSX Data Center for vSphere – Verteilte Firewall

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

VMware Cloud Director unterstützt Dienste für verteilte Firewalls in von NSX Data Center for vSphere gestützten Organisations-VDCs. Wie in der NSX Data Center for vSphere-Dokumentation erläutert, handelt es sich bei dieser verteilten Firewall um eine Kernel-Embedded-Hypervisor-Firewall, die Transparenz und Kontrolle für virtualisierte Arbeitslasten und Netzwerke zur Verfügung stellt. 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 verteilte Firewall unterstützt ein Sicherheitsmodell mit Mikrosegmentierung, bei dem der Ost-West-Datenverkehr bei fast maximal möglicher Verarbeitungsrate untersucht werden kann.

Wie in der NSX Data Center for vSphere-Dokumentation erläutert, erstellt die verteilte 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 verteilte 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 verteilten Firewall zur Verfügung gestellt werden, finden Sie in der NSX Data Center for vSphere-Dokumentation.

Aktivieren der verteilten Firewall eines von NSX Data Center for vSphere gestützten Organisations-VDC

Bevor Sie das Mandantenportal verwenden, um mit den von NSX Data Center for vSphere bereitgestellten Funktionen für verteilte Firewalls in einem Organisations-VDC zu arbeiten, muss die verteilte Firewall für dieses Organisations-VDC aktiviert werden. Ein VMware Cloud Director-Systemadministrator oder ein Benutzer, dem die Berechtigung **org_vdc_distributed_firewall_enable** zugewiesen wurde, kann die verteilte Firewall für das Organisations-VDC aktivieren.

Sie verwenden den Bildschirm „Verteilte Firewall“ im Mandantenportal, um die verteilte Firewall für ein Organisations-VDC zu aktivieren.

Voraussetzungen

Stellen Sie sicher, dass der Organisation, zu der das Organisations-VDC gehört, die folgenden Rechte zugewiesen wurden:

- Verteilte Firewall für Organisations-VDC: Aktivieren/Deaktivieren
- Verteilte Firewall für Organisations-VDC: Regeln konfigurieren
- Verteilte Firewall für Organisations-VDC: Regeln anzeigen

Der VMware Cloud Director-**Systemadministrator** weist einer Organisation Rechte zu. Das Recht „Verteilte Firewall für Organisations-VDC: Aktivieren/Deaktivieren“ ist erforderlich, um die verteilte Firewall über die Benutzeroberfläche des Mandantenportals zu aktivieren. Das Recht „Verteilte Firewall für Organisations-VDC: Regeln anzeigen“ ist für die Anzeige von Firewallregeln im Mandantenportal erforderlich, und das Recht „Verteilte 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 „Verteilte Firewall für Organisations-VDC: Aktivieren/Deaktivieren“ gewährt. Unter den vordefinierten Rollen in einem VMware Cloud Director-System hat nur die Rolle „Systemadministrator“ dieses Recht standardmäßig.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles 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 Regeln für verteilte Firewalls konfigurieren möchten.
- 3 Klicken Sie auf **Dienste konfigurieren**.
- 4 Aktivieren Sie die verteilte Firewall auf der Registerkarte **Verteilte Firewall**.

Nächste Schritte

Eine Beschreibung der Standardregel für die verteilte Firewall finden Sie unter [Verwalten der NSX Data Center for vSphere-Regeln für verteilte Firewalls mithilfe des Mandantenportals](#).

Verwalten der NSX Data Center for vSphere-Regeln für verteilte Firewalls mithilfe des Mandantenportals

Wie in der Dokumentation für NSX Data Center for vSphere erläutert, werden die standardmäßigen Firewallereinstellungen auf Datenverkehr angewendet, der keiner der benutzerdefinierten Firewallregeln entspricht. Im VMware Cloud Director Tenant Portal hat die Standardregel für die verteilte Firewall die Bezeichnung „Zulässige Standardregel“.

Die Funktion „Verteilte Firewall“ muss in einem Organisations-VDC aktiviert werden, bevor Sie die Einstellungen für die verteilte Firewall im VMware Cloud Director Tenant Portal verwalten können.

Die Standardregel für die verteilte Firewall 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 verteilte Firewalls weder löschen noch ändern.

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 verteilten Firewall eines von NSX Data Center for vSphere gestützten Organisations-VDC](#)
- 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 **Virtuelles 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 Regel für verteilte Firewalls

Verwenden Sie in einer VMware Cloud Director-Umgebung zum Ändern einer vorhandenen Regel für verteilte Firewalls eines virtuellen Organisations-Datencenters den Bildschirm **Verteilte 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 **Virtuelles 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 Regeln für verteilte Firewalls 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 auf die Schaltfläche **Löschen** oberhalb der Regeltabelle 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 von DHCP für NSX Data Center for vSphere-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 aktivierten 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 NSX Data Center for vSphere-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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

VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.

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 Domänennamen 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 NSX Data Center for vSphere-Edge-Gateways

Die DHCP-Relay-Funktion, die von NSX in Ihrer VMware Cloud Director-Umgebung bereitgestellt wird, ermöglicht Ihnen die Nutzung Ihrer vorhandenen DHCP-Infrastruktur von Ihrer VMware

Cloud 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 werden.

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 NSX Data Center for vSphere-Edge-Gateway

Die NSX-Software in Ihrer VMware Cloud Director-Umgebung stellt dem Edge-Gateway die Funktionalität zur Relay-gestützten Weiterleitung von DHCP-Meldungen an DHCP-Server bereit, die sich außerhalb Ihres VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.

- 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 auf einem NSX Data Center for vSphere-Edge-Gateway

Mithilfe der NSX Data Center for vSphere-Software in der VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 NSX Data Center for vSphere-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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	<p>Geben Sie die erforderliche IP-Adresse ein oder wählen Sie die zugeteilte IP-Adresse aus der Liste aus.</p> <p>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.</p>
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	<p>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.</p> <p>ICMP-Meldungen werden anhand des Feldtyps identifiziert. Der ICMP-Typ ist standardmäßig auf „Alle“ festgelegt.</p>
Übersetzte(r) IP/Bereich	<p>Geben Sie die IP-Adresse oder einen Bereich von IP-Adressen ein, in die Zieladressen in eingehenden Paketen übersetzt werden.</p> <p>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.</p>
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.
Quell-IP-Adresse	Wenn Sie möchten, dass die Regel nur für den Datenverkehr zu einer bestimmten Domäne angewendet wird, geben Sie eine IP-Adresse für diese Domäne oder einen IP-Adressbereich im CIDR-Format ein. Wenn Sie dieses Textfeld leer lassen, gilt die DNAT-Regel für alle IP-Adressen innerhalb des lokalen Subnetzes.
Quellport	(Optional) Geben Sie eine Portnummer für die Quelle ein.
Beschreibung	(Optional) Geben Sie eine aussagekräftige Beschreibung für die DNAT-Regel ein.
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 den Bereich von IP-Adressen ein, der auf diese Regel angewendet werden soll, oder wählen Sie die zugewiesene IP-Adresse aus der Liste aus. 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.
Ziel-IP-Adresse	(Optional) Wenn Sie möchten, dass die Regel nur für den Datenverkehr zu einer bestimmten Domäne angewendet wird, geben Sie eine IP-Adresse für diese Domäne oder einen IP-Adressbereich im CIDR-Format ein. Wenn Sie dieses Textfeld leer lassen, gilt die SNAT-Regel für alle Ziele außerhalb des lokalen Subnetzes.
Zielport	(Optional) Geben Sie eine Portnummer für das Ziel ein.
Beschreibung	(Optional) Geben Sie eine aussagekräftige Beschreibung für die SNAT-Regel ein.
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 NSX Data Center for vSphere Edge-Gateways](#).

Erweiterte Routing-Konfiguration für NSX Data Center for vSphere-Edge-Gateways

Sie können das statische und dynamische Routing auf Ihren NSX Data Center for vSphere-Edge-Gateways konfigurieren.

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 Data Center for vSphere bereitgestellten Routing-Funktionen finden Sie in der NSX Data Center for vSphere-Dokumentation.

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 Data Center for vSphere 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 NSX Data Center for vSphere-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Gateway-Schnittstellen zugeordnet ist. Andernfalls schlägt die Konfiguration dieser statischen Route fehl.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 NSX Data Center for vSphere Edge-Gateways](#).

Konfigurieren des OSPF-Protokolls

Sie können das OSPF-Routing-Protokoll (Open Shortest Path First) für die dynamischen Routing-Funktionen eines NSX Data Center for vSphere-Edge-Gateways konfigurieren. Eine häufige Anwendung von OSPF auf einem Edge-Gateway in einer VMware Cloud Director-Umgebung besteht im Austausch von Routing-Informationen zwischen Edge-Gateways in VMware Cloud Director.

Das NSX-Edge-Gateway unterstützt OSPF, ein internes Gateway-Protokoll, das IP-Pakete nur innerhalb einer einzelnen Routing-Domäne weiterleitet. Wie in der *Administratorokumentation 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 NSX Data Center for vSphere-Edge-Gateway](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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.
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>

Option	Beschreibung
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> <hr/> <p>Vorsicht Eine Regel des Typs <code>Alle blockieren</code> wird am Ende der Filter erzwungen.</p> <hr/> <p>Fügen Sie einen Filter zur Tabelle hinzu, indem Sie auf das Plusymbol (+) 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere-Edge-Gateway konfigurieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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**.

Lastenausgleich mit NSX Data Center for vSphere

Der Lastausgleichsdienst verteilt eingehende Dienstanforderungen an mehrere Server und sorgt dabei dafür, dass die Lastverteilung für den Benutzer erkennbar ist. Der Lastausgleich bietet hohe Anwendungsverfügbarkeit und ermöglicht eine optimale Ressourcennutzung, maximalen Durchsatz, kurze Reaktionszeit und verhindert gleichzeitig eine Überlastung.

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.

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 NSX Data Center for vSphere-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.

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 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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>
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**.

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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	<p>(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.</p> <p>Hinweis Die Verwendung dieses Headers wird nicht unterstützt, wenn Sie SSL-Passthrough aktiviert haben.</p>
Pool-seitiges SSL aktivieren	<p>(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.</p>

- 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 zum Beibehalten Ihrer Änderungen auf **Behalten**.


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“.
 - Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- Navigieren Sie zu **Lastausgleichsdienst > Dienstüberwachung**.
- Klicken Sie auf die Schaltfläche **Erstellen** ()
- 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 zum Beibehalten Ihrer Änderungen auf **Behalten**.

Beispiel: Erweiterungen unterstützt für jedes Protokoll

Tabelle 5-4. 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 5-5. 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 5-6. 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 <i>#days</i> 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 zum Beibehalten Ihrer Änderungen auf **Behalten**.

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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.

- 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/2.2/configuration.html>.

- 6 Klicken Sie zum Beibehalten Ihrer Änderungen auf **Behalten**.

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 NSX Data Center for vSphere-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 zum Beibehalten Ihrer Änderungen auf **Behalten**.

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 NSX Data Center for vSphere Edge-Gateways](#)

Konfigurieren des sicheren Zugriffs mithilfe von VPN auf einem NSX Data Center for vSphere-Edge-Gateway

Sie können die VPN-Funktionen konfigurieren, die von der NSX Data Center for vSphere-Software auf Ihren NSX Data Center for vSphere-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 VMware Cloud 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 VMware Cloud 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 NSX Data Center for vSphere-Edge-Gateway in einer VMware Cloud Director-Umgebung ermöglichen Remotebenutzern die sichere Verbindung mit den privaten Netzwerken und Anwendungen in den Organisations-VDCs, die von diesem Edge-Gateway gestützt werden. Sie können verschiedene SSL VPN-Plus-Dienste auf dem Edge-Gateway konfigurieren.

In Ihrer VMware Cloud 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 auf einem NSX Data Center for vSphere-Edge-Gateway](#).

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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Gateway geben die Remotebenutzer dieselbe IP-Adresse und den Port an, die bzw. den Sie in diesen Servereinstellungen festlegen.

3 Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Gateway

Das System legt standardmäßig einige SSL VPN-Plus-Einstellungen für ein Edge-Gateway in Ihrer VMware Cloud Director-Umgebung fest. Auf dem Bildschirm **Allgemeine Einstellungen** auf der Registerkarte **SSL VPN-Plus** im VMware Cloud 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 NSX Data Center for vSphere-Edge-Gateway zu beginnen.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 2 Klicken Sie auf die Registerkarte **SSL VPN-Plus**.

Nächste Schritte

Konfigurieren Sie die SSL VPN-Plus-Standard Einstellungen im Bildschirm **Allgemein**. Weitere Informationen finden Sie unter [Anpassen der allgemeinen SSL VPN-Plus-Einstellungen für ein NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Gateway geben die Remotebenutzer dieselbe IP-Adresse und den Port an, die bzw. 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere-Edge-Gateway](#).

Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem NSX Data Center for vSphere-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.

Option	Aktion
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 NSX Data Center for vSphere-Edge-Gateway](#).

Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem NSX Data Center for vSphere-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 im aktiven Modus konfigurierten FTP-Servers müssen Sie ein weiteres privates Netzwerk für den FTP-Server hinzufügen und die 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 NSX Data Center for vSphere-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>

Option	Aktion
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> <hr/> <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. <hr/>
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 NSX Data Center for vSphere-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 NSX Data Center for vSphere Edge-Gateways](#).

Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 das Upgrade installieren.
- 6 Klicken Sie auf **Änderungen speichern**.

Anpassen der allgemeinen SSL VPN-Plus-Einstellungen für ein NSX Data Center for vSphere-Edge-Gateway

Das System legt standardmäßig einige SSL VPN-Plus-Einstellungen für ein Edge-Gateway in Ihrer VMware Cloud Director-Umgebung fest. Auf dem Bildschirm **Allgemeine Einstellungen** auf der Registerkarte **SSL VPN-Plus** im VMware Cloud 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.

Option	Beschreibung
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 NSX Data Center for vSphere-Edge-Gateways in einer VMware Cloud 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 (AES256-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“.

Um die Größe Ihrer Edge-Gateway-Konfiguration anzuzeigen, navigieren Sie zum Edge-Gateway und klicken Sie auf den Namen des Edge-Gateways.

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 NSX Data Center for vSphere-Edge-Gateway konfigurieren.

2 Konfigurieren von IPsec-VPN-Site-Verbindungen für das NSX Data Center for vSphere-Edge-Gateway

Verwenden Sie den Bildschirm **IPsec-VPN-Sites** im VMware Cloud 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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Gateway konfigurieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 NSX Data Center for vSphere-Edge-Gateway](#).

Konfigurieren von IPsec-VPN-Site-Verbindungen für das NSX Data Center for vSphere-Edge-Gateway

Verwenden Sie den Bildschirm **IPsec-VPN-Sites** im VMware Cloud 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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>
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>

Option	Aktion
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>
Authentifizierung	<p>Wählen Sie eine Authentifizierung aus. Zu den Optionen gehören:</p> <ul style="list-style-type: none"> ■ PSK <p>„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.</p> ■ Zertifikat <p>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.</p>
Gemeinsam verwendeten Schlüssel ändern	<p>(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.</p>

Option	Aktion
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. <p>Dies ist der Standardwert.</p> <ul style="list-style-type: none"> ■ <code>passthroughSubnets=PeerSubnet/IPAddress</code>, um überlappende Subnetze zu unterstützen.

5 Klicken Sie auf **Behalten**.

6 Klicken Sie auf **Änderungen speichern**.

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 NSX Data Center for vSphere-Edge-Gateway](#).

Aktivieren des IPsec-VPN-Diensts auf einem NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 NSX Data Center for vSphere-Edge-Gateway](#).

L2 VPN konfigurieren

Die NSX Data Center for vSphere-Edge-Gateways in einer VMware Cloud Director-Umgebung unterstützen L2 VPN. Mit L2 VPN können Sie Ihr Organisations-VDC erweitern, indem Sie ermöglichen, dass virtuelle Maschinen Netzwerkkonnektivität unter Verwendung derselben IP-Adresse über geografische Grenzen hinweg beibehalten. Sie können den L2 VPN-Dienst auf einem Edge-Gateway konfigurieren.

NSX Data Center for vSphere 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.

Navigieren zum Bildschirm „L2 VPN“

Zum Konfigurieren des L2 VPN-Diensts für ein NSX Data Center for vSphere-Edge-Gateway müssen Sie zum Bildschirm **L2 VPN** navigieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 2 Navigieren Sie zu **VPN > L2 VPN**.

Nächste Schritte

Konfigurieren Sie den L2 VPN-Server. Weitere Informationen finden Sie unter [Konfigurieren des NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Server](#).

Konfigurieren des NSX Data Center for vSphere-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.
- [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	
Kennwort bestätigen	Die Benutzeranmeldedaten auf der Peer-Site müssen mit den Anmeldedaten auf der Clientseite identisch sein.

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**.

Nächste Schritte

Aktivieren Sie den L2 VPN-Dienst auf diesem Edge-Gateway. Weitere Informationen finden Sie unter [Aktivieren des L2 VPN-Diensts auf einem NSX Data Center for vSphere-Edge-Gateway](#).

Konfigurieren des NSX Data Center for vSphere-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**.
- 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**.

Nächste Schritte

Aktivieren Sie den L2 VPN-Dienst auf diesem Edge-Gateway. Weitere Informationen finden Sie unter [Aktivieren des L2 VPN-Diensts auf einem NSX Data Center for vSphere-Edge-Gateway](#).

Aktivieren des L2 VPN-Diensts auf einem NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Gateway

Sie können die vorhandene L2 VPN-Dienstkonfiguration des Edge-Gateways entfernen. Mit dieser 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 ist deaktiviert und die Konfigurationsdetails werden aus dem Edge-Gateway entfernt.

SSL-Zertifikatsverwaltung auf einem NSX Data Center for vSphere-Edge-Gateway

Die NSX Data Center for vSphere-Software in der VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Data Center for vSphere-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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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.
Bei aktiviertem FIPS-Modus müssen RSA-Schlüsselgrößen größer oder gleich 2048 Bit sein.
 - 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.

