

vCloud Director Service Provider Admin Portal-Handbuch

28. MÄRZ 2019

VMware Cloud Director 9.7

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

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

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

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

Copyright © 2018-2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise.](#)

Inhalt

1 Informationen zum vCloud Director Service Provider Admin Portal 8

Aktuelle Informationen 9

2 Erste Schritte mit vCloud Director Service Provider Admin Portal 10

Überblick über die vCloud Director-Verwaltung 10

Anmelden bei vCloud Director Service Provider Admin Portal 14

Anzeigen von Aufgaben 14

Beenden einer in Bearbeitung befindlichen Aufgabe 15

Anzeigen von Ereignissen 16

3 Verwalten von vSphere-Ressourcen 17

Hinzufügen von vCenter Server- und NSX-Ressourcen 18

Anhängen einer vCenter Server-Instanz allein oder zusammen mit einer NSX Manager-Instanz 18

Zuweisen des NSX-Lizenzschlüssels in vCenter Server 22

Registrieren einer NSX-T Manager-Instanz 22

Anzeigen der vCenter Server-Instanzen 23

Bearbeiten der vCenter Server-Einstellungen 24

Aktivieren oder Deaktivieren einer vCenter Server-Instanz 24

Erneutes Verbinden einer vCenter Server-Instanz 25

Aktualisieren einer vCenter Server-Instanz 25

Aktualisieren der Speicherrichtlinien einer vCenter Server-Instanz 25

Aufheben der Registrierung einer vCenter Server-Instanz 26

Bearbeiten der NSX Manager-Einstellungen 26

Bearbeiten der NSX-T Manager-Einstellungen 27

Löschen einer NSX-T Manager-Instanz 27

Ressourcenlisten für mehrere Standorte 27

4 Verwalten von virtuellen Provider-Datencentern 29

Aktivieren oder Deaktivieren eines virtuellen Provider-Datencenters 29

Löschen eines virtuellen Provider-Datencenters 30

Bearbeiten der allgemeinen Einstellungen eines virtuellen Provider-Datencenters 30

Zusammenführen von virtuellen Provider-Datencentern 31

Anzeigen der virtuellen Organisations-Datencenter eines virtuellen Provider-Datencenters 32

Anzeigen der Datenspeicher in einem virtuellen Provider-Datencenter 32

Anzeigen der externen Netzwerke in einem virtuellen Provider-Datencenter 33

Verwalten der VM-Speicherrichtlinien auf einem virtuellen Provider-Datencenter 34

Hinzufügen einer VM-Speicherrichtlinie zu einem virtuellen Provider-Datencenter	34
Aktivieren oder Deaktivieren einer VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter	35
Löschen einer VM-Speicherrichtlinie aus einem virtuellen Provider-Datencenter	35
Bearbeiten der Metadaten für eine VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter	36
Verwalten der Ressourcenpools in einem virtuellen Provider-Datencenter	36
Hinzufügen eines Ressourcenpools zu einem virtuellen Provider-Datencenter	36
Aktivieren oder Deaktivieren eines Ressourcenpools in einem virtuellen Provider-Datencenter	37
Trennen eines Ressourcenpools von einem virtuellen Provider-Datencenter	38
Bearbeiten der Metadaten für ein virtuelles Provider-Datencenter	39

5 Verwalten von Organisationen 40

Wissenswertes über Leases	40
Erstellen einer Organisation	41
Konfigurieren von Katalogen für eine Organisation	41
Konfigurieren von Richtlinien für eine Organisation	42

6 Verwalten von virtuellen Organisations-Datencentern 44

Funktionsweise von Zuweisungsmodellen	44
Vorgeschlagene Verwendung der Zuweisungsmodelle	46
Flex-Zuweisungsmodell	47
Zuweisungspool-Zuweisungsmodell	48
Zuweisungsmodell Pay-As-You-Go	50
Reservierungspool-Zuweisungsmodell	51
Grundlegendes zu Computing-Richtlinien	51
Computing-Richtlinien für virtuelle Provider-Datencenter	52
Computing-Richtlinien für virtuelle Datencenter	55
Erstellen eines virtuellen Organisations-Datencenters	59
Aktivieren oder Deaktivieren eines virtuellen Organisations-Datencenters	62
Löschen eines virtuellen Organisations-Datencenters	62
Ändern des Namens und der Beschreibung eines virtuellen Organisations-Datencenters	63
Ändern der Zuweisungsmodelleinstellungen eines virtuellen Organisations-Datencenters	63
Ändern der Speichereinstellungen eines virtuellen Organisations-Datencenters	64
Ändern der VM-Bereitstellungseinstellungen eines Organisations-VDC	64
Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC	65
Ändern der Standardspeicherrichtlinie für ein virtuelles Organisations-Datencenter	65
Bearbeiten des Grenzwerts einer Speicherrichtlinie für ein virtuelles Organisations-Datencenter	66
Ändern der Metadaten für eine VM-Speicherrichtlinie in einem virtuellen Organisations-Datencenter	66

Aktivieren oder Deaktivieren einer Speicherrichtlinie in einem virtuellen Organisations-Datencenter	67
Löschen einer Speicherrichtlinie aus einem virtuellen Organisations-Datencenter	68
Bearbeiten der Netzwerkeinstellungen eines Organisations-VDCs	68
Ändern der Metadaten für ein virtuelles Organisations-Datencenter	70
Anzeigen der Ressourcenpools eines virtuellen Organisations-Datencenters	70
Verwalten der Distributed Firewall in einem virtuellen Organisations-Datencenter	71
Aktivieren der Distributed Firewall eines Organisations-VDCs	71
Hinzufügen einer Distributed Firewall-Regel	72
Bearbeiten einer Distributed Firewall-Regel	75
Benutzerdefiniertes Gruppieren von Objekten	76
Arbeiten mit Sicherheitsgruppen	79
Arbeiten mit Sicherheitstags	83

7 Verwalten von Edge-Gateways 88

Arbeiten mit Edge-Clustern	89
Hinzufügen eines Edge-Gateways	91
Konfigurieren von Edge-Gateway-Diensten	93
Verwalten einer Edge-Gateway-Firewall	93
Verwalten des DHCP-Protokolls für Edge-Gateways	97
Hinzufügen einer SNAT- oder DNAT-Regel	103
Konfiguration für erweitertes Routing	105
Lastausgleich	116
Sicherer Zugriff mit virtuellen privaten Netzwerken	131
SSL-Zertifikatsverwaltung	160
Benutzerdefiniertes Gruppieren von Objekten	169
Anzeigen der Netzwerknutzung und der IP-Zuweisungen auf einem Edge-Gateway	172
Bearbeiten der Edge-Gateway-Eigenschaften	172
Aktivieren oder Deaktivieren von Distributed Routing auf einem Edge-Gateway	173
Ändern der externen Netzwerke und der Edge-Gateway-Einstellungen	173
Bearbeiten der allgemeinen Einstellungen für ein Edge-Gateway	174
Bearbeiten des Standard-Gateways für ein Edge-Gateway	174
Bearbeiten der IP-Einstellungen für ein Edge-Gateway	175
Bearbeiten der unterzugewiesenen IP-Pools eines Edge-Gateways	175
Bearbeiten von Ratengrenzwerten für ein Edge-Gateway	176
Edge-Gateway erneut bereitstellen	176
Löschen eines Edge-Gateways	177
Statistiken und Protokolle für ein Edge-Gateway	177
Anzeigen von Statistiken	177
Protokollierung aktivieren	178
Aktivieren des SSH-Befehlszeilenzugriffs auf ein Edge-Gateway	180

8	Verwalten von VDC-Organisationsnetzwerken	181
	Verwalten eines NSX-T-VDC-Organisationsnetzwerks	181
	Hinzufügen eines NSX-T-VDC-Organisationsnetzwerks	181
	Bearbeiten eines NSX-T-VDC-Organisationsnetzwerks	182
	Löschen eines NSX-T-VDC-Organisationsnetzwerks	183
9	Verwalten von SDDCs und SDDC-Proxys	184
10	Verwalten von Systemadministratoren und Rollen	186
	Verwalten von Rechten und Rollen	186
	Vordefinierte Rollen und ihre Rechte	188
	Neue Rechte in dieser Version	196
	Verwalten von Rechtepaketen	198
	Verwalten von globalen Mandantenrollen	200
	Verwalten von Anbieterrollen	204
	Verwalten von Anbieterbenutzern und -gruppen	206
	Verwalten von Anbieterbenutzern	206
	Verwalten von Anbietergruppen	209
11	Verwalten der Systemeinstellungen	211
	Verwalten von Identitätsanbietern	211
	Verwalten von LDAP-Verbindungen	211
	Konfigurieren Ihres Systems für die Verwendung eines SAML-Identitätsanbieters	215
	Verwalten von Plug-Ins	216
	Hochladen eines Plug-Ins	217
	Aktivieren oder Deaktivieren eines Plug-Ins	218
	Löschen eines Plug-Ins	218
	Veröffentlichen oder Rückgängigmachen der Veröffentlichung eines Plug-Ins in einer Organisation	218
	Anpassen der vCloud Director-Portale	219
12	Überwachen von vCloud Director	221
	vCloud Director und Kostenberichte	221
	Anzeigen von Nutzungsinformationen für ein virtuelles Provider-Datencenter	222
13	Verwalten von Diensten	223
	Integrieren von vRealize Orchestrator mit vCloud Director	223
	Registrieren einer vRealize Orchestrator-Instanz bei vCloud Director	224
	Erstellen einer Dienstkategorie	225
	Bearbeiten einer Dienstkategorie	225
	Importieren eines Diensts	226