Benutzerdefinierte Gruppierungsobjekte für NSX Data Center for vSphere-Edge-Gateways

Die NSX Data Center for vSphere-Software in der VMware Cloud 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 VMware Cloud 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 Edge-Gateway aus, das Sie bearbeiten möchten, 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 Sicherheitsdienst aus, den Sie bearbeiten möchten, 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 VMware Cloud 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	a Navigieren Sie zu Netzwerk > Edges . b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf Dienste konfigurieren . c Klicken Sie auf Gruppierungsobjekte .
Öffnen über Sicherheitsdienste	a Navigieren Sie zu Netzwerk > Sicherheit . b Wählen Sie den Sicherheitsdienst aus, den Sie bearbeiten möchten, 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 VMware Cloud 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 VMware Cloud 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 Edge-Gateway aus, das Sie bearbeiten möchten, 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 Sicherheitsdienst aus, den Sie bearbeiten möchten, 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 VMware Cloud 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 VMware Cloud 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 Edge-Gateway aus, das Sie bearbeiten möchten, 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 Sicherheitsdienst aus, den Sie bearbeiten möchten, 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 NSX Data Center for vSphere-Edge-Gateway

Sie können Statistiken und Protokolle für ein NSX Data Center for vSphere-Edge-Gateway anzeigen.

Anzeigen von Statistiken

Sie können Statistiken auf dem Bildschirm **Edge-Gateway-Dienste** anzeigen.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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. Auf dem Bildschirm werden Diagramme für den Datenverkehr angezeigt, der über die Schnittstellen des ausgewählten Edge-Gateways und für die Firewall fließt. 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

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass Ihre Rolle das Recht **Systemprotokollierung konfigurieren** umfasst.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 2 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 VMware Cloud Director-Systemadministrator bereits einen Syslog-Server für die VMware Cloud Director-Umgebung konfiguriert hat, verwendet das System standardmäßig diesen Syslog-Server. Die zugehörige IP-Adresse wird im Bildschirm **Edge-Einstellungen** angezeigt.

3 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 über ein NSX Data Center for vSphere-Edge-Gateway

Sie können den SSH-Befehlszeilenzugriff über ein Edge-Gateway aktivieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf **Edge-Gateways**.
 - b Wählen Sie das Edge-Gateway aus, das Sie bearbeiten möchten, und klicken Sie auf **Dienste**.
- 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	Standardmäßig lautet der SSH-Benutzername admin .
Kennwort erneut eingeben	
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 Sicherheits-Tags für NSX Data Center for vSphere-Edge-Gateways

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 virtuelle 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 **Virtuelles 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 **Virtuelles 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 **Virtuelles 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 **Virtuelles 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 für NSX Data Center for vSphere-Edge-Gateways](#).

.

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 **Virtuelles 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 für NSX Data Center for vSphere-Edge-Gateways](#).

Arbeiten mit Sicherheitsgruppen für NSX Data Center for vSphere-Edge-Gateways

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 zum Beibehalten Ihrer Änderungen auf **Behalten**.

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.

Verwalten von NSX-T Data Center-Edge-Gateways

Ein NSX-T Data Center-Edge-Gateway stellt ein geroutetes VDC-Organisationsnetzwerk oder ein Datacenter-Gruppennetzwerk mit Konnektivität zu externen Netzwerken und IP-Verwaltungseigenschaften bereit. Es kann auch Dienste bereitstellen, wie z. B. Firewall, Netzwerkadressübersetzung (NAT), IPSec-VPN, DNS-Weiterleitung und DHCP, die standardmäßig aktiviert sind.

Dedizierte externe Netzwerke

Um eine vollständig geroutete Netzwerktopologie in einem virtuellen Datacenter bereitzustellen, kann Ihr **Systemadministrator** ein externes Netzwerk für ein bestimmtes NSX-T Data Center-Edge-Gateway reservieren.

In dieser Konfiguration besteht eine 1:1-Beziehung zwischen dem externen Netzwerk und dem NSX-T Data Center-Edge-Gateway, und andere Edge-Gateways können keine Verbindung mit dem externen Netzwerk herstellen.

Ein logischer NSX-T Data Center-Tier-0-Router oder ein VRF-Gateway, das mit einem dedizierten externen Netzwerk verknüpft ist, ist Teil des Mandantennetzwerk-Stacks. Das externe Netzwerk wird als Teil der Routing-Domäne des VMware Cloud Director-Netzwerks betrachtet.

Ein dediziertes externes Netzwerk bietet zusätzliche Edge-Gateway-Routing-Dienste, wie z. B. die Routenankündigungsverwaltung und die BGP-Konfiguration (Border Gateway Protocol).

Sie können entscheiden, welches der an das Edge-Gateway angehängten Netzwerke für das externe Netzwerk angekündigt werden soll. Dies ermöglicht eine Mischung aus NAT-gerouteten und vollständig gerouteten VDC-Organisationsnetzwerken.

Hinzufügen eines IP Set zu einem NSX-T Data Center-Edge-Gateway

Um Firewallregeln zu erstellen und einem NSX-T Data Center-Edge-Gateway hinzuzufügen, müssen Sie zuerst IP Sets erstellen. IP Sets sind Gruppen von Objekten, auf die die Firewallregeln angewendet werden. Durch die Kombination mehrerer Objekte in IP Sets kann die Gesamtzahl der zu erstellenden Firewallregeln reduziert werden.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das NSX-T Edge-Gateway.

- 3 Klicken Sie unter **Sicherheit** auf die Registerkarte **IP Sets** und dann auf **Neu**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für das IP Set ein.
- 5 Geben Sie eine IP-Adresse oder einen IP-Adressbereich für die virtuellen Maschinen ein, die im IP Set enthalten sind, und klicken Sie auf **Hinzufügen**.
- 6 Um die Firewallgruppe zu speichern, klicken Sie auf **Speichern**.

Ergebnisse

Sie haben ein IP Set erstellt und dem NSX-T Edge-Gateway hinzugefügt.

Nächste Schritte

[Hinzufügen einer Firewallregel für NSX-T Data Center Edge-Gateways](#)

Hinzufügen einer Firewallregel für NSX-T Data Center Edge-Gateways

Um den eingehenden und ausgehenden Netzwerkdatenverkehr zu und von einem NSX-T Data Center-Edge-Gateway zu steuern, erstellen Sie Firewallregeln.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Falls der Bildschirm **Firewall** unter dem Abschnitt „Dienste“ noch nicht angezeigt wird, klicken Sie auf die Registerkarte **Firewall**.
- 4 Klicken Sie auf **Regeln bearbeiten**.
- 5 Klicken Sie auf die Schaltfläche **Neue oben**.
Über der ausgewählten Regel wird eine Zeile für die neue Regel hinzugefügt.
- 6 Konfigurieren Sie die Firewallregel.

Option	Beschreibung
Name	Geben Sie einen Namen für die Regel ein.
Zustand	Um die Regel bei der Erstellung zu aktivieren, verwenden Sie die Umschaltoption Zustand .
Anwendungen	(Optional) Zur Auswahl eines bestimmten Portprofils, für das die Regel gilt, aktivieren Sie die Umschaltoption Anwendungen und klicken auf Speichern .
Quelle	<p>Wählen Sie eine Option aus und klicken Sie auf Beibehalten.</p> <ul style="list-style-type: none"> ■ Um Datenverkehr von einer beliebigen Quelladresse zuzulassen oder zu verweigern, aktivieren Sie die Umschaltoption Beliebige Quelle. ■ Um Datenverkehr von bestimmten Firewallgruppen zuzulassen oder zu verweigern, wählen Sie die Firewallgruppen aus der Liste aus.

Option	Beschreibung
Ziel	<p>Wählen Sie eine Option aus und klicken Sie auf Beibehalten.</p> <ul style="list-style-type: none"> ■ Um Datenverkehr zu einer beliebigen Zieladresse zuzulassen oder zu verweigern, aktivieren Sie die Umschaltoption Beliebiges Ziel. ■ Um Datenverkehr zu bestimmten Firewallgruppen zuzulassen oder zu verweigern, wählen Sie die Firewallgruppen aus der Liste aus.
Aktion	<p>Wählen Sie im Dropdown-Menü Aktion eine Option aus.</p> <ul style="list-style-type: none"> ■ Wählen Sie Annehmen aus, um Datenverkehr von oder zu den angegebenen Quellen, Zielen und Diensten zuzulassen. ■ Wählen Sie Verwerfen aus, um Datenverkehr von oder zu den angegebenen Quellen, Zielen und Diensten ohne Benachrichtigung des blockierten Clients zu blockieren. ■ Zum Blockieren des Datenverkehrs von oder zu den angegebenen Quellen, Zielen und Diensten und Informieren des blockierten Clients über abgelehnten Datenverkehr wählen Sie Ablehnen aus.
IP-Protokoll	Wählen Sie aus, ob die Regel auf IPv4- oder IPv6-Datenverkehr angewendet werden soll.
Richtung	<p>Wählen Sie die Datenverkehrsrichtung aus, auf die die Regel angewendet werden soll.</p> <p>Hinweis In VMware Cloud Director 10.2.1 und höheren Versionen ist diese Option nicht mehr verfügbar.</p>
Protokollierung aktivieren	Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung aktivieren .

7 Klicken Sie auf **Speichern**.

8 Wiederholen Sie diese Schritte, um zusätzliche Regeln zu konfigurieren.

Ergebnisse

Nachdem die Firewallregeln erstellt wurden, werden sie in der Liste der Firewallregeln des Edge-Gateways angezeigt. Sie können die Regeln nach Bedarf nach oben oder unten verschieben, bearbeiten oder löschen.

Hinzufügen einer SNAT- oder DNAT-Regel zu einem NSX-T-Edge-Gateway

Um die IP-Quelladresse von einer privaten in eine öffentliche IP-Adresse zu ändern, erstellen Sie eine Quell-NAT-Regel (SNAT). Um die IP-Zieladresse von einer öffentlichen in eine private IP-Adresse zu ändern, erstellen Sie eine NAT-Zielregel (DNAT).

Bei der Konfiguration einer SNAT- oder DNAT-Regel auf einem Edge-Gateway in der VMware Cloud Director-Umgebung konfigurieren Sie die Regel immer aus der Perspektive des Organisations-VDC.

Eine SNAT-Regel übersetzt die IP-Quelladresse von Paketen, die aus einem VDC-Organisationsnetzwerk an ein externes Netzwerk oder an ein anderes VDC-Organisationsnetzwerk gesendet werden.

Eine Regel des Typs KEINE SNAT verhindert die Übersetzung der internen IP-Adresse von Paketen, die aus 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.

Eine Regel des Typs KEINE DNAT verhindert die Übersetzung der externen IP-Adresse von Paketen, die ein VDC-Organisationsnetzwerk von einem externen Netzwerk oder einem anderen VDC-Organisationsnetzwerk empfängt.

VMware Cloud Director unterstützt die automatische Routenneuverteilung, wenn Sie NAT-Dienste auf einem NSX-T Data Center-Edge-Gateway verwenden.

Wichtig Wenn Sie Tanzu Kubernetes-Cluster verwenden, notieren Sie sich die auf dem Edge-Gateway erstellte SNAT-Systemregel, um das Erstellen einer widersprüchlichen Regel zu vermeiden.

Voraussetzungen

Die öffentliche IP-Adresse muss bereits der Edge-Gateway-Schnittstelle, für die Sie die Regel hinzufügen möchten, hinzugefügt worden sein.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway und dann unter **Dienste** auf **NAT**.
- 3 Klicken Sie auf **Neu**, um eine Regel hinzuzufügen.
- 4 Konfigurieren Sie eine SNAT- oder KEINE SNAT-Regel (von innen nach außen).

Option	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Regel ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.
Schnittstellentyp	Wählen Sie im Dropdown-Menü SNAT oder KEINE SNAT aus.
Externe IP	<p>Abhängig vom Typ der von Ihnen erstellten Regel wählen Sie eine der Optionen aus.</p> <ul style="list-style-type: none"> ■ Wenn Sie eine SNAT-Regel erstellen, geben Sie die öffentliche IP-Adresse des Edge-Gateways ein, für das Sie die SNAT-Regel konfigurieren. ■ Wenn Sie eine Regel des Typs KEINE SNAT erstellen, lassen Sie das Textfeld leer.
Interne IP	Geben Sie die IP-Adresse oder eine Liste der IP-Adressen der virtuellen Maschinen ein, für die Sie SNAT konfigurieren, damit sie Datenverkehr an das externe Netzwerk senden können.

Option	Beschreibung
Ziel-IP	(Optional) Wenn die Regel nur für den Datenverkehr zu einer bestimmten Domäne gelten soll, geben Sie eine IP-Adresse für diese Domäne oder eine IP-Adressliste ein. Wenn Sie dieses Textfeld leer lassen, gilt die SNAT-Regel für alle Ziele außerhalb des lokalen Subnetzes.
Erweiterte Einstellungen (optional)	<p>Klicken Sie auf die Registerkarte Erweiterte Einstellungen, um weitere Einstellungen anzuzeigen.</p> <p>Zustand</p> <p>Um die Regel bei der Erstellung zu aktivieren, aktivieren Sie die Umschaltoption Zustand.</p> <p>Protokollierung</p> <p>Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung.</p> <p>Priorität</p> <p>Wenn eine Adresse über mehrere NAT-Regeln verfügt, können Sie diesen Regeln verschiedene Prioritäten zuweisen und somit die Reihenfolge bestimmen, in der sie angewendet werden. Ein niedrigerer Wert bedeutet eine höhere Priorität für diese Regel.</p> <p>Firewall-Übereinstimmung</p> <p>Sie können eine Regel für die Firewall-Übereinstimmung festlegen, um die Anwendung der Firewall während NAT anzugeben. Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus.</p> <ul style="list-style-type: none"> ■ Zum Anwenden von Firewallregeln auf die interne Adresse einer NAT-Regel wählen Sie Interne Adresse abgleichen aus. ■ Zum Anwenden von Firewallregeln auf die externe Adresse einer NAT-Regel wählen Sie Externe Adresse abgleichen aus. ■ Zum Überspringen der Anwendung von Firewallregeln wählen Sie Bypass aus.

5 Konfigurieren Sie eine DNAT- oder KEINE DNAT-Regel (von außen nach innen).

Option	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Regel ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.
Schnittstellentyp	Wählen Sie im Dropdown-Menü DNAT oder KEINE DNAT aus.
Externe IP	<p>Geben Sie die öffentliche IP-Adresse des Edge-Gateways ein, für das Sie die DNAT-Regel konfigurieren.</p> <p>Die eingegebenen IP-Adressen müssen dem Edge-Gateway unterzugewiesen werden.</p>
Externer Port	(Optional) Geben Sie einen Port ein, in den die DNAT-Regel die Übersetzung für die auf den virtuellen Maschinen eingehenden Pakete vornimmt.

Option	Beschreibung
Interne IP	<p>Abhängig vom Typ der von Ihnen erstellten Regel wählen Sie eine der Optionen aus.</p> <ul style="list-style-type: none"> ■ Wenn Sie eine DNAT-Regel erstellen, geben Sie die IP-Adresse oder eine Liste der IP-Adressen der virtuellen Maschinen ein, für die Sie DNAT konfigurieren, damit diese Datenverkehr vom externen Netzwerk empfangen können. ■ Wenn Sie eine Regel des Typs KEINE DNAT erstellen, lassen Sie das Textfeld leer.
Anwendung	<p>(Optional) Wählen Sie ein spezifisches Anwendungsportprofil aus, auf das die Regel angewendet werden soll.</p> <p>Das Anwendungsportprofil enthält einen Port und ein Protokoll, das der eingehende Datenverkehr auf dem Edge-Gateway verwendet, um eine Verbindung mit dem internen Netzwerk herzustellen.</p>
Erweiterte Einstellungen (optional)	<p>Klicken Sie auf die Registerkarte Erweiterte Einstellungen, um weitere Einstellungen anzuzeigen.</p> <p>Zustand</p> <p>Um die Regel bei der Erstellung zu aktivieren, aktivieren Sie die Umschaltoption Zustand.</p> <p>Protokollierung</p> <p>Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung.</p> <p>Priorität</p> <p>Wenn eine Adresse über mehrere NAT-Regeln verfügt, können Sie diesen Regeln verschiedene Prioritäten zuweisen und somit die Reihenfolge bestimmen, in der sie angewendet werden. Ein niedrigerer Wert bedeutet eine höhere Priorität für diese Regel.</p> <p>Firewall-Übereinstimmung</p> <p>Sie können eine Regel für die Firewall-Übereinstimmung festlegen, um die Anwendung der Firewall während NAT anzugeben. Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus.</p> <ul style="list-style-type: none"> ■ Zum Anwenden von Firewallregeln auf die interne Adresse einer NAT-Regel wählen Sie Interne Adresse abgleichen aus. ■ Zum Anwenden von Firewallregeln auf die externe Adresse einer NAT-Regel wählen Sie Externe Adresse abgleichen aus. ■ Zum Überspringen der Anwendung von Firewallregeln wählen Sie Bypass aus.

6 Klicken Sie auf **Speichern**.

7 Wiederholen Sie diese Schritte, um zusätzliche Regeln zu konfigurieren.

Konfigurieren eines DNS-Weiterleitungsdiensts auf einem NSX-T-Edge-Gateway

Konfigurieren Sie zur Weiterleitung von DNS-Abfragen an externe DNS-Server eine DNS-Weiterleitung.

Im Rahmen der Konfiguration des DNS-Weiterleitungsdiensts können Sie auch bedingte Weiterleitungszonen hinzufügen. Eine bedingte Weiterleitungszone wird als Liste mit bis zu fünf FQDN-DNS-Zonen konfiguriert. Wenn eine DNS-Abfrage mit einem Domännennamen aus dieser Liste übereinstimmt, wird die Abfrage von der entsprechenden Weiterleitungszone an die Server weitergeleitet.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway und unter **IP-Verwaltung** auf **DNS**.
- 3 Klicken Sie im Abschnitt **DNS-Weiterleitung** auf **Bearbeiten**.
- 4 Um den DNS-Weiterleitungsdienst zu aktivieren, verwenden Sie die Umschaltoption **Zustand**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für die standardmäßige DNS-Zone ein.
- 6 Geben Sie eine oder mehrere, durch Kommas getrennte IP-Adressen für den Upstream-Server ein.
- 7 Klicken Sie auf **Speichern**.
- 8 (Optional) Fügen Sie eine bedingte Weiterleitungszone hinzu.
 - a Klicken Sie im Abschnitt **Bedingte Weiterleitungszone** auf **Hinzufügen**.
 - b Geben Sie einen Namen für die Weiterleitungszone ein.
 - c Geben Sie eine oder mehrere, durch Kommas getrennte IP-Adressen für den Upstream-Server ein.
 - d Geben Sie einen oder mehrere, durch Kommas getrennte Domännennamen ein und klicken Sie auf **Speichern**.

Erstellen von benutzerdefinierten Anwendungsportprofilen

Zum Erstellen von Firewall- und NAT-Regeln können Sie vorkonfigurierte Anwendungsportprofile und benutzerdefinierte Anwendungsportprofile verwenden.

Anwendungsportprofile enthalten eine Kombination aus einem Protokoll und einem Port oder einer Gruppe von Ports, die für Firewall- und NAT-Dienste auf dem Edge-Gateway verwendet wird. Zusätzlich zu den standardmäßigen Portprofilen, die für NSX-T Data Center vorkonfiguriert sind, können Sie benutzerdefinierte Anwendungsportprofile erstellen.

Wenn Sie ein benutzerdefiniertes Anwendungsportprofil auf einem Edge-Gateway erstellen, wird es für alle anderen NSX-T Data Center-Edge-Gateways sichtbar, die sich im selben Organisations-VDC befinden.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Klicken Sie unter **Sicherheit** auf **Anwendungsportprofile**.
- 4 Klicken Sie im Abschnitt **Benutzerdefinierte Anwendungen** auf **Neu**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für das Anwendungsportprofil ein.
- 6 Wählen Sie ein Protokoll aus dem Dropdown-Menü aus.
- 7 Geben Sie einen Port oder einen durch Kommas getrennten Portbereich ein und klicken Sie auf **Speichern**.

Nächste Schritte

Verwenden Sie Anwendungsportprofile, um Firewall- und NAT-Regeln zu erstellen. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für NSX-T Data Center Edge-Gateways](#) und [Hinzufügen einer SNAT- oder DNAT-Regel zu einem NSX-T-Edge-Gateway](#).

Richtlinienbasiertes IPSec-VPN für NSX-T Data Center-Edge-Gateways

Ab Version 10.1 unterstützt VMware Cloud Director richtlinienbasiertes IPSec-VPN mit Site-to-Site-Konnektivität zwischen einer NSX-T Data Center-Edge-Gateway-Instanz und einer Remote-Site.

IPSec-VPN bietet Site-to-Site-Konnektivität zwischen einem Edge-Gateway und Remote-Sites, die ebenfalls NSX-T Data Center verwenden oder mit Drittanbieter-Hardware-Routern oder VPN-Gateways, die IPSec unterstützen, konfiguriert sind.

Richtlinienbasiertes IPSec-VPN erfordert, dass eine VPN-Richtlinie auf Pakete angewendet wird, um zu ermitteln, welcher Datenverkehr vor dem Passieren eines VPN-Tunnels durch IPSec geschützt werden soll. Dieser VPN-Typ wird als statisch betrachtet, da die VPN-Richtlinieneinstellungen bei einer Änderung der lokalen Netzwerktopologie und -konfiguration ebenfalls aktualisiert werden müssen, um die Änderungen zu berücksichtigen.

NSX-T Data Center-Edge-Gateways unterstützen die Split-Tunnel-Konfiguration, wobei der IPSec-Datenverkehr eine Routing-Priorität hat.

VMware Cloud Director unterstützt die automatische Routenneuverteilung, wenn Sie IPSec-VPN auf einem NSX-T-Edge-Gateway verwenden.

Konfigurieren des richtlinienbasierten NSX-T-IPSec-VPN

Sie können die Site-to-Site-Konnektivität zwischen einem NSX-T Data Center-Edge-Gateway und Remote-Sites konfigurieren. Die Remote-Sites müssen NSX-T Data Center verwenden und über Hardwarerouter von Drittanbietern oder VPN-Gateways verfügen, die IPSec unterstützen.

VMware Cloud Director unterstützt die automatische Route Redistribution, wenn Sie IPSec-VPN auf einem NSX-T Data Center-Gateway konfigurieren.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Klicken Sie unter **Dienste** auf **IPSec-VPN**.
- 4 Um einen IPSec-VPN-Tunnel zu konfigurieren, klicken Sie auf **Neu**.
- 5 Geben Sie einen Namen und, optional, eine Beschreibung für den IPSec-VPN-Tunnel ein.
- 6 Um den Tunnel bei der Erstellung zu aktivieren, aktivieren Sie die Option **Aktiviert**.
- 7 Wählen Sie einen vorinstallierten Schlüssel für die Eingabe aus.

Hinweis Der vorinstallierte Schlüssel muss am anderen Ende des IPSec-VPN-Tunnels identisch sein.

- 8 Geben Sie eine der IP-Adressen ein, die für das Edge-Gateway für den lokalen Endpoint verfügbar sind.

Hinweis Bei der IP-Adresse muss es sich entweder um die primäre IP des Edge-Gateways oder um eine IP-Adresse handeln, die dem Edge-Gateway vom externen Netzwerk separat zugeteilt wird.

- 9 Geben Sie mindestens eine lokale IP-Subnetz-Adresse in CIDR-Notation ein, die für den IPSec-VPN-Tunnel verwendet werden soll.
- 10 Geben Sie die IP-Adresse für die Remote-Site ein.
- 11 Geben Sie mindestens eine Remote-IP-Subnetz-Adresse in CIDR-Notation ein, die für den IPSec-VPN-Tunnel verwendet werden soll.
- 12 (Optional) Zum Aktivieren der Protokollierung wählen Sie die Option **Protokollierung** aus.
- 13 Klicken Sie auf **Speichern**.
- 14 Um sicherzustellen, dass der Tunnel funktioniert, wählen Sie ihn aus und klicken auf **Statistik anzeigen**.

Wenn der Tunnel funktioniert, wird für die Optionen **Tunnelstatus** und **IKE-Dienststatus** die Option **Erreichbar** angezeigt.

Ergebnisse

Der neu erstellte IPSec-VPN-Tunnel wird in der Ansicht **IPSec-VPN** angezeigt. Der IPSec-VPN-Tunnel wird mit einem Standardsicherheitsprofil erstellt.

Nächste Schritte

Sie können die IPSec-VPN-Tunnel-Einstellungen bearbeiten und das entsprechende Sicherheitsprofil nach Bedarf anpassen.

Anpassen des Sicherheitsprofils eines IPSec-VPN-Tunnels

Wenn Sie das vom System generierte Sicherheitsprofil, das Ihrem IPSec-VPN-Tunnel bei der Erstellung zugewiesen wurde, nicht verwenden möchten, können Sie es anpassen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Klicken Sie unter **Dienste** auf **IPSec-VPN**.
- 4 Wählen Sie den IPSec-VPN-Tunnel aus und klicken Sie auf **Anpassung des Sicherheitsprofils**.
- 5 Konfigurieren Sie die IKE-Profile.

Die IKE-Profile (Internet Key Exchange) stellen Informationen zu den Algorithmen bereit, die zur Authentifizierung, Verschlüsselung und Einrichtung eines gemeinsamen geheimen Schlüssels zwischen Netzwerksites verwendet werden, wenn Sie einen IKE-Tunnel einrichten.

- a Wählen Sie eine IKE-Protokollversion aus, um eine Sicherheitsverbindung (Security Association, SA) in der IPSec-Protokollsuite einzurichten.

Option	Bezeichnung
IKEv1	Wenn Sie diese Option auswählen, initiiert das IPSec-VPN nur das IKEv1-Protokoll und antwortet auch nur auf dieses Protokoll.
IKEv2	Die Standardoption. Wenn Sie diese Version auswählen, initiiert das IPSec-VPN nur das IKEv2-Protokoll und antwortet auch nur auf dieses Protokoll.
IKE-Flex	Wenn Sie diese Option auswählen und die Tunneleinrichtung mit dem IKEv2-Protokoll fehlschlägt, wird die Quellsite nicht zurückgesetzt und initiiert keine Verbindung mit dem IKEv1-Protokoll. Stattdessen wird die Verbindung akzeptiert, falls die Remote-Site eine Verbindung mit dem IKEv1-Protokoll initiiert.

- b Wählen Sie einen unterstützten Verschlüsselungsalgorithmus aus, der bei der IKE-Verhandlung (Internet Key Exchange) verwendet wird.
- c Wählen Sie im Dropdown-Menü **Digest** einen sicheren Hashing-Algorithmus aus, der während der IKE-Verhandlung verwendet wird.

- d Wählen Sie im Dropdown-Menü **Diffie-Hellman-Gruppe** eines der Kryptografieschemata aus, die es der Peer-Site und dem Edge-Gateway ermöglichen, einen gemeinsamen geheimen Schlüssel über einen unsicheren Kommunikationskanal einzurichten.
- e (Optional) Ändern Sie im Textfeld **Gültigkeitsdauer der Zuordnung** die Standardanzahl von Sekunden, bis der IPSec-Tunnel wiederhergestellt werden muss.

6 Konfigurieren Sie den IPSec-VPN-Tunnel.

- a Um Perfect Forward Secrecy zu aktivieren, wählen Sie die entsprechende Option aus.
- b Wählen Sie eine Defragmentierungsrichtlinie aus.

Die Defragmentierungsrichtlinie hilft bei der Verarbeitung von Defragmentierungsbits im inneren Paket.

Option	Bezeichnung
Kopieren	Kopiert das Defragmentierungsbit aus dem inneren IP-Paket in das äußere Paket.
Löschen	Ignoriert das im inneren Paket anwesende Defragmentierungsbit.

- c Wählen Sie einen unterstützten Verschlüsselungsalgorithmus aus, der bei der IKE-Verhandlung (Internet Key Exchange) verwendet wird.
- d Wählen Sie im Dropdown-Menü **Digest** einen sicheren Hashing-Algorithmus aus, der während der IKE-Verhandlung verwendet wird.
- e Wählen Sie im Dropdown-Menü **Diffie-Hellman-Gruppe** eines der Kryptografieschemata aus, die es der Peer-Site und dem Edge-Gateway ermöglichen, einen gemeinsamen geheimen Schlüssel über einen unsicheren Kommunikationskanal einzurichten.
- f (Optional) Ändern Sie im Textfeld **Gültigkeitsdauer der Zuordnung** die Standardanzahl von Sekunden, bis der IPSec-Tunnel wiederhergestellt werden muss.

7 (Optional) Ändern Sie im Textfeld **Prüfintervall** die Standardanzahl der Sekunden für die Erkennung von ausgefallenen Peers.

8 Klicken Sie auf **Speichern**.

Ergebnisse

In der Ansicht „IPSec-VPN“ wird das Sicherheitsprofil des IPSec-VPN-Tunnels als **Benutzerdefiniert** angezeigt.

Konfigurieren dedizierter externer Netzwerkdienste

Um eine vollständig geroutete Netzwerktopologie in einem virtuellen Datacenter bereitzustellen, kann der **Systemadministrator** ein externes Netzwerk für ein bestimmtes NSX-T Data Center-Edge-Gateway reservieren.

Bei Verwendung eines dedizierten externen Netzwerks können Sie zusätzliche Routing-Dienste konfigurieren, wie z. B. die Routenankündigungsverwaltung und die BGP-Konfiguration (Border Gateway Protocol).

Verfahren

1 Verwalten der Routenankündigung

Mithilfe der Routenankündigung können Sie in einem virtuellen Datacenter (VDC) einer Organisation eine vollständig geroutete Netzwerkumgebung erstellen.

2 Konfigurieren von allgemeinen BGP-Einstellungen

Sie können eine externe oder interne Border Gateway Protocol (eBGP oder iBGP)-Verbindung zwischen einem NSX-T Data Center-Edge-Gateway mit einem dedizierten externen Netzwerk und einem Router in Ihrer physischen Infrastruktur konfigurieren.

3 Erstellen einer IP-Präfixliste

Sie können IP-Präfixlisten erstellen, die eine oder mehrere IP-Adressen enthalten. Sie verwenden IP-Präfixlisten, um BGP-Nachbarn Zugriffsberechtigungen für die Routenankündigung zuzuweisen.

4 Hinzufügen eines BGP-Nachbarn

Sie können einzelne Einstellungen für die BGP-Routing-Nachbarn konfigurieren, wenn Sie sie hinzufügen.

Verwalten der Routenankündigung

Mithilfe der Routenankündigung können Sie in einem virtuellen Datacenter (VDC) einer Organisation eine vollständig geroutete Netzwerkumgebung erstellen.

Sie können entscheiden, welches der an das NSX-T Data Center-Edge-Gateway angehängten Subnetze für das dedizierte externe Netzwerk angekündigt werden soll.

Wenn dem Ankündigungsfilter kein Subnetz hinzugefügt wird, wird die Route dorthin dem externen Netzwerk nicht angekündigt. In diesem Fall bleibt das Subnetz privat.

Hinweis VMware Cloud Director kündigt jedes VDC-Organisationsnetzwerk an, das unter die angegebene Route fällt. Aus diesem Grund müssen Sie nicht für jedes Subnetz, das Teil eines angekündigten Netzwerks ist, einen Filter erstellen.

Die Routenankündigung wird automatisch auf dem NSX-T Data Center-Edge-Gateway konfiguriert.

VMware Cloud Director unterstützt die automatische Route Redistribution (Routenneuverteilung), wenn Sie auf einem NSX-T-Edge-Gateway die Routenankündigung verwenden. Die Route Redistribution wird automatisch auf dem logischen Tier-0-Router konfiguriert, der das dedizierte externe Netzwerk darstellt.

Voraussetzungen

- Stellen Sie sicher, dass der **Systemadministrator** einem NSX-T Data Center-Edge-Gateway in Ihrer Organisation ein externes Netzwerk zugewiesen hat.
- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Klicken Sie unter **Routing** auf **Routenankündigung** und **Bearbeiten**.
- 4 Um ein anzukündigendes Subnetz hinzuzufügen, klicken Sie auf **Hinzufügen**.
- 5 Fügen Sie ein IPv4- oder IPv6-Subnetz hinzu.

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

Konfigurieren von allgemeinen BGP-Einstellungen

Sie können eine externe oder interne Border Gateway Protocol (eBGP oder iBGP)-Verbindung zwischen einem NSX-T Data Center-Edge-Gateway mit einem dedizierten externen Netzwerk und einem Router in Ihrer physischen Infrastruktur konfigurieren.

BGP trifft wichtige Routing-Entscheidungen mithilfe einer Tabelle mit IP-Netzwerken oder Präfixen, die mehrere Routen zwischen autonomen Systemen (AS) festlegen.

Der Begriff „BGP-Speaker“ bezieht sich 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 beizubehalten.

Hinweis In einem Edge-Gateway, das mit einem von einem VRF-Gateway gestützten externen Netzwerk verbunden ist, sind die Einstellungen für die lokale AS-Nummer und das ordnungsgemäße Neustarten schreibgeschützt. Der **Systemadministrator** kann diese Einstellungen auf dem untergeordneten Tier-0-Gateway in NSX-T Data Center bearbeiten.

Voraussetzungen

- Stellen Sie sicher, dass der **Systemadministrator** einem NSX-T Data Center-Edge-Gateway in Ihrer Organisation ein externes Netzwerk zugewiesen hat.
- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Klicken Sie unter **Routing** auf **BGP** und klicken Sie unter **Konfiguration** auf **Bearbeiten**.
- 4 Wählen Sie die Option **Status** aus, um BGP zu aktivieren.
- 5 Geben Sie die ID-Nummer des autonomen Systems (AS) ein, die für die lokale AS-Funktion des Protokolls verwendet werden soll.

VMware Cloud Director weist dem Edge-Gateway die lokale AS-Nummer zu. Das Edge-Gateway kündigt diese ID an, wenn es eine Verbindung mit seinen BGP-Nachbarn in anderen autonomen Systemen herstellt.

- 6 Wählen Sie im Dropdown-Menü die Option **Graceful Restart-Modus** aus.

Option	Bezeichnung
Hilfsmodus und Graceful Restart	<p>Es ist nicht empfehlenswert, die Funktion „Graceful Restart“ auf dem Edge-Gateway zu aktivieren, da BGP-Peerings von allen Gateways immer aktiv sind.</p> <p>Bei einem Failover verlängert die Funktion „Graceful Restart“ die Zeit, die ein Remotenachbar benötigt, um ein alternatives Tier-0-Gateway auszuwählen. Dies verzögert die BFD-basierte Konvergenz.</p> <p>Hinweis Die Konfiguration des Edge-Gateways gilt für alle BGP-Nachbarn, es sei denn, die spezifische Konfiguration eines Nachbarn überschreibt sie.</p>
Nur Hilfsmodus	Nützlich für das Reduzieren oder Eliminieren der Unterbrechung des Datenverkehrs, der mit Routen verknüpft ist, die von einem Nachbarn gelernt wurden, der einen Graceful Restart ermöglicht. Der Nachbar muss seine Weiterleitungstabelle beibehalten können, während er einen Neustart durchläuft.
Deaktivieren	Deaktivieren Sie den Graceful Restart-Modus auf dem Edge-Gateway.

- 7 (Optional) Ändern Sie den Standardwert für den Graceful Restart-Timer.
- 8 (Optional) Ändern Sie den Standardwert für den Timer für veraltete Routen.
- 9 Wählen Sie die Option **ECMP** aus, um ECMP zu aktivieren.
- 10 Klicken Sie auf **Speichern**.

Nächste Schritte

- [Erstellen einer IP-Präfixliste](#)
- [Hinzufügen eines BGP-Nachbarn](#)

Erstellen einer IP-Präfixliste

Sie können IP-Präfixlisten erstellen, die eine oder mehrere IP-Adressen enthalten. Sie verwenden IP-Präfixlisten, um BGP-Nachbarn Zugriffsberechtigungen für die Routenankündigung zuzuweisen.

Die IP-Präfixlisten werden über BGP-Nachbarfilter referenziert, um die Anzahl der BGP-Updates zu begrenzen, die zwischen BGP-Peers ausgetauscht werden. Mithilfe der Routenfilterung können Sie die Menge an Systemressourcen reduzieren, die für BGP-Updates benötigt wird.

Beispielsweise können Sie die IP-Adresse 192.168.100.3/27 zur IP-Präfixliste hinzufügen und verhindern, dass die Route zum Edge-Gateway neu verteilt wird.

Sie können auch eine IP-Adresse mit den Modifizierern `less than or equal to (le)` (kleiner als oder gleich) und `greater than or equal to (ge)` (größer als oder gleich) anhängen, um die Route Redistribution zu ermöglichen oder einzuschränken. Beispielsweise entsprechen die Modifizierer „ge 26“ und „le 32“ der IP-Adresse 192.168.100.3/27 den Subnetzmasken, die größer oder gleich 26 Bit und kleiner oder gleich 32 Bit sind.

Voraussetzungen

- Stellen Sie sicher, dass der **Systemadministrator** einem NSX-T Data Center-Edge-Gateway in Ihrer Organisation ein externes Netzwerk zugewiesen hat.
- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- [Konfigurieren von allgemeinen BGP-Einstellungen](#).