- [Auffinden eines Diensts](#) 227
- [Ausführen eines Diensts](#) 227
- [Ändern einer Dienstkategorie](#) 228
- [Aufheben der Registrierung eines Diensts](#) 229
- [Veröffentlichen eines Diensts](#) 229

14 Verwalten von benutzerdefinierten Entitäten 231

- [Auffinden einer benutzerdefinierten Entität](#) 231
- [Bearbeiten einer benutzerdefinierten Entitätsdefinition](#) 232
- [Hinzufügen einer benutzerdefinierten Entitätsdefinition](#) 232
- [Benutzerdefinierte Entitätsinstanzen](#) 233
- [Verknüpfen einer Aktion mit einer benutzerdefinierten Entität](#) 234
- [Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entität](#) 235
- [Veröffentlichen einer benutzerdefinierten Entität](#) 235
- [Löschen einer benutzerdefinierten Entität](#) 236

Informationen zum vCloud Director Service Provider Admin Portal

1

Das *vCloud Director Service Provider Admin Portal-Handbuch* enthält Informationen zur Verwendung des Service Provider Admin Portal. Sie verwalten und überwachen Organisationen, Rechte, Rollen, Benutzer und Gruppen in Ihrer Cloud über das service provider admin portal. Sie können auch durch NSX-T gestützte VDC-Organisationsnetzwerke erstellen und verwalten.

Zielgruppe

Dieses Handbuch richtet sich an Dienstanbieteradministratoren, die die im vCloud Director Service Provider Admin Portal bereitgestellten Funktionen verwenden möchten.

Verwandte Dokumentation

Weitere Informationen über die Funktionen, die einem Administrator bei Verwendung der vCloud Director-Webkonsole anstelle des vCloud Directorservice provider admin portal zur Verfügung stehen, finden Sie im *vCloud Director-Administratorhandbuch*

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

Aktuelle Informationen

Dieses *vCloud Director Service Provider Admin Portal-Handbuch* wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *vCloud Director Service Provider Admin Portal-Handbuch*.

Revision	Beschreibung
5. April 2019	Die Informationen in den Kapiteln Funktionsweise von Zuweisungsmodellen und Grundlegendes zu Computing-Richtlinien wurden überarbeitet.
28. März 2019	Erstversion.

Erste Schritte mit vCloud Director Service Provider Admin Portal

2

Das vCloud Director Service Provider Admin Portal ist eine dedizierte Schnittstelle für Diensteanbieteradministratoren.

Dieses Kapitel enthält die folgenden Themen:

- [Überblick über die vCloud Director-Verwaltung](#)
- [Anmelden bei vCloud Director Service Provider Admin Portal](#)
- [Anzeigen von Aufgaben](#)
- [Beenden einer in Bearbeitung befindlichen Aufgabe](#)
- [Anzeigen von Ereignissen](#)

Überblick über die vCloud Director-Verwaltung

Mit VMware vCloud Director können Sie sichere Clouds mit mehreren Mandanten einrichten, indem Sie virtuelle Infrastrukturressourcen in virtuellen Datencentern poolen und sie an Benutzer über webbasierte Portale und Programmschnittstellen als vollautomatischen, katalogbasierten Dienst bereitstellen.

Das *vCloud Director-Administratorhandbuch* enthält Informationen zum Hinzufügen von Ressourcen zum System, zum Erstellen und Bereitstellen von Organisationen, zum Verwalten von Ressourcen und Organisationen und zum Überwachen des Systems.

vSphere- und NSX-Ressourcen

vCloud Director stellt Prozessorleistung und Arbeitsspeicher für den Betrieb virtueller Maschinen auf der Grundlage von vSphere-Ressourcen bereit. Darüber hinaus stellen vSphere-Datenspeicher Speicherplatz für Dateien von virtuellen Maschinen und andere Dateien, die beim Betrieb der virtuellen Maschinen benötigt werden, zur Verfügung. vCloud Director verwendet auch vSphere Distributed Switches, vSphere-Portgruppen und NSX Data Center for vSphere, um virtuelle Maschinennetzwerke zu unterstützen.

vCloud Director kann auch Ressourcen von NSX-T Data Center verwenden. Informationen über die Registrierung einer NSX-T Manager-Instanz in Ihrer Cloud finden Sie im *vCloud Director Service Provider Admin Portal-Handbuch* oder im *vCloud API-Programmierhandbuch für Diensteanbieter*.

Sie können die zugrunde liegenden vSphere- und NSX-Ressourcen zur Erstellung von Cloud-Ressourcen verwenden.

Ab Version 9.7 kann vCloud Director als HTTP-Proxyserver fungieren, mit dem Sie Organisationen den Zugriff auf die zugrunde liegende vSphere-Umgebung ermöglichen können.

Cloud-Ressourcen

Cloud-Ressourcen sind eine Abstraktion der zugrunde liegenden vSphere-Ressourcen. Sie stellen die Rechen- und Arbeitsspeicherressourcen für virtuelle Maschinen und vApps unter vCloud Director bereit. Eine vApp ist ein virtuelles System, das eine oder mehrere virtuelle Maschinen sowie Parameter zur Festlegung von Betriebsdetails enthält. Cloud-Ressourcen bieten auch Zugriff auf Speicher und Netzwerkkonnektivität.

Cloud-Ressourcen sind u. a. virtuelle Provider- und Organisations-Datencenter, externe Netzwerke, virtuelle Organisations-Datencenter-Netzwerke und Netzwerkpools. Darüber hinaus führt vCloud Director 9.7 das Software-Defined Data Center (SDDC) und die SDDC-Proxys als Cloudressourcen ein, die Zugriff auf die zugrunde liegende vSphere-Umgebung über vCloud Director ermöglichen.

Bevor Sie Cloud-Ressourcen zu vCloud Director hinzufügen können, müssen Sie vSphere-Ressourcen hinzufügen.

SDDCs und SDDC-Proxys

vCloud Director 9.7 führt das SDDC als Cloud-Ressource ein, in der eine vollständige vCenter Server-Installation gekapselt ist. Ein SDDC enthält einen oder mehrere SDDC-Proxys, die Zugriffspunkte auf verschiedene Komponenten der zugrunde liegenden vSphere-Umgebung sind. Der Anbieter kann ein SDDC und Proxys erstellen und aktivieren. Der Anbieter kann ein SDDC und dessen Proxys für Mandanten veröffentlichen.

Um SDDCs und Proxys zu erstellen und zu verwalten, müssen Sie die vCloud OpenAPI verwenden. Weitere Informationen finden Sie unter *Erste Schritte mit vCloud OpenAPI* auf <https://code.vmware.com>.

Virtuelle Provider-Datencenter

Virtuelle Provider-Datencenter kombinieren die Rechen- und Arbeitsspeicherressourcen eines einzelnen vCenter Server-Ressourcenpools mit den Speicherressourcen eines oder mehrerer Datenspeicher, die für diesen Ressourcenpool zur Verfügung stehen.

Ein virtuelles Provider-Datencenter kann Netzwerkressourcen aus einer NSX Manager-Instanz verwenden, die mit der vCenter Server-Instanz verknüpft ist, oder aus einer NSX-T Manager-Instanz, die mit der Cloud registriert ist.

Sie können mehrere virtuelle Provider-Datencenter für Benutzer an unterschiedlichen geografischen Standorten oder aus verschiedenen Geschäftseinheiten oder auch für Benutzer mit eigenen Systemleistungsanforderungen erstellen.

Virtuelle Organisations-Datencenter

Virtuelle Organisations-Datencenter stellen Ressourcen für Organisationen bereit. Sie werden von einem virtuellen Provider-Datencenter abgetrennt. Virtuelle Organisations-Datencenter stellen eine Umgebung bereit, in der virtuelle Systeme gespeichert, bereitgestellt und betrieben werden können. Darüber hinaus stellen sie auch Speicher für virtuelle Medien, beispielsweise Disketten und CD-ROMs, bereit.