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Klicken Sie unter **Routing** auf **BGP** und **IP-Präfixlisten**.
- 4 Um eine IP-Präfixliste hinzuzufügen, klicken Sie auf **Neu**.
- 5 Geben Sie einen Namen und, optional, eine Beschreibung für die Präfixliste ein.
- 6 Klicken Sie auf **Neu** und fügen Sie eine CIDR-Notation für das Präfix hinzu.
- 7 Wählen Sie im Dropdown-Menü eine Aktion aus, die auf das Präfix angewendet werden soll.
- 8 (Optional) Geben Sie die Modifizierer `greater than or equal to` und `less than or equal to` ein, um die Route Redistribution zu ermöglichen oder einzuschränken.

Nächste Schritte

- Sie können die IP-Präfixliste nach Bedarf bearbeiten oder löschen.
- Konfigurieren Sie die Routenfilterung. Weitere Informationen finden Sie im [Hinzufügen eines BGP-Nachbarn](#).

Hinzufügen eines BGP-Nachbarn

Sie können einzelne Einstellungen für die BGP-Routing-Nachbarn konfigurieren, wenn Sie sie hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass der **Systemadministrator** einem NSX-T Data Center-Edge-Gateway in Ihrer Organisation ein externes Netzwerk zugewiesen hat.
- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben oder dass Ihnen eine Rolle mit entsprechenden Rechten zugewiesen ist.
- Stellen Sie sicher, dass Sie die globalen BGP-Einstellungen für das Edge-Gateway konfiguriert haben. Weitere Informationen finden Sie im [Konfigurieren von allgemeinen BGP-Einstellungen](#).
- Wenn Sie die Routenfilterung verwenden, stellen Sie sicher, dass Sie IP-Präfixlisten erstellt haben. Weitere Informationen finden Sie im [Erstellen einer IP-Präfixliste](#).

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das Edge-Gateway.
- 3 Klicken Sie unter **Routing** auf **BGP** und dann auf **Nachbarn**.
- 4 Um einen neuen BGP-Nachbarn hinzuzufügen, klicken Sie auf **Neu**.
- 5 Geben Sie die allgemeinen Einstellungen für den neuen BGP-Nachbarn ein.
 - a Geben Sie eine IPv4- oder IPv6-Adresse für den neuen BGP-Nachbarn ein.
 - b Geben Sie eine Remotenummer des autonomen Systems (AS) im ASPLAIN-Format ein.
 - c Geben Sie ein Zeitintervall zwischen dem Senden von Keep Alive-Nachrichten an einen BGP-Peer ein.
 - d Geben Sie ein Zeitintervall ein, bevor Sie einen BGP-Peer als ausgefallen deklarieren.
 - e Wählen Sie im Dropdown-Menü die Option **Graceful Restart-Modus** für diesen Nachbarn aus.

Option	Bezeichnung
Deaktivieren	Überschreibt die Einstellungen des globalen Edge-Gateways und deaktiviert den Graceful Restart-Modus für diesen Nachbarn.
Nur Hilfsmodus	Überschreibt die Einstellungen des globalen Edge-Gateways und konfiguriert den Graceful Restart-Modus für diesen Nachbarn als Nur Hilfsmodus .
Graceful Restart und Hilfsmodus	Überschreibt die Einstellungen des globalen Edge-Gateways und konfiguriert den Graceful Restart-Modus für diesen Nachbarn als Graceful Restart und Hilfsmodus .

- f Wählen Sie die Option **AllowAS-in** aus, um den Empfang von Routen mit demselben AS zu aktivieren.
 - g Wenn der BGP-Nachbar eine Authentifizierung erfordert, geben Sie das Kennwort für den BGP-Nachbarn ein.
- 6 Konfigurieren Sie die Einstellungen für die bidirektionale Weiterleitungserkennung (Bidirectional Forwarding Detection, BFD) für den neuen BGP-Nachbarn.
 - a (Optional) Wählen Sie die Option **BFD** aus, um BFD für die Fehlererkennung zu aktivieren.
 - b Legen Sie im Textfeld „BFD-Intervall“ das Zeitintervall für das Senden von Taktsignalkpaketen fest.
 - c Geben Sie im Textfeld **Dead Multiple** ein, wie oft das Senden der Taktsignalkpakete durch den BGP-Nachbarn fehlschlagen kann, bevor BFD den BGP-Nachbarn als ausgefallen ansieht.
- 7 (Optional) Konfigurieren Sie die Routenfilterung.
 - a Wählen Sie im Dropdown-Menü **IP-Adressfamilie** eine IP-Adressfamilie aus.
 - b Um einen eingehenden Filter zu konfigurieren, wählen Sie eine IP-Präfixliste aus.
 - c Um einen ausgehenden Filter zu konfigurieren, wählen Sie eine IP-Präfixliste aus.
- 8 Klicken Sie auf **Speichern**.

Nächste Schritte

Sie können den Status jedes BGP-Nachbarn anzeigen, bearbeiten oder BGP-Nachbarn nach Bedarf löschen.

Arbeiten mit NSX Advanced Load Balancing

Indem Sie als **Organisationsadministrator** virtuelle Dienste, die Datenverkehr über mehrere Serverpools verteilen, konfigurieren, können Sie die Arbeitslasten in Ihren von NSX-T Data Center gestützten Datencentern ausgleichen.

Ab Version 10.2 bietet VMware Cloud Director Lastausgleichsdienste mithilfe der Funktionen von VMware NSX Advanced Load Balancer (Avi Networks).

VMware Cloud Director unterstützt L4- und L7-Lastausgleich, den Sie auf einem NSX-T Data Center-Edge-Gateway konfigurieren können.

Layer-4-Lastausgleich (L4) leitet Datenverkehr basierend auf Daten aus Netzwerk- und Transportebenenprotokollen weiter, z. B. IP-Adresse und TCP-Port.

Layer-7-Lastausgleich (L7) verteilt Datenverkehr basierend auf Attributen wie HTTP-Header, Uniform Resource Identifier, SSL-Sitzungs-ID und HTML-Formulardaten.

Aktivieren des Lastausgleichsdiensts auf einem NSX-T Data Center-Edge-Gateway.

Ein **Organisationsadministrator** kann Lastausgleichsdienste erst konfigurieren, nachdem ein **Systemadministrator** den Lastausgleichsdienst auf dem NSX-T Data Center-Edge-Gateway aktiviert hat.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Systemadministrator** haben.
- Vergewissern Sie sich, dass Sie VMware NSX Advanced Load Balancer in Ihrer Cloud-Infrastruktur integriert haben. Weitere Informationen zum Verwalten von NSX Advanced Load Balancer finden Sie unter *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das NSX-T Data Center-Edge-Gateway, auf dem Lastausgleich aktiviert werden soll.
- 3 Klicken Sie unter „Lastausgleichsdienst“ auf **Allgemeine Einstellungen**.
- 4 Klicken Sie auf **Bearbeiten** und schalten Sie die Option **Lastausgleichsdienst-Zustand** ein.
- 5 Geben Sie ein Netzwerk-CIDR für das Subnetz eines Dienstnetzwerks ein, dessen IP-Adressen für die Erstellung von virtuellen Diensten verwendet werden sollen.

Sie können das Standardsubnetzes des Dienstnetzwerks verwenden, indem Sie das Kontrollkästchen **Standardeinstellungen verwenden** aktivieren.
- 6 Klicken Sie auf **Speichern**.

Nächste Schritte

[Zuweisen einer Dienstmodulgruppe zu einem NSX-T Data Center-Edge-Gateway.](#)

Zuweisen einer Dienstmodulgruppe zu einem NSX-T Data Center-Edge-Gateway

Ein **Organisationsadministrator** kann Lastausgleichsdienste auf einem NSX-T Data Center-Edge-Gateway erst konfigurieren, wenn ein **Systemadministrator** dem Edge-Gateway eine Dienstmodulgruppe zugewiesen hat.

Die vom NSX Advanced Load Balancer bereitgestellte Lastausgleichs-Computing-Infrastruktur ist in Dienstmodulgruppen gegliedert. Ein **Systemadministrator** kann einem NSX-T Data Center-Edge-Gateway eine oder mehrere Dienstmodulgruppen zuweisen.

Alle Dienstmodulgruppen, die einem einzelnen Edge Gateway zugewiesen sind, verwenden dasselbe Dienstnetzwerk.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Systemadministrator** haben.

- [Aktivieren des Lastausgleichsdiensts auf einem NSX-T Data Center-Edge-Gateway..](#)

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das NSX-T Data Center-Edge-Gateway, dem Sie eine Dienstmodulgruppe zuweisen möchten.
- 3 Klicken Sie unter „Lastausgleichsdienst“ auf **Dienstmodulgruppen**.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Wählen Sie eine verfügbare Dienstmodulgruppe in der Liste aus.
- 6 Geben Sie einen Wert für die maximale Anzahl an virtuellen Diensten ein, die auf dem Edge-Gateway platziert werden können.
- 7 Geben Sie die Anzahl für die garantierten virtuellen Dienste ein, die dem Edge-Gateway zur Verfügung stehen.
- 8 Klicken Sie zum Bestätigen der Einstellungen auf **Speichern**.

Bearbeiten der Einstellungen einer Dienstmodulgruppe

Ein **Systemadministrator** kann die maximale Anzahl unterstützter virtueller Dienste und die Anzahl der reservierten virtuellen Dienste für eine Dienstmodulgruppe bearbeiten.

Wenn nach der Synchronisierung einer Dienstmodulgruppe die neue maximale Anzahl unterstützter virtueller Dienste niedriger als die Anzahl der reservierten virtuellen Dienste ist, wird die Dienstmodulgruppe als „Überlastet“ gekennzeichnet.

Wenn eine Dienstmodulgruppe überlastet ist, kann die Erstellung eines neuen virtuellen Diensts fehlschlagen, selbst wenn das Edge-Gateway, auf dem der virtuelle Dienst erstellt wird, über ausreichend reservierte Kapazität verfügt.

Um beim Bearbeiten der Einstellungen einer Dienstmodulgruppe zu verhindern, dass die Erstellung des virtuellen Diensts fehlschlägt, verringern Sie die maximale Anzahl unterstützter virtueller Dienste nicht unter die Anzahl der ursprünglich reservierten virtuellen Dienste.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Systemadministrator** haben.
- [Aktivieren des Lastausgleichsdiensts auf einem NSX-T Data Center-Edge-Gateway..](#)
- [Zuweisen einer Dienstmodulgruppe zu einem NSX-T Data Center-Edge-Gateway](#) eine Dienstmodulgruppe zu.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.

- 2 Klicken Sie auf das NSX-T Data Center-Edge-Gateway, dem die Dienstmodulgruppe zugewiesen ist.
- 3 Klicken Sie unter „Lastausgleichsdienst“ auf **Dienstmodulgruppen**.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Bearbeiten Sie die Anzahl der maximal zulässigen virtuellen Dienste, die vom Edge-Gateway verwendet werden können.

Verringern Sie die Anzahl nicht, es sei denn, dies ist obligatorisch. Andernfalls treten beim Erstellen virtueller Dienste möglicherweise Fehler auf.
- 6 Bearbeiten Sie die Anzahl der garantierten virtuellen Dienste, die dem Edge-Gateway zur Verfügung stehen.
- 7 Klicken Sie auf **Speichern**.

Hinzufügen eines Serverpools für den Lastausgleichsdienst

Bei einem Serverpool handelt es sich um eine aus einem oder mehreren Servern bestehende Gruppe, die zur Ausführung derselben Anwendung und zur Bereitstellung von Hochverfügbarkeit konfiguriert wird.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben.
- Stellen Sie sicher, dass der **Systemadministrator** Lastausgleich auf dem NSX-T Edge-Gateway aktiviert hat.
- Stellen Sie sicher, dass der **Systemadministrator** dem Edge-Gateway mindestens eine Dienstmodulgruppe zugewiesen hat.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das NSX-T Data Center-Edge-Gateway, für das ein Lastausgleichsdienst-Pool konfiguriert werden soll.
- 3 Klicken Sie unter „Lastausgleichsdienst“ auf **Pools** und dann auf **Hinzufügen**.

4 Konfigurieren Sie die allgemeinen Einstellungen für den Lastausgleichsdienst-Pool.

- a Geben Sie einen aussagekräftigen Namen und optional eine Beschreibung für den Serverpool ein.
- b Wählen Sie eine algorithmische Ausgleichsmethode aus.

Mithilfe des Lastausgleichsalgorithmus wird die Verteilung eingehender Verbindungen unter den Mitgliedern des Serverpools festgelegt.

Option	Bezeichnung
Geringste Anzahl an Verbindungen	Neue Verbindungen werden an den Server gesendet, der aktuell die geringste Anzahl an Verbindungen aufweist.
Round-Robin	Neue Verbindungen werden in sequenzieller Reihenfolge an den nächsten geeigneten Server im Pool gesendet.
Schnellste Antwort	Neue Verbindungen werden an den Server gesendet, der aktuell die schnellste Reaktion auf neue Verbindungen oder Anforderungen bereitstellt.
Konsistenter Hash	Neue Verbindungen werden auf die Server verteilt, indem die IP-Adresse des Clients zum Generieren eines IP-Hashschlüssels verwendet wird.
Geringste Last	Neue Verbindungen werden unabhängig von der Anzahl der Verbindungen, die der Server aufweist, an den Server mit der geringsten Last gesendet.
Geringste Anzahl an Servern	Anstatt alle Verbindungen oder Anforderungen auf alle Server zu verteilen, legt der Lastausgleichsdienst die geringste Anzahl an Servern fest, die zum Erfüllen der aktuellen Client-Last erforderlich sind.
Zufällig	Der Lastausgleichsdienst wählt Server nach dem Zufallsprinzip aus.
Geringste Anzahl an Aufgaben	Die Last wird basierend auf dem Server-Feedback adaptiv ausgeglichen.
Kernaffinität	Jeder CPU-Kern verwendet eine Teilmenge von Servern, wobei jeder Server von einer Teilmenge von Kernen genutzt wird. Hierdurch ergibt sich im Prinzip eine n:n-Zuordnung zwischen Servern und Kernen.

- c Um den Serverpool bei der Erstellung zu aktivieren, schalten Sie die Option **Zustand** ein.
- d Geben Sie einen Standardport für den Zielserver ein, der für den Datenverkehr zum Poolmitglied verwendet werden soll.
- e (Optional) Geben Sie in das Textfeld **Zeitlimit für ordnungsgemäßes Deaktivieren** die maximale Zeit in Minuten zum ordnungsgemäßen Deaktivieren eines Poolmitglieds ein.

Der virtuelle Dienst wartet so lange, bis die vorhandenen Verbindungen zu den deaktivierten Mitgliedern geschlossen werden.

- f (Optional) Zum Aktivieren passiver Integritätsüberwachung schalten Sie die Option **Passive Integritätsüberwachung** ein.
- g (Optional) Wählen Sie eine aktive Integritätsüberwachung aus.

Option	Bezeichnung
HTTP	Zum Validieren der Integrität werden eine HTTP-Anforderung und eine -Antwort verwendet.
HTTPS	Wird für Webserver, die mit HTTPS verschlüsselt sind, zum Validieren der Integrität verwendet.
TCP	Die TCP-Verbindung wird zum Validieren der Integrität verwendet.
UDP	Ein UDP-Datagramm wird zum Validieren der Integrität verwendet.
PING	Ein ICMP-Ping wird zum Validieren der Integrität verwendet.

5 Fügen Sie dem Serverpool ein Mitglied hinzu.

- a Klicken Sie auf die Registerkarte **Mitglieder** und dann auf **Hinzufügen**.
- b Geben Sie eine IP-Adresse für das Poolmitglied ein.
- c Schalten Sie die Option **Zustand** ein, um das Poolmitglied zu aktivieren.
- d (Optional) Fügen Sie einen benutzerdefinierten Port für das Serverpoolmitglied hinzu.

Als Portnummer wird standardmäßig der Zielport verwendet, den Sie für den Pool eingegeben haben.

- e Geben Sie ein Verhältnis für das Poolmitglied ein.

Das Verhältnis der einzelnen Poolmitglieder bezeichnet den Datenverkehr, der an jedes Serverpoolmitglied gesendet wird. Ein Server mit einem Verhältnis von 2 empfängt zweimal mehr Datenverkehr als ein Server mit einem Verhältnis von 1. Der Standardwert ist 1.

6 Konfigurieren Sie auf der Registerkarte **SSL-Einstellungen** die SSL-Einstellungen zum Validieren der Zertifikate, die von den Mitgliedern des Lastausgleichsdienst-Pools angezeigt werden.

- a Zum Aktivieren von SSL schalten Sie die Option **SSL-aktiviert** ein.
- b Zum Ausblenden von Zertifikaten mit privaten Schlüsseln und ausschließlichen Anzeigen einer Liste mit CA-Zertifikaten aktivieren Sie das Kontrollkästchen **Dienstzertifikate ausblenden**.

7 Um die Überprüfung des allgemeinen Namens für Serverzertifikate zu aktivieren, schalten Sie die Option **Überprüfung des allgemeinen Namens** ein und geben Sie bis zu 10 Domännennamen für den Pool ein.

8 Klicken Sie auf **Speichern**.

Nächste Schritte

[Erstellen eines virtuellen Diensts.](#)

Erstellen eines virtuellen Diensts

Ein virtueller Dienst überwacht den Datenverkehr für eine IP-Adresse, verarbeitet Clientanforderungen und leitet gültige Anforderungen an ein Mitglied des Lastausgleichsdienst-Serverpools weiter.

Bei einem virtuellen Dienst handelt es sich um eine Kombination aus einer IP-Adresse und einem Port, der ein einzelnes Netzwerkprotokoll verwendet. Der virtuelle Dienst wird für externe Netzwerke angekündigt und überwacht Clientanforderungen. Wenn ein Client eine Verbindung zum virtuellen Dienst herstellt, leitet der Lastausgleichsdienst die Anforderung an ein Mitglied des konfigurierten Lastausgleichsdienst-Serverpools weiter.

Zum Sichern von SSL-Beendigung für einen virtuellen Dienst können Sie ein Zertifikat aus der Zertifikatsbibliothek verwenden. Weitere Informationen finden Sie unter [Importieren von Zertifikaten in die Zertifikatsbibliothek](#).