Eine einzelne Organisation kann über mehrere virtuelle Organisations-Datencenter verfügen.

vCloud Director-Netzwerk

vCloud Director unterstützt drei Netzwerktypen.

- Externe Netzwerke
- VDC-Organisationsnetzwerke
- vApp-Netzwerke

Einige virtuelle Organisations-Datencenter-Netzwerke und alle vApp-Netzwerke werden von Netzwerkpools unterstützt.

Externe Netzwerke

Bei einem externen Netzwerk handelt es sich um ein logisches, differenziertes Netzwerk auf der Basis einer vSphere-Portgruppe. VDC-Organisationsnetzwerke können eine Verbindung zu externen Netzwerken herstellen und auf diese Weise für die virtuellen Maschinen in vApps Internetkonnektivität bereitstellen.

Ab Version 9.5 unterstützt vCloud Director externe IPv6-Netzwerke. Ein externes IPv6-Netzwerk unterstützt sowohl IPv4- als auch IPv6-Subnetze, und ein externes IPv4-Netzwerk unterstützt sowohl IPv4- als auch IPv6-Subnetze.

Standardmäßig ist die Berechtigung zum Erstellen und Verwalten von externen Netzwerken **Systemadministratoren** vorbehalten.

VDC-Organisationsnetzwerke

Ein VDC-Organisationsnetzwerk ist ein Bestandteil eines vCloud Director-Organisations-VDCs. Es steht allen vApps in der Organisation zur Verfügung. VDC-Organisationsnetzwerke ermöglichen es vApps, Daten in einer Organisation miteinander auszutauschen. Um externe Konnektivität bereitzustellen, können Sie ein VDC-Organisationsnetzwerk mit einem externen Netzwerk verbinden. Sie können auch ein isoliertes virtuelles Organisations-Datencenter-Netzwerk erstellen, das auf die interne Organisation beschränkt ist.

vCloud Director 9.5 führt IPv6-Unterstützung für direkte und geroutete VDC-Organisationsnetzwerke ein.

Beginnend mit vCloud Director 9.5 können **Systemadministratoren** isolierte virtuelle Datencenter-Netzwerke erstellen, die von einem logischen NSX-T-Switch unterstützt werden. **Organisationsadministratoren** können isolierte virtuelle Datencenter-Netzwerke erstellen, die von Netzwerkpools unterstützt werden.

vCloud Director 9.5 führt auch VDC-übergreifende Netzwerke ein, indem erweiterte Netzwerke in virtuellen Datencenter-Gruppen konfiguriert werden.

Standardmäßig können nur **Systemadministratoren** direkte und VDC-übergreifende Netzwerke erstellen. Sowohl **Systemadministratoren** als auch **Organisationsadministratoren** verfügen über die erforderlichen Berechtigungen, virtuelle Organisations-Datencenter-Netzwerke zu verwalten; die Berechtigungen von **Organisationsadministratoren** sind jedoch stärker eingeschränkt.

vApp-Netzwerke

vApp-Netzwerke sind Bestandteile von vApps und ermöglichen es virtuellen Maschinen in der vApp, Daten miteinander auszutauschen. Damit eine vApp mit anderen vApps in der Organisation kommunizieren kann, können Sie das vApp-Netzwerk mit einem VDC-Organisationsnetzwerk verbinden. Wenn das VDC-Organisationsnetzwerk mit einem externen Netzwerk verbunden ist, kann die vApp mit vApps in anderen Organisationen kommunizieren. vApp-Netzwerke werden von Netzwerkpools gestützt.

Die meisten Benutzer mit Zugriff auf eine vApp können eigene vApp-Netzwerke erstellen und verwalten. Informationen zum Arbeiten mit Netzwerken in einer vApp finden Sie im *Handbuch für das vCloud Director Mandantenportal*.

Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die in einem virtuellen Organisations-Datencenter zur Verfügung gestellt werden. Ein Netzwerkpool wird von vSphere-Netzwerkressourcen wie VLAN-IDs oder Portgruppen unterstützt. In vCloud Director werden anhand von Netzwerkpools VDC-Organisationsnetzwerke mit NAT Routing und interne VDC-Organisationsnetzwerke sowie alle vApp-Netzwerke erstellt. Der Datenverkehr in den einzelnen Netzwerken wird auf der Ebene von Layer 2 von allen anderen Netzwerken isoliert.

Jedes Organisations-VDC in vCloud Director kann einen Netzwerkpool haben. Mehrere Organisations-VDCs können einen Netzwerkpool gemeinsam nutzen. Der Netzwerkpool für ein Organisations-VDC stellt die Netzwerke bereit, die erstellt wurden, um das Netzwerkkontingent für ein Organisations-VDC zu erfüllen.

Die Berechtigung zum Erstellen und Verwalten von Netzwerkpools ist **Systemadministratoren** vorbehalten.

Organisationen

vCloud Director unterstützt mehrere Mandanten mithilfe von Organisationen. Eine Organisation ist eine Verwaltungseinheit für eine Sammlung von Benutzern, Gruppen und Rechenressourcen. Benutzer melden sich auf der Ebene von Organisationen mit den Anmeldeinformationen an, 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. Die Aufgaben von **Organisationsadministratoren** sind in *Handbuch für das vCloud Director Mandantenportal* beschrieben.

Benutzer und Gruppen

Organisationen können über eine beliebige Anzahl an Benutzern und Gruppen verfügen.

Organisationsadministratoren können Benutzer erstellen und Benutzer und Gruppen aus einem Verzeichnisdienst wie LDAP importieren. Der **Systemadministrator** verwaltet den Satz von Rechten, die in jeder Organisation zur Verfügung stehen. Der **Systemadministrator** kann globale Mandantenrollen für eine oder mehrere Organisationen erstellen und veröffentlichen. Der **Organisationsadministrator** kann lokale Rollen in seinen Organisationen erstellen.

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. **Systemadministratoren** können einer Organisation erlauben, Kataloge zu veröffentlichen, um sie anderen Organisationen zur Verfügung zu stellen. **Organisationsadministratoren** können auswählen, welche Objekte des Katalogs sie für die Benutzer bereitstellen möchten.

Anmelden bei vCloud Director Service Provider Admin Portal

Sie können mithilfe eines Webbrowsers auf das vCloud Director Service Provider Admin Portal zugreifen.

Voraussetzungen

Sie müssen über Systemadministratorrechte verfügen, um auf das vCloud Director Service Provider Admin Portal zugreifen zu können.

Verfahren

- 1 Geben Sie die Service Provider Admin Portal-URL der vCloud Director-Site in einem Browser ein und drücken Sie die Eingabetaste.
Geben Sie beispielsweise **`https://vcloud.example.com/provider`** ein.
- 2 Melden Sie sich mit dem Benutzernamen und Kennwort des Systemadministrators an.

Anzeigen von Aufgaben

Im Service Provider Admin Portal können Sie kürzlich bearbeitete Aufgaben und deren Status anzeigen.

Die Aufgabenansicht eignet sich hervorragend, um auf einen Blick den Status von Aufgaben im Service Provider Admin Portal anzuzeigen. In der Ansicht wird angezeigt, wann die Aufgaben ausgeführt wurden und ob die Ausführung erfolgreich war. Dieses Tool kann im ersten Schritt zur Fehlerbehebung bei Problemen in Ihrer Umgebung eingesetzt werden.

Die blauen und roten Infotipps über dem Aufgabensymbol zeigen die Anzahl der ausgeführten und fehlgeschlagenen Aufgaben an.

Verfahren

- ◆ Wählen Sie im Menü oben rechts das Aufgabensymbol () aus.

Ergebnisse

Eine Liste der kürzlich bearbeiteten Aufgaben wird zusammen mit der Uhrzeit, zu der die Aufgabe ausgeführt wurde, und dem Status der Aufgabe angezeigt.

Beenden einer in Bearbeitung befindlichen Aufgabe


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

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

Voraussetzungen

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

Verfahren

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

Ergebnisse


Der Vorgang wird beendet.

Anzeigen von Ereignissen


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

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

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Ereignisse** aus.

Die Liste aller Ereignisse wird angezeigt, sowie die Zeit, zu der das Ereignis aufgetreten ist, und der Status des Ereignisses.

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

- 3 (Optional) Klicken Sie auf ein Ereignis, um die Ereignisdetails anzuzeigen.