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben.
- Stellen Sie sicher, dass der **Systemadministrator** Lastausgleich auf dem NSX-T Edge-Gateway aktiviert hat.
- Stellen Sie sicher, dass der **Systemadministrator** dem Edge-Gateway mindestens eine Dienstmodulgruppe zugewiesen hat.
- [Hinzufügen eines Serverpools für den Lastausgleichsdienst](#)

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Netzwerk** und dann auf die Registerkarte **Edge-Gateways**.
- 2 Klicken Sie auf das NSX-T Data Center-Edge-Gateway, auf dem ein virtueller Dienst erstellt werden soll.
- 3 Klicken Sie unter „Lastausgleichsdienst“ auf **Virtuelle Dienste** und dann auf **Hinzufügen**.
- 4 Geben Sie einen aussagekräftigen Namen und optional eine Beschreibung für den virtuellen Dienst ein.
- 5 Um den virtuellen Dienst bei der Erstellung zu aktivieren, schalten Sie die Option **Aktiviert** ein.
- 6 Wählen Sie eine Dienstmodulgruppe für den virtuellen Dienst aus.
- 7 Wählen Sie einen Lastausgleichsdienst-Pool für den virtuellen Dienst aus.
- 8 Geben Sie eine IP-Adresse für den virtuellen Dienst ein.

9 Wählen Sie den Typ des virtuellen Diensts aus.

Option	Bezeichnung
HTTP	<p>Der virtuelle Dienst überwacht nicht sichere HTTP-Anforderungen der Ebene 7.</p> <p>Bei Auswahl dieses Diensttyps wird das Textfeld des Dienstports automatisch mit dem Wert 80 befüllt, den Sie durch eine andere gültige Portnummer ersetzen können.</p>
HTTPS	<p>Der virtuelle Dienst überwacht sichere HTTPS-Anforderungen der Ebene 7.</p> <p>Bei Auswahl dieses Diensttyps wird das Textfeld des Dienstports automatisch mit dem Wert 443 befüllt, den Sie durch eine andere gültige Portnummer ersetzen können. Wählen Sie ein SSL-Zertifikat aus, das für SSL-Beendigung verwendet werden soll.</p>
L4	<p>Der virtuelle Dienst überwacht Anforderungen der Ebene 4.</p> <p>Bei Auswahl dieses Diensttyps wird das Textfeld des Dienstports automatisch mit dem Wert 80 befüllt, den Sie durch eine andere gültige Portnummer ersetzen können.</p>
L4-TLS	<p>Der virtuelle Dienst überwacht sichere TLS-Anforderungen der Ebene 4.</p> <p>Bei Auswahl dieses Diensttyps wird das Textfeld des Dienstports automatisch mit dem TCP-Port 443 befüllt, den Sie durch eine andere gültige Portnummer ersetzen können. Wählen Sie ein SSL-Zertifikat aus, das für SSL-Beendigung verwendet werden soll.</p>

10 Klicken Sie auf **Speichern**.

Verwenden benannter Festplatten und Überprüfen von Speicherrichtlinien

6

Im VMware Cloud Director-Mandantenportal können Sie benannte Festplatten erstellen und verwalten und die Speicherrichtlinien des Organisations-VDC überprüfen.

Dieses Kapitel enthält die folgenden Themen:

- Erstellen und Verwenden benannter Festplatten
- Überprüfen der Eigenschaften von Speicherrichtlinien

Erstellen und Verwenden benannter Festplatten

Benannte Festplatten sind eigenständige virtuelle Festplatten, die Sie in Organisations-VDCs erstellen. **Organisationsadministratoren** und Benutzer mit den entsprechenden Rechten können benannte Festplatten erstellen, entfernen und aktualisieren und sie mit virtuellen Maschinen verbinden.

Wenn Sie eine benannte 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 an eine beliebige im VDC bereitgestellte virtuelle Maschine anhängen. Wenn Sie über die Berechtigung **Freigegebene Festplatte erstellen** verfügen, können Sie eine freigegebene Festplatte erstellen, die an mehrere VMs angehängt werden kann. 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.

Hinweis Obwohl vSphere Konfigurationen wie Windows Server Failover Cluster (WSFC) unterstützt und Sie eine gemeinsam genutzte Festplatte über die gemeinsame Verwendung des physischen SCSI-Busses erstellen können, bietet VMware Cloud Director 10.2 keine Unterstützung für diese Funktion. Beim Erstellen einer gemeinsam genutzten Festplatte in VMware Cloud Director erstellen Sie lediglich eine zugrunde liegende unabhängige persistente Festplatte in vSphere mit aktiviertem Multiwriter-Modus.

Wenn Sie eine benannte Festplatte anhängen, können Sie keine VM-Snapshots erstellen. Wenn eine freigegebene Festplatte an eine virtuelle Maschine angehängt wurde, können Sie die zugehörigen Festplatteneinstellungen nicht über die Detailansicht der VM bearbeiten.

Wenn das Organisations-VDC über eine Speicherrichtlinie mit aktivierter VM-Verschlüsselung verfügt, können Sie VMs und Festplatten verschlüsseln, indem Sie sie mit Speicherrichtlinien verknüpfen, die über die VM-Verschlüsselungsfunktion verfügen. Weitere Informationen finden Sie im [Verschlüsselung virtueller Maschinen](#).

Erstellen einer benannten Festplatte

Sie können eine benannte Festplatte erstellen und sie zu einem späteren Zeitpunkt an eine oder mehrere virtuelle Maschinen anhängen.

Um eine benannte Festplatte zu erstellen, müssen Sie deren Namen und Größe angeben. Sie können optional eine Beschreibung angeben und ein von der Festplatte zu verwendendes Speicherprofil auswählen. Sie können eine freigegebene Festplatte erstellen, die an mehrere VMs angehängt werden kann.

Hinweis Obwohl vSphere Konfigurationen wie Windows Server Failover Cluster (WSFC) unterstützt und Sie eine gemeinsam genutzte Festplatte über die gemeinsame Verwendung des physischen SCSI-Busses erstellen können, bietet VMware Cloud Director 10.2 keine Unterstützung für diese Funktion. Beim Erstellen einer gemeinsam genutzten Festplatte in VMware Cloud Director erstellen Sie lediglich eine zugrunde liegende unabhängige persistente Festplatte in vSphere mit aktiviertem Multiwriter-Modus.

Voraussetzungen

- 1 Sie müssen über eine Rolle als **Organisationsadministrator** oder die Rechte eines Festplattenbesitzers verfügen.
- 2 Wenn Sie eine freigegebene Festplatte erstellen möchten, müssen Sie über die Berechtigung **Freigegebene Festplatte erstellen** verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich unter **Speicher** die Option **Benannte 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 benannten Festplatte ein.
- 6 Wählen Sie in den Dropdown-Menüs **Bustyp** und **Bus-Subtyp** jeweils den Bustyp und den Bus-Subtyp aus.
- 7 Wenn Sie die benannte Festplatte an mehrere VMs anhängen möchten, aktivieren Sie das Kontrollkästchen **Freigabefähig**.

Sie können diese Einstellung zu einem späteren Zeitpunkt nicht mehr ändern.

8 Klicken Sie auf **Speichern**.

Nächste Schritte

Verwenden Sie die VMware Cloud Director-API, um die unabhängige Festplatte an eine virtuelle Maschine anzuhängen. Siehe *VMware Cloud Director API-Programmierhandbuch* auf [VMware {code}](#).

Bearbeiten einer benannten Festplatte

Nachdem Sie die Festplatte erstellt haben, können Sie deren Namen, Beschreibung, Speicherrichtlinie und Größe ändern.

Sie können die Einstellung **Freigabefähig** einer benannten Festplatte nicht bearbeiten.

Voraussetzungen

- 1 Sie müssen über eine Rolle als **Organisationsadministrator** oder die Rechte eines Festplattenbesitzers verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich unter **Speicher** die Option **Benannte 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.
- 4 Klicken Sie auf **Speichern**.

Anhängen einer benannten Festplatte an eine virtuelle Maschine

Nachdem Sie eine benannte Festplatte in einem VDC erstellt haben, können Sie sie an eine beliebige virtuelle Maschine anhängen, die im VDC bereitgestellt wird. Sie können eine freigegebene benannte Festplatte an mehrere VMs anhängen.

Voraussetzungen

Sie müssen über eine Rolle als **Organisationsadministrator** oder die Rechte eines Festplattenbesitzers verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich unter **Speicher** die Option **Benannte Festplatten** aus.
- 2 Klicken Sie auf das Optionsfeld neben dem Namen der benannten Festplatte, die Sie an eine virtuelle Maschine anhängen möchten, und klicken Sie dann auf **Anhängen**.

- 3 Wählen Sie im Dropdown-Menü eine virtuelle Maschine aus, an die die benannte Festplatte angehängt werden soll, und klicken Sie auf **Anwenden**.
- 4 Wenn Sie eine andere VM an eine freigegebene Festplatte anhängen möchten, wiederholen Sie [Schritt 2](#) und [Schritt 3](#).

Nächste Schritte

Sie können nach Bedarf weitere benannte Festplatten an die VM anhängen oder von dieser trennen.

Löschen einer benannten Festplatte

Wenn Sie keine benannte Festplatte benötigen, können Sie sie löschen.

Voraussetzungen

Sie müssen über eine Rolle als **Organisationsadministrator** oder die Rechte eines Festplattenbesitzers verfügen.

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden möchten, und wählen Sie im linken Bereich unter **Speicher** die Option **Benannte 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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**.

Sie können den Namen, den Grenzwert, IOPS-Einstellungen und Metadatendetails der Speicherrichtlinie überprüfen.

Überprüfen und Bearbeiten der Eigenschaften von virtuellen Datencentern

7

Als **Organisationsadministrator** können Sie die Eigenschaften des virtuellen Datencenters überprüfen. Sie können den Zugriff auf Organisations-VDCs auch durch Benutzer und Gruppen in Ihrer Organisation steuern.

Dieses Kapitel enthält die folgenden Themen:

- Überprüfen der Eigenschaften von virtuellen Datencentern
- Überprüfen der Metadaten des virtuellen Datencenters
- Begrenzen des Zugriffs auf ein Organisations-VDC auf bestimmte Benutzer und Gruppen in Ihrer Organisation

Überprüfen der Eigenschaften von virtuellen Datencentern

Sie können die Eigenschaften der virtuellen Datencenter 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 **Virtuelles Datencenter** auf die Karte des virtuellen Datencenters, das Sie erkunden 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 Datencenter gehören das Zuweisungsmodell und die vCPU sowie die CPU- und Speichernutzung.

Überprüfen der Metadaten des virtuellen Datacenters

VMware Cloud 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-Datacenters überprüfen.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, das Sie erkunden möchten.
- 2 Klicken Sie unter **Einstellungen** auf **Metadaten**.
Die Liste der verfügbaren Metadaten wird angezeigt.

Begrenzen des Zugriffs auf ein Organisations-VDC auf bestimmte Benutzer und Gruppen in Ihrer Organisation

Als **Organisationsadministrator** können Sie den Zugriff auf jedes der Organisations-VDCs in Ihrer Organisation auf bestimmte Benutzer und Gruppen begrenzen.

Standardmäßig werden Organisations-VDCs für alle Benutzer und Gruppen freigegeben, deren Rolle das Recht **Zugriff auf alle Organisations-VDCs zulassen** umfasst.

Wenn Ihre Organisation über mehrere Organisations-VDCs verfügt und diese separat verwaltet werden sollen, können Sie eine als Organisations-VDC-Administratorrolle fungierende benutzerdefinierte Rolle erstellen, sie bestimmten Benutzern oder Gruppen in Ihrer Organisation zuweisen und ihnen damit nur Zugriff auf die Computing- und Netzwerkressourcen eines bestimmten VDC gewähren.

Voraussetzungen

- 1 Vergewissern Sie sich, dass Sie die Rolle **Organisationsadministrator** haben.
- 2 Erstellen Sie eine benutzerdefinierte Rolle für die Benutzer und Gruppen, denen Sie Zugriff auf ein bestimmtes Organisations-VDC geben möchten. Diese Rolle darf das Recht **Zugriff auf alle Organisations-VDCs zulassen** nicht umfassen. Weitere Informationen finden Sie im [Kapitel 13 Verwalten von Benutzern, Gruppen und Rollen](#).

Verfahren

- 1 Klicken Sie im Dashboard-Bildschirm **Virtuelles Datacenter** auf die Karte des virtuellen Datacenters, dessen Zugriff Sie beschränken möchten.

2 Klicken Sie unter **Einstellungen** auf **Freigaben**.

Die Liste der Benutzer und Gruppen innerhalb der Organisation, die Zugriff auf das VDC haben, wird angezeigt.

3 Um die Zugriffseinstellungen für das Organisations-VDC zu ändern, klicken Sie auf **Bearbeiten**.

4 Wählen Sie **Bestimmte Benutzer und Gruppen** aus.

5 Wählen Sie in der Liste **Benutzer** die Benutzer aus, denen Sie Zugriff auf das VDC gewähren möchten.

6 Wählen Sie in der Liste **Gruppen** die Gruppen aus, denen Sie Zugriff auf das VDC gewähren möchten.

7 Um das VDC für die ausgewählten Benutzer und Gruppen freizugeben, klicken Sie auf **Freigeben**.

Ergebnisse

Der Zugriff auf das Organisations-VDC ist auf die von Ihnen ausgewählten Benutzer und Gruppen beschränkt.

Arbeiten mit dedizierten vCenter Server-Instanzen, -Endpoints und -Proxys



Sie können auf eine dedizierte vCenter Server-Umgebung oder vCenter Server-Komponenten über das VMware Cloud Director Tenant Portal zugreifen.

Dedizierte vSphereDatencenter

In VMware Cloud Director kapselt ein SDDC (Software-Defined Data Center) eine gesamte dedizierte vCenter Server-Umgebung.

Durch dedizierte vCenter Server-Instanzen in VMware Cloud Director entfällt die Notwendigkeit, dass eine vCenter Server-Instanz öffentlich zugänglich sein muss.

Der **Systemadministrator** kann eine oder mehrere dedizierte vCenter Server-Instanzen in Ihrer Organisation veröffentlichen. Sie können die Endpoints verwenden, um auf die Benutzeroberfläche oder die API der Proxy- bzw. Nicht-Proxy-Komponenten zuzugreifen.

Endpoints

Eine dedizierte vCenter Server-Instanz kann einen oder mehrere Endpoints enthalten, die Zugriff auf verschiedene Komponenten aus der zugrunde liegenden Umgebung bieten. Endpoints stellen einen Zugriffspunkt auf eine Datencenter-Komponente bereit, z. B. eine vCenter Server-Instanz, einen ESXi-Host, eine NSX Manager-Instanz oder eine NSX-T Manager-Instanz.

Endpoints können mit einem Proxy verbunden sein oder nicht.

Proxys

VMware Cloud Director kann als HTTPS-Proxy-Server fungieren und den Zugriff auf eine dedizierte vCenter Server-Instanz sowie auf verschiedene Komponenten gemeinsam genutzter oder dedizierter vCenter Server-Instanzen, die Ihre Umgebung stützen, ermöglichen.

Sie können sich über Ihr VMware Cloud Director-Konto bei der Benutzeroberfläche oder der API der Proxy-Komponenten anmelden.

Um auf Proxy-Komponenten zugreifen zu können, müssen Sie entweder Chrome Browser Extension for VMware Cloud Director verwenden oder Ihren Browser manuell mit Ihren Proxy-Einstellungen konfigurieren.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden von Chrome Browser Extension for VMware Cloud Director](#)
- [Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen](#)
- [Anmelden bei der Benutzeroberfläche einer Komponente mithilfe eines Endpoints](#)

Verwenden von Chrome Browser Extension for VMware Cloud Director

Sie können Chrome Browser Extension for VMware Cloud Director zum Anmelden bei den vSphere-Proxy-Komponenten in Ihrer Umgebung verwenden.

Chrome Browser Extension for VMware Cloud Director bietet Proxy-Konfiguration und -Authentifizierung.

Chrome Browser Extension for VMware Cloud Director unterstützt Multisite-Umgebungen.

Sie können die Erweiterung zu Ihrem Chrome-Browser über den [Chrome Web Store](#) hinzufügen.

Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen

Bevor Sie auf die Benutzeroberfläche einer vSphere-Proxy-Komponente zugreifen können, müssen Sie die Proxys einrichten, die in Ihrer Organisation veröffentlicht werden.

Um Ihren Browser für die Verwendung Ihrer veröffentlichten Proxys zu konfigurieren, kopieren Sie die URL der PAC-Datei (proxy auto-config) in Ihren Browser.

Hinweis Wenn der **Systemadministrator** ein dediziertes vSphere-Datencenter für Ihre Organisation veröffentlicht oder einem Ihrer dedizierten vSphere-Datencenter einen Proxy hinzufügt, dauert es möglicherweise einige Minuten, bis der Browser die PAC von der angegebenen URL erneut abrufen. Um eine Aktualisierung des Browsers zu erzwingen, können Sie diesen Vorgang wiederholen.

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 VMware Cloud Director Tenant Portal.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Datencenter** und dann auf **Virtuelles Datencenter**.
- 2 Klicken Sie im Bereich **Dedizierte vSphere-Datencenter** auf **Klicken Sie hier, um das Proxy-Konfigurationshandbuch anzuzeigen**.
- 3 Kopieren Sie die PAC-URL und klicken Sie auf **Weiter**.
- 4 Folgen Sie den Anweisungen, um Ihren Browser so zu konfigurieren, dass er auf die PAC-URL verweist.
- 5 Wenn eine Proxy-Komponente selbstsignierte Zertifikate verwendet, importieren Sie die Zertifikate in Ihren Browser.
 - a Klicken Sie auf der Ziel-vSphere-Datencenter-Karte auf **Aktionen** und dann auf **Zertifikat importieren**.
 - b Laden Sie das Zertifikat und die Zertifikatswiderrufsliste (CRL) herunter.
 - c Importieren Sie das heruntergeladene Zertifikat in Ihren Browser.

Weitere Informationen finden Sie im Benutzerhandbuch Ihres Browsers.

Anmelden bei der Benutzeroberfläche einer Komponente mithilfe eines Endpoints

Sie können Endpoints verwenden, um mit Ihrem VMware Cloud Director-Konto auf die Benutzeroberfläche von Komponenten mit oder ohne Proxy zuzugreifen.