Detail	Beschreibung
Ereignis	Der Name des Ereignisses Wenn Sie beispielsweise eine vApp ändern, um virtuelle Maschinen darin einzuschließen, ist das Ereignis, das den gesamten Vorgang startet, <i>Aufgabe „vApp ändern“ starten</i> .
Ereignis-ID	Die ID der Aufgabe
Typ	Das Objekt, für das die Aufgabe durchgeführt wurde. Wenn Sie eine virtuelle Maschine erstellt haben, ist der Typ z. B. <i>vm</i> .
Ziel	Das Zielobjekt des Ereignisses Wenn Sie beispielsweise eine vApp ändern, um virtuelle Maschinen darin einzuschließen, ist das Ziel des Ereignisses <i>Aufgabe „vApp ändern“ startenvdcUpdateVapp</i> .
Status	Der Status des Ereignisses, z. B. „Erfolgreich“ oder „Fehlgeschlagen“
Dienst-Namespace	Der Dienstname, z. B. <i>com.vmware.vcloud</i>
Organisation	Der Name der Organisation
Besitzer	Der Benutzer, der das Ereignis ausgelöst hat
Zeitpunkt des Auftretens	Datum und Uhrzeit, wann das Ereignis aufgetreten ist

Verwalten von vSphere-Ressourcen

3

vCloud Director entnimmt seine Ressourcen der zugrunde liegenden virtuellen vSphere-Infrastruktur. Sie registrieren vSphere-Ressourcen in vCloud Director, um sie anschließend Organisationen in der vSphere-Installation zur Nutzung zuzuweisen.

vCloud Director verwendet eine oder mehrere vCenter Server-Umgebungen, um die virtuellen Datencenter zu unterstützen. Ab Version 9.7 kann vCloud Director auch eine vCenter Server-Umgebung verwenden, um ein SDDC mit einem oder mehreren Proxys zu kapseln. Sie können Mandanten ermöglichen, diese Proxys als Zugriffspunkte auf die zugrunde liegende vSphere-Umgebung von vCloud Director mit ihren vCloud Director-Konten zu verwenden.

Bevor Sie eine vCenter Server-Instanz in vCloud Director verwenden können, müssen Sie diese vCenter Server-Instanz anhängen.

Wenn Sie ein virtuelles Provider-Datencenter erstellen, das von einer angehängten vCenter Server-Instanz unterstützt wird, wird diese vCenter Server-Instanz als für den Dienstanbieter veröffentlicht angezeigt, was auch als „anbieterzentriert“ bezeichnet wird. Informationen zum Erstellen eines virtuellen Provider-Datencenters finden Sie unter im *vCloud Director Administratorhandbuch*.

Wenn Sie ein SDDC erstellen, in dem eine angehängte vCenter Server-Instanz gekapselt ist, wird diese vCenter Server-Instanz als für Mandanten veröffentlicht angezeigt, was auch als „mandantenzentriert“ bezeichnet wird. Informationen zum Erstellen eines SDDC finden Sie unter [Kapitel 9 Verwalten von SDDCs und SDDC-Proxys](#).

Hinweis Standardmäßig können Sie mit einer angehängten vCenter Server-Instanz entweder ein Provider-VDC oder ein SDDC erstellen. Wenn Sie ein Provider-VDC erstellt haben, das von einer vCenter Server-Instanz gestützt wird, können Sie diese vCenter Server-Instanz nicht zum Erstellen eines SDDC verwenden, bzw. umgekehrt. Sie können die vCloud-API verwenden, um die Systemeinstellungen Ihrer vCloud Director-Installation zu ändern, sodass eine vCenter Server-Instanz sowohl ein Provider-VDC als auch ein SDDC stützen kann.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen von vCenter Server- und NSX-Ressourcen](#)
- [Anzeigen der vCenter Server-Instanzen](#)

- Bearbeiten der vCenter Server-Einstellungen
- Aktivieren oder Deaktivieren einer vCenter Server-Instanz
- Erneutes Verbinden einer vCenter Server-Instanz
- Aktualisieren einer vCenter Server-Instanz
- Aktualisieren der Speicherrichtlinien einer vCenter Server-Instanz
- Aufheben der Registrierung einer vCenter Server-Instanz
- Bearbeiten der NSX Manager-Einstellungen
- Bearbeiten der NSX-T Manager-Einstellungen
- Löschen einer NSX-T Manager-Instanz
- Ressourcenlisten für mehrere Standorte

Hinzufügen von vCenter Server- und NSX-Ressourcen

vCloud Director stellt CPU, Arbeitsspeicher und Speicher für den Betrieb virtueller Maschinen auf der Grundlage von vSphere-Ressourcen bereit. Darüber hinaus kann vCloud Director ab Version 9.7 als HTTP-Server zwischen Mandanten und der zugrunde liegenden vSphere-Umgebung fungieren.