Voraussetzungen

Wenn Sie auf eine Komponente mit Proxy zugreifen möchten, [Konfigurieren des Browsers mit den gewünschten Proxy-Einstellungen](#) oder [Verwenden von Chrome Browser Extension for VMware Cloud Director](#) in Google Chrome hinzu.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Datencenter** und dann auf **Virtuelles Datencenter**.
- 2 Wählen Sie die Registerkarte **Dedizierte vSphere-Datencenter** aus.
- 3 Öffnen Sie den Endpoint der dedizierten vCenter Server-Instanz.
 - Zum Öffnen des Standard-Endpoints klicken Sie auf **vSphere öffnen**.
 - Zum Öffnen eines nicht standardmäßigen Endpoints führen Sie die folgenden Schritte aus:
 - Klicken Sie auf das Menü **Aktionen**, dann auf **Endpoints anzeigen**.
 - Klicken Sie auf die Endpoint-URL.

Wenn Sie auf eine Komponente mit Proxy zugreifen, wird eine neue Karte mit Ihren Proxy-Anmeldedaten geöffnet.

- 4 Wenn Sie sich bei einer Komponente mit Proxy anmelden, greifen Sie mithilfe Ihrer Anmeldedaten auf die Komponente zu.

- a Kopieren Sie den Benutzernamen und das Kennwort.

- b Um den Proxy zu aktivieren, klicken Sie auf **Öffnen**.

Eine neue Karte wird geöffnet und fordert Sie zur Authentifizierung anhand des Proxys auf.

- c Fügen Sie im Textfeld **Benutzername** den kopierten Benutzernamen ein.

- d Fügen Sie im Textfeld **Kennwort** das kopierte Kennwort ein und klicken Sie auf **OK**.

Arbeiten mit vApp-Vorlagen

9

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](#)
- [Importieren einer virtuellen Maschine aus vCenter Server als vApp-Vorlage](#)
- [Zuweisen einer VM-Platzierungsrichtlinie und einer VM-Größenrichtlinie zu einer vApp-Vorlage](#)
- [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 [Freigeben eines Katalogs](#).


Voraussetzungen

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


Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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.

VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **vApp-Vorlagen** aus.

Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf **Neu**.

- 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.

Importieren einer virtuellen Maschine aus vCenter Server als vApp-Vorlage

Wenn Sie **Systemadministrator**-Rechte haben, können Sie vCenter Server-VMs in VMware Cloud Director als vApp-Vorlagen in Katalogen importieren.

Voraussetzungen

Um VMs aus vCenter Server als vApp-Vorlagen anzuzeigen und zu importieren, stellen Sie sicher, dass Sie über **Systemadministrator**-Rechte verfügen.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **vApp-Vorlagen** aus.
Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf **Von vCenter importieren**.
- 3 Wählen Sie im Dropdown-Menü die vCenter Server-Instanz aus, aus der Sie eine vApp-Vorlage importieren möchten.
- 4 Wählen Sie aus der Liste der virtuellen Maschinen eine Vorlage aus.
- 5 Geben Sie einen Namen und optional eine Beschreibung für die vApp-Vorlage ein.

- 6 Wählen Sie im Dropdown-Menü einen Katalog aus, dem die vApp-Vorlage hinzugefügt werden soll.
- 7 (Optional) Um die virtuelle Quellmaschine zu deaktivieren, aktivieren Sie die Option **Virtuelle Maschine verschieben**.
- 8 (Optional) Markieren Sie die vApp-Vorlage als bevorzugte Vorlage im Katalog.
- 9 Klicken Sie auf **Importieren**.

Zuweisen einer VM-Platzierungsrichtlinie und einer VM-Größenrichtlinie zu einer vApp-Vorlage

Um die VMs einer vApp-Vorlage mit bestimmten VM-Platzierungs- und VM-Größenrichtlinien zu verknüpfen, können Sie einzelne VMs einer vApp-Vorlage mit den Richtlinien kennzeichnen, die Sie zuweisen möchten.

Ab VMware Cloud Director 10.0 können Sie zulassen, dass Benutzer die vordefinierten VM-Platzierungs- oder VM-Größenrichtlinien beim Bearbeiten einer VM ändern.

Hinweis Nach dem Upgrade auf VMware Cloud Director 10.0 oder höher werden alle Taggings bereits vorhandener Vorlagen änderbar. Wenn Sie die Änderungen an den vordefinierten VM-Platzierungs- oder VM-Größenrichtlinien nicht zulassen möchten, müssen Sie das Kontrollkästchen **Änderbar** für die Richtlinien, die nicht änderbar sein sollen, deaktivieren.

Voraussetzungen

- Für diesen Vorgang ist das Recht zum Bearbeiten einer vApp-Vorlage erforderlich.
- Vergewissern Sie sich, dass mindestens eine vApp-Vorlage in Ihrer VMware Cloud Director-Umgebung vorhanden ist.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **vApp-Vorlagen** aus.
Die Liste der Vorlagen wird in einer Rasteransicht angezeigt.
- 2 Aktivieren Sie das Optionsfeld neben der vApp-Vorlage, die Sie kennzeichnen möchten, und klicken Sie auf **Mit Computing-Richtlinien kennzeichnen**.
- 3 Wenn Sie einer VM in der vApp-Vorlage eine VM-Platzierungsrichtlinie zuweisen möchten, wählen Sie eine Richtlinie aus dem Dropdown-Menü **VM-Platzierungsrichtlinie** in der Zeile aus, die der VM entspricht.
- 4 Wenn Sie einer VM in der vApp-Vorlage eine VM-Größenrichtlinie zuweisen möchten, wählen Sie eine Richtlinie aus dem Dropdown-Menü **VM-Größenrichtlinie** in der Zeile aus, die der VM entspricht.

- 5 (Optional) Damit die Benutzer die vordefinierten VM-Platzierungs- oder VM-Größenrichtlinien beim Bearbeiten einer VM ändern können, aktivieren Sie das Kontrollkästchen **Änderbar** unter dem Dropdown-Menü für die Richtlinie.
- 6 Klicken Sie auf **Tag**.

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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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](#).

Arbeiten mit Katalogen

11

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 VMware Cloud Director-Installation freigegeben oder extern veröffentlicht werden, um den Zugriff für Organisationen außerhalb der VMware Cloud Director-Installation zu ermöglichen.

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director-Installation zugreifen können. Eine Organisation außerhalb der VMware Cloud 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](#)

- [Ändern des Besitzers 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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.

Ändern des Besitzers eines Katalogs

Ein **Organisationsadministrator** kann den Besitzer eines Katalogs ändern.

Bevor Sie einen Benutzer löschen können, der Besitzer eines Katalogs ist, müssen Sie zuerst den Besitzer ändern oder den Katalog löschen.


Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **Kataloge** aus.

Die Liste der Kataloge wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf die Listenleiste () links neben einem Katalog und wählen Sie **Besitzer ändern** aus.

Die Liste der Benutzer, die auf den Katalog zugreifen können, wird in der Rasteransicht des Fensters **Besitzer ändern** angezeigt.

- 3 Wählen Sie den Benutzer aus, den Sie zum neuen Besitzer des Katalogs machen möchten, und klicken Sie auf **OK**.

Ergebnisse

Auf der Registerkarte **Kataloge** ändert sich der Name des Katalogbesitzers in der Rasteransicht.


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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Metadatennamen, 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 Metadatennamen 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **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

12

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.

Wenn Ihrer Organisation der Zugriff auf Vorlagen für virtuelle Datacenter bereitgestellt wurde, können Sie über das VMware Cloud Director Tenant Portal anhand der verfügbaren Vorlagen virtuelle Datacenter erstellen.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen verfügbarer Vorlagen für virtuelle Datacenter](#)
- [Instanzieren eines virtuellen Datacenters anhand 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

- ◆ Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **Organisations-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.

Instanzieren eines virtuellen Datacenters anhand einer Vorlage

Wenn ein Systemadministrator eine Vorlage für Organisations-VDCs (Virtual Data Center) erstellt und die Vorlage in Ihrer Organisation veröffentlicht, können Sie ein Organisations-VDC anhand der Vorlage erstellen.

Voraussetzungen

Für diesen Vorgang sind die Rechte erforderlich, die in der vordefinierten Rolle namens **Organisationsadministrator** oder einer Rolle mit Rechten zum Anzeigen und Instanzieren von Vorlagen für Organisations-VDCs enthalten sind.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie im linken Bereich **Organisations-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**.

Ab VMware Cloud Director 10.2.2 müssen Sie nach Auswahl einer Vorlage auf **VDC instanzieren** klicken.

- 3 Geben Sie einen Namen für das VDC und optional eine Beschreibung 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

13

Sie können Organisationsadministratoren einzeln oder als Teil einer LDAP-Gruppe zu VMware Cloud 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 VMware Cloud Director-Organisation erstellen.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
Die Liste der Benutzer wird angezeigt.
- 3 Klicken Sie auf **Neu**.
- 4 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 Wenn Sie eine bestimmte Beschränkung für die Ressourcen festlegen möchten, die dem Benutzer zur Verfügung stehen, aktivieren Sie die Umschaltfläche **Benutzerkontingent konfigurieren**.

Wenn Sie die Umschaltfläche beim Abschließen des Assistenten aktivieren, werden Sie von VMware Cloud Director an die Seite **Kontingente** umgeleitet. Sie können Kontingente für die Anzahl der Tanzu Kubernetes-Cluster, für alle oder für vom Benutzer verwaltete ausgeführte VMs, für verbrauchte CPU, Arbeitsspeicher und Speicher hinzufügen. Wählen Sie **Unbegrenzt** aus, wenn der Benutzer über unbegrenzte Ressourcen des ausgewählten Typs verfügen soll.

- 7 Wählen Sie die Rolle aus, die Sie dem Benutzer zuweisen möchten.

Das Menü **Verfügbare Rollen** besteht aus einer Liste vordefinierter Rollen und aller benutzerdefinierter 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 der 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 VMware Cloud Director-Mandantenportal oder Cloud Director OpenAPI verwenden, um Benutzer und Gruppen in seiner Organisation zu verwalten und ihnen Rollen zuzuweisen, einschließlich der vordefinierten Rolle Organisationsadministrator . Ein Organisationsadministrator kann Cloud Director OpenAPI zum Erstellen oder Aktualisieren der für die Organisation lokalen Rollenobjekte verwenden. Von einem Organisationsadministrator erstellte oder geänderte Rollen sind für andere Organisationen nicht sichtbar.

Vordefinierte Rolle	Beschreibung
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.

- 8 (Optional) Geben Sie die Kontaktinformationen wie Name, E-Mail-Adresse, Telefonnummer und Instant Messaging-ID ein.
- 9 Klicken Sie auf **Speichern**.

Nächste Schritte

Wenn Sie Kontingentkonfiguration für den Benutzer aktiviert haben und von VMware Cloud Director an die Seite **Kontingente** umgeleitet werden, finden Sie weitere Informationen unter [Verwalten der Ressourcenkontingente eines Benutzers](#).

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 [Aktivieren der Verwendung eines SAML-Identitätsanbieter für die Organisation](#).

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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

1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.

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 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 VMware Cloud Director anmeldet. Zum Löschen eines Benutzers müssen Sie zuerst sein Konto deaktivieren.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 Ihre Auswahl.
- 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 VMware Cloud 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 zu löschende Konto.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.

- 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 der Ressourcenkontingente eines Benutzers

Sie können den Grenzwert für den gesamten Ressourcenverbrauch eines Benutzers verwalten. Sie können die Kontingente des Benutzers für VMs, Tanzu Kubernetes-Cluster, CPU, Arbeitsspeicher oder Speicher hinzufügen, bearbeiten und entfernen.

Die Benutzer können nur die Kontingente anzeigen, die für ihren Benutzertyp relevant sind. Benutzer erben Kontingente der Gruppe, der sie angehören. Wenn ein Benutzer ein Ressourcenkontingent der zugehörigen Gruppe erbt und über ein explizites für diese Ressource definiertes Kontingent auf Benutzerebene verfügt, hat das Kontingent auf Benutzerebene Vorrang vor dem Kontingent auf Gruppenebene.

Weitere Informationen zum Erstellen oder Importieren von Benutzern finden Sie unter [Erstellen eines Benutzers](#) oder [Benutzer importieren](#).

Voraussetzungen

Stellen Sie sicher, dass Sie über die notwendigen Berechtigungen zum Hinzufügen, Bearbeiten und Löschen von Ressourcenkontingenten verfügen. Standardmäßig können **Organisationsadministratoren** die Benutzerkontingente ändern.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Benutzer**.
- 3 Wählen Sie den Namen eines Benutzers und dann die Registerkarte **Kontingente** aus.

Benutzer weisen standardmäßig keine Kontingente auf. Alle Benutzer, die zu einer Gruppe gehören, erben die Kontingente der Gruppe. Wenn der Benutzer zu einer Gruppe gehört, die über ein Kontingent für Ressourcen verfügt, wird das Kontingent in der Liste der Kontingente des Benutzers als nicht änderbar angezeigt.

- 4 Klicken Sie auf **Bearbeiten**.
- 5 Ändern Sie das Kontingent für den ausgewählten Benutzer.

Sie können Kontingente für die Anzahl der Tanzu Kubernetes-Cluster, für alle oder für vom Benutzer verwaltete ausgeführte VMs, für verbrauchte CPU, Arbeitsspeicher und Speicher hinzufügen, bearbeiten oder entfernen. Wählen Sie **Unbegrenzt** aus, wenn der Benutzer über unbegrenzte Ressourcen des ausgewählten Typs verfügen soll.

- 6 Klicken Sie auf **Speichern**.

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 [Aktivieren der Verwendung eines SAML-Identitätsanbieters für die Organisation](#).

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Gruppen**.
Die Liste der Benutzergruppen wird angezeigt.
- 3 Klicken Sie auf **Gruppe importieren**.

- Wählen Sie eine Quelle aus, aus der Sie die Benutzergruppe importieren möchten.

Sie können nur den quellseitigen LDAP-Server oder SAML-Server anzeigen, den Sie als Identitätsanbieter konfiguriert haben.

Quelle	Aktion
LDAP	<p>Importieren Sie eine Benutzergruppe 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 Benutzergruppen aus, die Sie importieren möchten, und klicken Sie auf Hinzufügen.
SAML	<p>Importieren Sie Benutzergruppen von einem SAML-Server. Geben Sie die Namen der Gruppen ein, die Sie importieren möchten.</p> <p>Verwenden Sie für jeden Gruppennamen eine neue Zeile.</p>

- Wählen Sie die Rolle aus, die Sie der zu importierenden Gruppe von Benutzern zuweisen möchten.
- Klicken Sie auf **Speichern**.

Nächste Schritte

Wenn Sie Kontingentkonfiguration für die Gruppe aktiviert haben und von VMware Cloud Director an die Seite **Kontingente** umgeleitet werden, finden Sie weitere Informationen unter [Verwalten der Ressourcenkontingente einer Gruppe](#).

Löschen einer Gruppe

Sie können eine Gruppe aus der VMware Cloud Director-Organisation entfernen, indem Sie die entsprechende LDAP-Gruppe löschen.

Wenn Sie eine LDAP-Gruppe löschen, werden Benutzer, deren VMware Cloud 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

- Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Gruppen**.
Die Liste der Benutzergruppen wird angezeigt.
- Klicken Sie auf das Optionsfeld neben dem Namen der zu löschenden Gruppe und anschließend auf **Löschen**.
- Um zu bestätigen, dass Sie die Gruppe löschen möchten, klicken Sie auf **OK**.

Bearbeiten einer Gruppe

Sie können eine Gruppe im VMware Cloud Director-Mandantenportal bearbeiten.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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**.

Verwalten der Ressourcenkontingente einer Gruppe

Indem Sie das Kontingent für eine Gruppe direkt festlegen, können Sie den Grenzwert des gesamten Ressourcenverbrauchs für jeden Benutzer in der Gruppe verwalten. Sie können die Kontingente der Gruppe für VMs, Tanzu Kubernetes-Cluster, CPU, Arbeitsspeicher oder Speicher hinzufügen, bearbeiten und entfernen. Die Kontingente der Gruppe werden auf jedes Mitglied der Gruppe angewendet.

Benutzer erben Kontingente der Gruppe, der sie angehören. Wenn ein Benutzer ein Ressourcenkontingent der zugehörigen Gruppe erbt und über ein explizites für diese Ressource definiertes Kontingent auf Benutzerebene verfügt, hat das Kontingent auf Benutzerebene Vorrang vor dem Kontingent auf Gruppenebene.

Informationen zum Importieren von Gruppen finden Sie unter [Importieren einer Gruppe](#).

Voraussetzungen

Stellen Sie sicher, dass Sie über die notwendigen Berechtigungen zum Hinzufügen, Bearbeiten und Löschen von Ressourcenkontingenten verfügen. Standardmäßig können **Organisationsadministratoren** die Gruppenkontingente ändern.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung** auf **Gruppen**.

- 3 Wählen Sie den Namen einer Gruppe und dann die Registerkarte **Kontingente** aus.

Gruppen weisen standardmäßig keine Kontingente auf. Alle Benutzer, die zu einer Gruppe gehören, erben die Kontingente der Gruppe. Wenn der Benutzer zu einer Gruppe gehört, die über ein Kontingent für Ressourcen verfügt, wird das Kontingent in der Liste der Kontingente des Benutzers als nicht änderbar angezeigt.

- 4 Klicken Sie auf **Bearbeiten**.
- 5 Ändern Sie das Kontingent für die ausgewählte Gruppe.

Sie können Kontingente für die Anzahl der Tanzu Kubernetes-Cluster, für alle oder für von der Gruppe verwaltete ausgeführte VMs, für verbrauchte CPU, Arbeitsspeicher und Speicher hinzufügen, bearbeiten oder entfernen. Wählen Sie **Unbegrenzt** aus, wenn die Benutzergruppe über unbegrenzte Ressourcen des ausgewählten Typs verfügen soll.

- 6 Klicken Sie auf **Speichern**.

Rollen und Rechte

VMware Cloud Director verwendet Rollen und Rechte, um zu bestimmen, welche Aktionen Benutzer in einer Organisation durchführen dürfen. In VMware Cloud 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 VMware Cloud 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 VMware Cloud Director-Rolle enthält einen Standardsatz an Rechten, die erforderlich sind, um in gemeinsamen Workflows enthaltene Vorgänge auszuführen. Standardmäßig werden alle globalen vordefinierten Mandantenrollen für jeder 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. Eine Liste der Rechte, die nur für die Rolle **Systemadministrator** verfügbar sind, finden Sie unter *VMware Cloud Director Service Provider Admin Portal-Handbuch*. 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 Cloud Director OpenAPI-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 Benutzer und Gruppen in seiner Organisation verwalten und ihnen Rollen zuweisen, 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 ein OAuth-Identitätsanbieter den Benutzer definiert, werden dem Benutzer die im Array `roles` des benutzereigenen OAuth-Tokens angegebenen Rollen zugewiesen.
- Wenn ein SAML-Identitätsanbieter den Benutzer definiert, werden dem Benutzer 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. Eine Liste der Rechte in vordefinierten Mandantenrollen finden Sie unter [Rechte in vordefinierten globalen Mandantenrollen](#).

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.

In den globalen Mandantenrollen in VMware Cloud Director enthaltene Rechte

Neuheiten in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	Auf alle Organisations-VDCs zugreifen	✓				
	Katalog: vApp von „Meine Cloud“ hinzufügen	✓	✓	✓		
	Katalog: Besitzer ändern	✓				
	Katalog: CLSP-Veröffentlichung abonnieren	✓	✓			
	Katalog: Katalog erstellen/löschen	✓	✓			
	Katalog: Eigenschaften bearbeiten	✓	✓			
	Katalog: Veröffentlichen	✓	✓			
	Katalog: Gemeinsame Nutzung	✓	✓			
	Katalog: ACL anzeigen	✓	✓			
	Katalog: Private und freigegebene Kataloge anzeigen	✓	✓	✓		
	Katalog: Veröffentlichte Kataloge anzeigen	✓				
	Benutzerdefinierte Entität: Alle benutzerdefinierten Entitätsinstanzen in der Organisation anzeigen	✓				
	Benutzerdefinierte Entität: Benutzerdefinierte Entitätsinstanz anzeigen	✓				
	Datenträger: Besitzer ändern	✓	✓			
	Laufwerk: Erstellen	✓	✓	✓		
	Laufwerk: Löschen	✓	✓	✓		
	Laufwerk: Eigenschaften bearbeiten	✓	✓	✓		
	Datenträger: Verschlüsselungsstatus anzeigen	✓		✓		

Neuheiten in dieser Version	Name des Rechts	Organisation sadministrator	Katalogau- tor	vApp- Autor	vApp- Benutzer	Nur Konsolenz- zugriff
	Laufwerk: Eigenschaften anzeigen	✓	✓	✓	✓	
	Allgemein: Administratorsteuerung	✓				
	Allgemein: Administratoransicht	✓				
	Allgemein: Benachrichtigung senden	✓				
	Gruppe/Benutzer: Ansicht	✓				
	Hybrid Cloud-Betrieb: Ticket zur Steuerung abrufen	✓				
	Hybrid Cloud-Betrieb: Ticket für Aus-der-Cloud-Tunnel abrufen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel-Ticket abrufen	✓				
	Hybrid Cloud-Betrieb: Aus-der-Cloud-Tunnel erstellen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel erstellen	✓				
	Hybrid Cloud-Betrieb: Aus-der-Cloud-Tunnel löschen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel löschen	✓				
	Hybrid Cloud-Betrieb: Endpunkt-Tag des Aus-der-Cloud-Tunnels aktualisieren	✓				
	Hybrid Cloud-Betrieb: Aus-der-Cloud-Tunnel anzeigen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel anzeigen	✓				
	Organisationsnetzwerk: Eigenschaften bearbeiten	✓				
	Organisationsnetzwerk: Ansicht	✓				
	Organisations-vDC-Computing-Richtlinie: Ansicht	✓	✓	✓	✓	
	Distributed Firewall für Organisations-vDC: Regeln konfigurieren	✓				
	Distributed Firewall für Organisations-vDC: Regeln anzeigen	✓				

Neuheiten in dieser Version	Name des Rechts	Organisation sadministrator	Katalogau- tor	vApp- Autor	vApp- Benutzer	Nur Konsolenz- zugriff
	Organisations-vDC-Gateway: DHCP konfigurieren	✓				
	Organisations-vDC-Gateway: DNS konfigurieren	✓				
	Organisations-vDC-Gateway: ECMP-Routing konfigurieren	✓				
	Organisations-vDC-Gateway: Firewall konfigurieren	✓				
	Organisations-vDC-Gateway: IPSec-VPN konfigurieren	✓				
	Organisations-vDC-Gateway: Lastausgleichsdienst konfigurieren	✓				
	Organisations-vDC-Gateway: NAT konfigurieren	✓				
	Organisations-vDC-Gateway: Statisches Routing konfigurieren	✓				
	Organisations-vDC-Gateway: Syslog konfigurieren	✓				
	Organisations-vDC-Gateway: In erweitertes Netzwerk konvertieren	✓				
	Organisations-vDC-Gateway: Ansicht	✓				
	Organisations-vDC-Gateway: DHCP anzeigen	✓				
	Organisations-vDC-Gateway: DNS anzeigen	✓				
	Organisations-vDC-Gateway: Firewall anzeigen	✓				
	Organisations-vDC-Gateway: IPSec-VPN anzeigen	✓				
	Organisations-vDC-Gateway: Lastausgleichsdienst anzeigen	✓				
	Organisations-vDC-Gateway: NAT anzeigen	✓				
	Organisations-vDC-Gateway: Statisches Routing anzeigen	✓				
	vDC-Organisationsnetzwerk: Eigenschaften bearbeiten	✓				

Neuheiten in dieser Version	Name des Rechts	Organisation administrator	Katalogau- tor	vApp- Autor	vApp- Benutzer	Nur Konsolenzugriff
	vDC-Organisationsnetzwerk: Eigenschaften anzeigen	✓		✓		
	Organisations-vDC- Speicherrichtlinie: Funktionen anzeigen	✓				
	Organisations-vDC- Speicherprofil: Standardwert festlegen	✓				
	Organisations-vDC: Bearbeiten	✓				
	Organisations-vDC: ACL bearbeiten	✓				
	Organisation-vDC: Firewall verwalten	✓				
	Organisations-vDC: Ansicht	✓	✓			
	Organisations-vDC: ACL anzeigen	✓				
	Organisations-VDC: Metriken anzeigen	✓				
	Organisations-vDC: VM-VM- Affinität bearbeiten	✓	✓	✓		
	Organisation: Zuordnungseinstellungen bearbeiten	✓				
	Organisation: Verbundeinstellungen bearbeiten	✓				
	Organisation: LDAP- Einstellungen bearbeiten	✓				
	Organisation: Lease-Richtlinie bearbeiten	✓				
	Organisation: OAuth- Einstellungen bearbeiten	✓				
	Organisation: Kennwortrichtlinie bearbeiten	✓				
	Organisation: Eigenschaften bearbeiten	✓				
	Organisation: Kontingent- Richtlinie bearbeiten	✓				
	Organisation: SMTP- Einstellungen bearbeiten	✓				

Neuheiten in dieser Version	Name des Rechts	Organisation administrator	Katalogau- tor	vApp- Autor	vApp- Benutzer	Nur Konsolenzugriff
	Organisation: Benutzer/Gruppe beim Bearbeiten der VDC-ACL aus Identitätsanbieter importieren	✓				
	Organisation: Ansicht	✓	✓	✓		
	Organisation: Metriken anzeigen	✓				
✓	Kontingentrichtlinienfunktionen: Ansicht	✓				
	Rolle: Erstellen, bearbeiten, löschen oder kopieren	✓				
	Dienstbibliothek: Dienstbibliotheken anzeigen	✓				
	UI-Plug-Ins: Ansicht	✓	✓	✓	✓	
	vApp-Vorlage/Medien: Kopieren	✓	✓	✓		
	vApp-Vorlage/Medien: Erstellen/hochladen	✓	✓			
	vApp-Vorlage/Medien: Bearbeiten	✓	✓	✓		
	vApp-Vorlage oder Medien: Ansicht	✓	✓	✓	✓	
	vApp-Vorlage: Besitzer ändern	✓	✓			
	vApp-Vorlage: Auschecken	✓	✓	✓	✓	
	vApp-Vorlage: Herunterladen	✓	✓			
	vApp: Besitzer ändern	✓				
	vApp: Kopieren	✓	✓	✓	✓	
	vApp: Erstellen/neu konfigurieren	✓	✓	✓		
	vApp: Löschen	✓	✓	✓	✓	
	vApp: Herunterladen	✓	✓	✓		
	vApp: Eigenschaften bearbeiten	✓	✓	✓	✓	
	vApp: VM-Computing-Richtlinie bearbeiten	✓	✓	✓		
	vApp: CPU der VM bearbeiten	✓	✓	✓		
	vApp: Festplatte der VM bearbeiten	✓	✓	✓		

Neuheiten in dieser Version	Name des Rechts	Organisation administrator	Katalogau- tor	vApp- Autor	vApp- Benutzer	Nur Konsolen- zugriff
	vApp: Arbeitsspeicher der VM bearbeiten	✓	✓	✓		
	vApp: VM-Netzwerk bearbeiten	✓	✓	✓	✓	
	vApp: VM-Eigenschaften bearbeiten	✓	✓	✓	✓	
	vApp: VM-Kennwordeinstellungen verwalten	✓	✓	✓	✓	✓
	vApp: Energievorgänge	✓	✓	✓	✓	
	vApp: Gemeinsame Nutzung	✓	✓	✓	✓	
	vApp: Snapshot-Vorgänge	✓	✓	✓	✓	
	vApp: Hochladen	✓	✓	✓		
	vApp: Konsole verwenden	✓	✓	✓	✓	✓
	vApp: ACL anzeigen	✓	✓	✓	✓	
	vApp: VM und Festplatten-Verschlüsselungsstatus der VM anzeigen	✓		✓		
	vApp: VM-Metriken anzeigen	✓		✓	✓	
	vApp: VM-Startoptionen	✓	✓	✓		
	vApp: VM-Metadaten zu vCenter	✓	✓	✓		
✓	VDC-Gruppe: Konfigurieren	✓				
✓	VDC-Gruppe: Ansicht	✓				
✓	VDC-Gruppe: Protokollierung konfigurieren	✓				
	VDC-Vorlage: Instantiieren	✓				
	VDC-Vorlage: Ansicht	✓				

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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 VMware Cloud Director-Erweiterungen steuern.
Infrastruktur	Rechte, die den Zugriff auf und die Verwaltung der Infrastrukturobjekte steuern, wie z. B. Datenspeicher, Festplatten, Hosts usw.
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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.

- 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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.

Konfigurieren von Identitätsanbietern

14

Sie können Ihre Cloud mit einem externen Identitätsanbieter integrieren und Benutzer und Gruppen in Ihre Organisation importieren.

Sie haben die Möglichkeit, Ihre Organisation für die Verwendung eines SAML-Identitätsanbieters zu aktivieren oder eine LDAP-Serververbindung zu konfigurieren.

Dieses Kapitel enthält die folgenden Themen:

- [Aktivieren der Verwendung eines SAML-Identitätsanbieter für die Organisation](#)
- [Bearbeiten von LDAP-Einstellungen für Ihre Organisation](#)
- [Konfigurieren, Testen und Synchronisieren einer LDAP-Verbindung](#)

Aktivieren der Verwendung eines SAML-Identitätsanbieter für die Organisation

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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 angeben 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 VMware Cloud Director-Metadaten. Weitere Informationen finden Sie in der Dokumentation Ihres SAML-Identitätsanbieters und im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.
- Importieren Sie Benutzer und Gruppen von Ihrem SAML-Identitätsanbieter. Weitere Informationen finden Sie unter [Kapitel 13 Verwalten von Benutzern, Gruppen und Rollen](#)

Bearbeiten von LDAP-Einstellungen für Ihre Organisation

Sie können Ihre Organisation so konfigurieren, dass die System-LDAP-Verbindung als gemeinsam genutzte Quelle für Benutzer und Gruppen verwendet wird. Zudem können Sie Ihre Organisation so konfigurieren, dass eine separate LDAP-Verbindung als private Quelle für Benutzer und Gruppen verwendet wird.

Voraussetzungen

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

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 2 Klicken Sie im linken Bereich unter **Identitätsanbieter**, auf **LDAP**.

Die aktuellen LDAP-Einstellungen werden angezeigt.

- 3 Klicken Sie auf der Registerkarte **LDAP-Einstellungen** auf **Bearbeiten**.
- 4 Konfigurieren Sie die LDAP-Quelle für Benutzer und Gruppen für Ihre Organisation und klicken Sie auf **Speichern**.

Option	Beschreibung
LDAP nicht verwenden	Die Organisation verwendet keinen LDAP-Server als Quelle für Organisationsbenutzer und -gruppen.
System-LDAP-Dienst von VMware Cloud Director	Die Organisation verwendet die von Ihrem Dienstanbieter konfigurierte VMware Cloud Director-System-LDAP-Verbindung. Geben Sie den Distinguished Name für die Organisationseinheit ein.
Benutzerdefinierter LDAP-Dienst	Die Organisation verwendet einen privaten LDAP-Server als Quelle für Organisationsbenutzer und -gruppen.

Nächste Schritte

Wenn Sie **Benutzerdefinierter LDAP-Dienst** ausgewählt haben, klicken Sie auf die Registerkarte **Benutzerdefiniertes LDAP**, um [Konfigurieren, Testen und Synchronisieren einer LDAP-Verbindung](#).

Konfigurieren, Testen und Synchronisieren einer LDAP-Verbindung

Wenn Sie eine LDAP-Verbindung konfigurieren möchten, legen Sie die Details des LDAP-Servers fest. Sie können die Verbindung testen, um sicherzustellen, dass Sie die korrekten Einstellungen eingegeben haben und die Benutzer- und Gruppenattribute korrekt zugeordnet sind. Sobald Sie über eine funktionierende LDAP-Verbindung verfügen, können Sie die Benutzer- und Gruppeninformationen jederzeit mit dem LDAP-Server synchronisieren.

Voraussetzungen

Wenn Sie eine Verbindung mit einem LDAP-Server über SSL (LDAPS) herstellen möchten, stellen Sie sicher, dass das Zertifikat Ihres LDAP-Servers mit der in Java 8 Update 181 eingeführten Endpoint-Identifikation konform ist. Der CN (Common Name, allgemeiner Name) oder der SAN (Subject Alternative Name, alternativer Antragstellername) des Zertifikats muss mit dem FQDN des LDAP-Servers übereinstimmen. Weitere Informationen finden Sie in den *Java 8-Versionsänderungen* unter <https://www.java.com>.

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

Verfahren

- 1 Geben Sie auf der Registerkarte **Verbindung** die erforderlichen Informationen für die LDAP-Verbindung ein.

Erforderliche Informationen	Beschreibung
Server	Der Hostname oder die IP-Adresse des LDAP-Servers.
Port	Die Nummer des Ports, den der LDAP-Server überwacht. Der Standardport für LDAP ist Port 389. Der Standardport für LDAPS ist Port 636.
Base Distinguished Name	Der Base Distinguished Name (DN) ist der Speicherort in dem LDAP-Verzeichnis, in dem VMware Cloud Director verbunden werden soll. Um die Verbindung auf Root-Ebene herzustellen, geben Sie nur die Domänenkomponenten ein, beispielsweise DC=beispiel,DC=com . Wenn Sie eine Verbindung mit einem Knoten in der Domänenbaumstruktur herstellen möchten, geben Sie den Distinguished Name für diesen Knoten ein, beispielsweise OU=ServiceDirector,DC=beispiel,DC=com . Wenn Sie die Verbindung unter Verwendung eines spezifischen Knotens in dem Verzeichnis herstellen, wird der Verzeichnissbereich, auf den VMware Cloud Director zugreifen kann, entsprechend eingeschränkt.
Connector-Typ	Der Typ Ihres LDAP-Servers. Kann Active Directory oder OpenLDAP sein.
SSL verwenden	Wenn es sich bei Ihrem Server um einen LDAPS-Server handelt, aktivieren Sie dieses Kontrollkästchen.
Alle Zertifikate akzeptieren	Wenn es sich bei Ihrem Server um einen LDAPS-Server handelt, aktivieren Sie dieses Kontrollkästchen oder laden Sie das LDAP-SSL-Zertifikat hoch.
Benutzerdefinierter Truststore	Wenn es sich bei Ihrem Server um einen LDAPS-Server handelt, klicken Sie entweder auf die Schaltfläche Hochladen und importieren Sie ein LDAP-SSL-Zertifikat oder wählen Sie Alle Zertifikate akzeptieren aus.
Authentifizierungsmethode	Die einfache Authentifizierung besteht darin, den DN und das Kennwort des Benutzers an den LDAP-Server zu senden. Wenn Sie LDAP verwenden, wird das LDAP-Kennwort als Klartext über das Netzwerk gesendet. Wenn Sie Kerberos verwenden möchten, müssen Sie die LDAP-Verbindung mithilfe der vCloud-API konfigurieren.
Benutzername	Geben Sie den vollständigen LDAP-DN (Distinguished Name) eines Dienstkontos mit Domänenadministratorrechten ein. VMware Cloud Director verwendet dieses Konto, um das LDAP-Verzeichnis abzufragen und Benutzerinformationen abzurufen. Wenn der LDAP-Server so konfiguriert ist, dass Lesezugriff auch ohne Angabe eines Benutzernamens möglich ist, können diese Textfelder frei gelassen werden.
Kennwort	Das Kennwort für das Dienstkonto, das eine Verbindung mit dem LDAP-Server herstellt. Wenn der LDAP-Server so konfiguriert ist, dass Lesezugriff auch ohne Angabe eines Benutzernamens möglich ist, können diese Textfelder frei gelassen werden.

- 2 Klicken Sie auf die Registerkarte **Benutzerattribute**, überprüfen Sie die Standardwerte für die Benutzerattribute und ändern Sie diese, falls in Ihrem LDAP-Verzeichnis ein anderes Schema verwendet wird.
- 3 Klicken Sie auf die Registerkarte **Gruppenattribute**, überprüfen Sie die Standardwerte für die Gruppenattribute und ändern Sie diese, falls in Ihrem LDAP-Verzeichnis ein anderes Schema verwendet wird.
- 4 Klicken Sie auf **Speichern**.
- 5 Wenn Sie das Kontrollkästchen **SSL verwenden** aktiviert haben und das Zertifikat des LDAPS-Servers noch nicht als vertrauenswürdig eingestuft wurde, bestätigen Sie im Fenster **Vertrauenswürdigkeitszertifikat**, dass Sie dem vom Server-Endpoint bereitgestellten Zertifikat vertrauen.
- 6 So testen Sie die LDAP-Verbindungseinstellungen und die LDAP-Attributzuordnungen:

- a Klicken Sie auf **Testen**.
- b Geben Sie das Kennwort des von Ihnen konfigurierten Benutzers des LDAP-Servers ein und klicken Sie auf **Testen**.

Wenn die Verbindung erfolgreich hergestellt wurde, wird ein grünes Häkchen angezeigt.

Die abgerufenen Benutzer- und Gruppenattributwerte werden in einer Tabelle angezeigt. Die Werte, die LDAP-Attributen erfolgreich zugeordnet wurden, werden mit grünen Häkchen markiert. Die Werte, bei denen es sich um keine zugeordneten LDAP-Attribute handelt, sind leer und werden mit roten Ausrufezeichen markiert.

- c Klicken Sie zum Beenden auf **Abbrechen**.

- 7 Um VMware Cloud Director mit dem konfigurierten LDAP-Server zu synchronisieren, klicken Sie auf **Synchronisieren**.

VMware Cloud Director synchronisiert die Benutzer- und Gruppeninformationen regelmäßig mit dem LDAP-Server. Wie häufig dies geschieht, hängt vom Synchronisierungsintervall ab, das Sie in den allgemeinen Systemeinstellungen festlegen.

Warten Sie einige Minuten, bis die Synchronisierung abgeschlossen ist.

Ergebnisse

Sie können Benutzer und Gruppen aus dem neu konfigurierten LDAP-Server importieren.

Sie können Zertifikate über VMware Cloud Director importieren, herunterladen, bearbeiten und löschen. Sie sind in der Lage, die Zertifikats-PEM-Daten in die Zwischenablage zu kopieren.

Dieses Kapitel enthält die folgenden Themen:

- [Importieren vertrauenswürdiger Zertifikate](#)
- [Importieren von Zertifikaten in die Zertifikatsbibliothek](#)

Importieren vertrauenswürdiger Zertifikate

Sie können Zertifikate von Servern importieren, mit denen VMware Cloud Director kommuniziert, wie z. B. vCenter Server, NSX Manager usw.

Bei Verwendung von VMware Cloud Director im FIPS-Modus müssen Sie FIPS-kompatible private Schlüssel verwenden. Sie können pyOpenSSL zum Erzeugen privater Schlüssel im FIPS-kompatiblen PKCS#8-Format verwenden. Wenn Sie private PKCS#8-Schlüssel mithilfe von OpenSSL erzeugen, sind die privaten Schlüssel nicht FIPS-kompatibel. Weitere Informationen zum FIPS-Modus finden Sie unter [Aktivieren des FIPS-Modus für die Zellen in der Servergruppe](#) oder [Aktivieren oder Deaktivieren des FIPS-Modus in der VMware Cloud Director-Appliance](#).

Voraussetzungen

Stellen Sie sicher, dass Sie sich als **Systemadministrator** oder **Organisationsadministrator** angemeldet haben.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Fensterbereich unter **Zertifikatsverwaltung** die Option **Vertrauenswürdige Zertifikate** aus und klicken Sie auf **Importieren**.
- 3 Laden Sie eine PEM-Datei mit den zu importierenden Zertifikaten hoch und klicken Sie auf **Importieren**.
- 4 (Optional) Bearbeiten Sie den Namen des Zertifikats.
- 5 Klicken Sie auf **Importieren**.

Nächste Schritte

- Laden Sie ein Zertifikat herunter.
- Bearbeiten Sie den Namen eines Zertifikats.
- Löschen Sie ein Zertifikat.
- Kopieren Sie die PEM-Daten in die Zwischenablage.

Importieren von Zertifikaten in die Zertifikatsbibliothek

In der VMware Cloud Director-Zertifikatsbibliothek können Sie Zertifikate importieren, die beim Erstellen von zu sichernden Elementen verwendet werden, wie z. B. Server, Edge-Gateways usw.

Die Zertifikatsbibliothek enthält Informationen zu einzelnen Zertifikaten, Zertifikatsketten, Privatschlüsseln, Ablaufdaten der Zertifikate sowie zu den von den Zertifikaten gesicherten Elementen usw.

Bei Verwendung von VMware Cloud Director im FIPS-Modus müssen Sie FIPS-kompatible selbstsignierte Zertifikate und private Schlüssel verwenden. Sie können selbstsignierte unverschlüsselte Zertifikate und private Schlüssel mithilfe von pyOpenSSL erzeugen. Wenn Sie selbstsignierte Zertifikate und private Schlüssel mithilfe von OpenSSL erzeugen, sind die Zertifikate und privaten Schlüssel nicht FIPS-kompatibel. Weitere Informationen zum FIPS-Modus finden Sie unter [Aktivieren des FIPS-Modus für die Zellen in der Servergruppe](#) oder [Aktivieren oder Deaktivieren des FIPS-Modus in der VMware Cloud Director-Appliance](#).

Voraussetzungen

Stellen Sie sicher, dass Sie sich als **Systemadministrator** oder **Organisationsadministrator** angemeldet haben.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Fensterbereich unter **Zertifikatsverwaltung** die Option **Zertifikatsbibliothek** aus und klicken Sie auf **Importieren**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für dieses Zertifikat in der Zertifikatsbibliothek ein und klicken Sie auf **Weiter**.
- 4 Laden Sie eine PEM-Datei mit der zu importierenden Zertifikatskette hoch und klicken Sie auf **Weiter**.
- 5 (Optional) Laden Sie eine private Schlüsseldatei hoch.
Die private Schlüsseldatei ist unter Umständen nicht durch eine Passphrase geschützt.
- 6 Klicken Sie auf **Importieren**.

Ergebnisse

Das importierte Zertifikat wird in der Liste der verfügbaren Zertifikate während der Erstellung von Elementen angezeigt, die gesichert werden müssen.

Nächste Schritte

- Laden Sie ein Zertifikat herunter.
- Bearbeiten Sie den Namen und die Beschreibung eines Zertifikats.
- Löschen Sie ein Zertifikat. Sie können nur Zertifikate löschen, die keine Elemente sichern.
- Kopieren Sie die PEM-Daten des Zertifikats in die Zwischenablage.

Als **Organisationsadministrator** können Sie verschiedene Einstellungen in Ihrer Organisation ändern. Sie können den Namen der Organisation, die E-Mail-Einstellungen, die Domäneneinstellungen, die Metadaten, die Richtlinien usw. ändern.

Sie können die VMware Cloud Director-API verwenden, um Meldungen zu Ereignissen und Aufgaben in Ihrer Organisation über das MQTT-Protokoll zu abonnieren. Informationen zum Abonnieren von Ereignissen und Aufgaben mithilfe eines MQTT-Clients finden Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

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 des Kennworts und der Richtlinien für Benutzerkonten in Ihrer Organisation](#)
- [Erstellen eines Dashboard für Sicherheitswarnungen](#)

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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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.

VMware Cloud 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 VMware Cloud Director kann ein Dienstanbieter oder Mandant mehrerer geografisch verteilter VMware Cloud Director-Installationen (Servergruppen) diese Installationen und die zugehörigen Organisationen als einzelne Entitäten verwalten und überwachen.

Das VMware Cloud Director-Mandantenportal bietet **Organisationsadministratoren** die Möglichkeit, Organisationen an zugehörigen Sites zuzuordnen.

Weitere Informationen zu Sitezuordnungen finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 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 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Administration**.

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**.

Erstellen eines Dashboard für Sicherheitswarnungen

Sie können Benachrichtigungen erstellen, die oben auf den Seiten der Benutzeroberfläche im Tenant Portal angezeigt werden. Die Meldungen können den Benutzern innerhalb einer Organisation oder den Benutzern in allen Organisationen angezeigt werden.

Sie können Sicherheitswarnungen nach deren Erstellung nicht mehr bearbeiten.

Voraussetzungen

Stellen Sie sicher, dass Sie sich als **Systemadministrator** angemeldet haben.

Verfahren

1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.

2 Wählen Sie im linken Fensterbereich unter **Einstellungen** die Option **Sicherheitswarnungen** aus und klicken Sie auf **Neu**.

3 Fügen Sie im Feld „Beschreibung“ den Text der Benachrichtigung hinzu.

Sie können Basismarkdown verwenden, um Links zu den Benachrichtigungen hinzuzufügen.

4 Wählen Sie die Priorität der Nachricht aus.

Die verschiedenen Prioritäten der Nachrichten werden in unterschiedlichen Farben dargestellt. Die Benachrichtigungen werden in der Reihenfolge ihrer Priorität angezeigt. Obligatorische Sicherheitswarnungen können weder verworfen noch in den Schlummermodus versetzt werden.

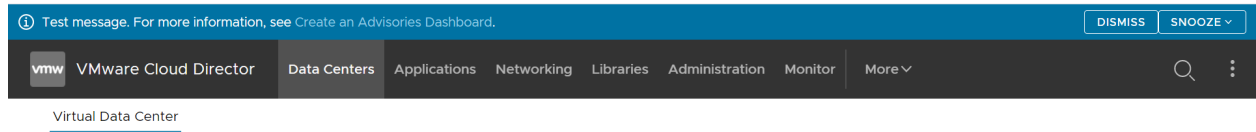
5 Wählen Sie den Zeitraum für die Anzeige der Benachrichtigung auf der Benutzeroberfläche aus.

Sie können alle Sicherheitswarnungen auf der Registerkarte **Sicherheitswarnungen** anzeigen. Diese werden der ausgewählten Benutzergruppe jedoch nur während des festgelegten Zeitraums angezeigt.

6 Klicken Sie auf **OK**.

Ergebnisse

Die Benachrichtigung wird über der oberen Navigationsleiste des ausgewählten Portals angezeigt.



Nächste Schritte

Löschen Sie die Benachrichtigung, indem Sie die Optionsschaltfläche neben der Benachrichtigung auswählen und auf **Löschen** klicken. Die Sicherheitswarnungen werden selbst nach deren Ablauf auf der Registerkarte **Sicherheitswarnungen** angezeigt. Um sie aus der Liste zu entfernen, müssen Sie sie löschen.

Bei den Elementen der Dienstbibliothek in VMware Cloud 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 VMware Cloud Director-Mandantenportal werden die vRealize Orchestrator-Workflows aufgelistet, die in VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Dienstbibliothek** aus.

Die Liste der Dienstelemente wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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 VMware Cloud Director ausführen.

Voraussetzungen

Dieser Vorgang erfordert, dass die Rechte unter „Dienstbibliothek“ in die vordefinierte Benutzerrolle aufgenommen werden.

Verfahren

- 1 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Dienstbibliothek** aus.

Die Liste der Dienstelemente wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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](#).

Ab VMware Cloud Director 10.2 können Dienstleister die VMware Cloud Director-API verwenden, um Erweiterungen zu erstellen, die den Mandanten zusätzliche VMware Cloud Director-Funktionen bieten. Wenn Ihnen ein Dienstleister Zugriff gewährt hat, können Sie definierte Entitäten verwalten und diese gemeinsam mit anderen Mandanten nutzen.

Dienstleister sind in der Lage, laufzeitdefinierte Entitäten (Runtime Defined Entities, RDEs) zu erstellen, wodurch Erweiterungen die erweiterungsspezifischen Informationen in VMware Cloud Director speichern und bearbeiten können. Beispielsweise kann eine Kubernetes-Erweiterung Informationen zu den Kubernetes-Clustern speichern, die sie in RDEs verwaltet. Die Erweiterung kann anschließend Erweiterungs-APIs für die Verwaltung dieser Cluster unter Verwendung der Informationen aus den RDEs bereitstellen.

Zugriff auf definierte Entitäten

Zwei ergänzende Mechanismen steuern den Zugriff auf RDEs.

- Rechte: Wenn ein Dienstleister einen RDE-Typ erstellt, so erstellt er ein Rechtspaket für den Typ. Ein Dienstleister muss Ihnen mindestens eines der fünf typspezifischen Rechte zuweisen: **Ansicht: TYPE**, **Bearbeiten: TYPE**, **Vollständige Kontrolle: TYPE**, **Administratoransicht: TYPE** und **Vollständige Kontrolle des Administrators: TYPE**.

Die Rechte **Ansicht: TYPE**, **Bearbeiten: TYPE** und **Vollständige Kontrolle: TYPE** funktionieren nur in Kombination mit einem ACL-Eintrag.

- Zugriffssteuerungsliste (ACL): Die ACL-Tabelle enthält Einträge, die den Zugriff der Benutzer auf bestimmte Entitäten im System definieren. Sie bietet eine zusätzliche Kontrollebene für die Entitäten. Beispiel: Das Recht **Bearbeiten: TYPE** gibt an, dass ein Benutzer Entitäten ändern kann, auf die er Zugriff hat, und die ACL-Tabelle legt fest, auf welche Entitäten der Benutzer Zugriff hat.

Tabelle 18-1. Rechte und ACL-Einträge für RDE-Vorgänge

Vorgang für Entität	Option	Beschreibung
Lesen	Recht Administratoransicht: TYPE	Benutzer mit diesem Recht können alle RDEs dieses Typs in einer Organisation sehen.
	Recht Ansicht: TYPE und ACL-Eintrag >= Ansicht	Benutzer mit diesem Recht und einer ACL auf Leseebene können RDEs dieses Typs anzeigen.
Ändern	Recht Vollständige Kontrolle des Administrators: TYPE	Benutzer mit diesem Recht können RDEs dieses Typs in allen Organisationen erstellen, anzeigen, ändern und löschen.
	Recht Bearbeiten: TYPE und ACL-Eintrag >= Ändern	Benutzer mit diesem Recht und ACL auf Änderungsebene können RDEs dieses Typs erstellen, anzeigen und ändern.
Löschen	Recht Vollständige Kontrolle des Administrators: TYPE	Benutzer mit diesem Recht können RDEs dieses Typs in allen Organisationen erstellen, anzeigen, ändern und löschen.
	Recht Vollständige Kontrolle: TYPE und ACL-Eintrag = Vollständige Kontrolle	Benutzer mit diesem Recht und Zugriffssteuerungsliste mit vollständiger Kontrolle können RDEs dieses Typs erstellen, anzeigen, ändern und löschen.

Freigeben definierter Entitäten für einen anderen Benutzer

Wenn ein **Systemadministrator** das Rechtspaket für einen definierten Entitätstyp veröffentlicht und Ihnen `ReadWrite`- oder `FullControl`-Zugriff gewährt hat bzw. Sie der Besitzer der definierten Entität sind, können Sie den Zugriff auf diese Entitäten für andere Benutzer freigeben.

- 1 Weisen Sie den Benutzerrollen, die die spezifische Zugriffsebene für die definierte Entität erhalten sollen, das Recht **Ansicht: TYPE**, **Bearbeiten: TYPE** oder **Vollständige Kontrolle: TYPE** aus dem Paket zu.

Hinweis Sie müssen als **Systemadministrator** oder **Organisationsadministrator** angemeldet sein, um Rechte zuzuweisen.

Sollen die Benutzer mit der Rolle **tkg_viewer** beispielsweise Tanzu Kubernetes-Cluster innerhalb der Organisation anzeigen können, müssen Sie der Rolle das Recht **Ansicht: Tanzu Kubernetes-Gastcluster** hinzufügen. Wenn Benutzer mit der Rolle **tkg_author** Tanzu Kubernetes-Cluster in dieser Organisation erstellen, anzeigen und ändern können sollen, fügen Sie dieser Rolle das Recht **Bearbeiten: Tanzu Kubernetes-Gastcluster** hinzu. Wenn Benutzer mit der Rolle **tkg_admin** Tanzu Kubernetes-Cluster in dieser Organisation erstellen, anzeigen, ändern und löschen können sollen, fügen Sie dieser Rolle das Recht **Vollständige Kontrolle: Tanzu Kubernetes-Gastcluster** hinzu.

2. Gewähren Sie dem jeweiligen Benutzer eine Zugriffssteuerungsliste (ACL), indem Sie den folgenden REST-API-Aufruf ausführen.

```
POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
[version]:[UUID]/accessControls
{
  "grantType" : "MembershipAccessControlGrant",
  "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
  "memberId" : "urn:vcloud:user:[User_ID]"
}
```

Access_level muss `ReadOnly`, `ReadWrite` oder `FullControl` sein. *User_ID* muss die ID des Benutzers sein, dem Sie den Zugriff auf die definierte Entität gewähren möchten.

Sie müssen über `ReadWrite`- oder `FullControl`-Zugriff auf eine Entität verfügen, um ACL-Zugriff auf diese Entität zu gewähren.

Benutzer mit der Rolle **tkg_viewer**, die im Beispiel beschrieben sind, können keinen ACL-Zugriff gewähren. Benutzer mit der Rolle **tkg_author** oder **tkg_admin** können den Zugriff auf eine VMWARE:TKGCLUSTER-Entität für Benutzer mit der Rolle **tkg_viewer**, **tkg_author** oder **tkg_admin** freigeben, indem Sie ihnen mit der API-Anforderung ACL-Zugriff gewähren.

Benutzer mit dem Recht **Vollständige Kontrolle des Administrators: Tanzu Kubernetes-Gastcluster** können ACL-Zugriff auf jede VMWARE:TKGCLUSTER-Entität gewähren.

Sie können auch REST-API-Aufrufe verwenden, um den Zugriff zu widerrufen oder anzuzeigen, wer Zugriff auf die Entität hat. Weitere Informationen finden Sie in der Dokumentation zur VMware Cloud Director-REST-API unter code.vmware.com.

Ändern des Besitzers einer definierten Entität

Der Besitzer einer definierten Entität oder ein Benutzer mit dem Recht **Vollständige Kontrolle des Administrators: TYPE** kann den Besitz auf einen anderen Benutzer übertragen, indem er das definierte Entitätsmodell aktualisiert und im Feld für den Besitzer die ID des neuen Besitzers angibt.

Dieses Kapitel enthält die folgenden Themen:

- [Arbeiten mit benutzerdefinierten Entitätsdefinitionen](#)

Arbeiten mit benutzerdefinierten Entitätsdefinitionen

Bei den benutzerdefinierten Entitätsdefinitionen in VMware Cloud Director handelt es sich um Objekttypen, die an vRealize Orchestrator-Objekttypen gebunden sind. Benutzer innerhalb einer VMware Cloud 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.

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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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-Objekttyp, 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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 Um eine neue benutzerdefinierte Entität hinzuzufügen, klicken Sie auf **Neu**.

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 Listenanzeige, um durch die verfügbaren nach Plug-Ins gruppierten vRealize Orchestrator-Objekttypen 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 VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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 Dienstanbieter, 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 Klicken Sie in der oberen Navigationsleiste auf **Bibliotheken** und wählen Sie unter **Dienste** die Option **Benutzerdefinierte Entitätsdefinitionen** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die alphabetisch nach Namen 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.