Informationen zu den Systemanforderungen von vCloud Director und den unterstützten Versionen von vCenter Server und ESXi finden Sie in den *VMware-Produkt-Interoperabilitätstabellen* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Anhängen einer vCenter Server-Instanz allein oder zusammen mit einer NSX Manager-Instanz

Sie hängen eine vCenter Server-Instanz an, sodass deren Ressourcen für die Verwendung in vCloud Director verfügbar werden. Sie können eine vCenter Server-Instanz zusammen mit der ihr zugeordneten NSX Manager-Instanz anhängen oder Sie können eine vCenter Server-Instanz allein anhängen.

vCloud Director kann eine vCenter Server-Instanz entweder mit der ihr zugeordneten NSX Manager-Instanz oder mit einer NSX-T Manager-Instanz verwenden.

Wenn vCloud Director diese vCenter Server-Instanz mit der ihr zugeordneten NSX Manager-Instanz verwendet werden soll, müssen Sie die vCenter Server- und die NSX Manager-Instanzen zusammen anhängen.

Wenn vCloud Director diese vCenter Server-Instanz mit einer NSX-T Manager-Instanz verwenden soll, müssen Sie die vCenter Server-Instanz allein anhängen. Nachdem Sie die vCenter Server-Instanz allein angehängt haben, müssen Sie wie unter [Registrieren einer NSX-T Manager-Instanz](#) angegeben vorgehen.

Hinweis Nachdem Sie eine vCenter Server-Instanz allein angehängt haben, können Sie die zugeordnete NSX Manager-Instanz nicht zu einem späteren Zeitpunkt hinzufügen. Sie können die Registrierung aufheben und die vCenter Server-Instanz zusammen mit der ihr zugeordneten NSX Manager-Instanz erneut anhängen.

Sie können eine vCenter Server-Instanz an eine beliebige Site aus Ihrer vCloud Director-Umgebung anhängen.

Voraussetzungen

- Wenn Sie vCloud Director zum Überprüfen der vCenter- und vSphere-SSO-Zertifikate konfiguriert haben, stellen Sie sicher, dass die vCenter Server-Zertifikate auf vCloud Director hochgeladen wurden. Informationen zu allgemeinen Systemeinstellungen finden Sie im *vCloud Director-Administratorhandbuch*.
- Wenn Sie vCloud Director zum Überprüfen von NSX Manager-Zertifikaten konfiguriert haben, stellen Sie sicher, dass die NSX Manager-Zertifikate auf vCloud Director hochgeladen wurden. Informationen zu allgemeinen Systemeinstellungen finden Sie im *vCloud Director-Administratorhandbuch*.

Verfahren

1 [Hinzufügen der vCenter Server-Instanz](#)

Um eine vCenter Server-Instanz hinzuzufügen, geben Sie die vCenter Server-Zugriffsdaten ein.


2 [\(Optional\) Hinzufügen der verknüpften NSX Manager-Instanz](#)

Wenn vCloud Director diese vCenter Server-Instanz mit der ihr zugeordneten NSX Manager-Instanz verwenden soll, müssen Sie NSX Manager-Zugriffsdaten hinzufügen.

Hinzufügen der vCenter Server-Instanz

Um eine vCenter Server-Instanz hinzuzufügen, geben Sie die vCenter Server-Zugriffsdaten ein.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter** und dann auf **Hinzufügen**.
- 3 Wenn Sie über eine Multisite-vCloud Director-Bereitstellung verfügen, wählen Sie im Dropdown-Menü **Site** die Site aus, der Sie diese vCenter Server-Instanz hinzufügen möchten, und klicken Sie auf **Weiter**.

- 4 Geben Sie einen Namen und optional eine Beschreibung für die vCenter Server-Instanz in vCloud Director ein.

- 5 Geben Sie die URL der vCenter Server-Instanz ein.

Wenn der Standardport verwendet wird, können Sie die Portnummer überspringen. Wenn ein benutzerdefinierter Port verwendet wird, fügen Sie die Portnummer hinzu.

Beispiel: **https://FQDN_or_IP_address:<custom_port_number>**.

- 6 Geben Sie den Benutzernamen und das Kennwort für das vCenter Server-Administratorkonto ein.
- 7 (Optional) Um die vCenter Server-Instanz nach der Registrierung zu deaktivieren, deaktivieren Sie die Umschaltoption **Aktiviert**.
- 8 Konfigurieren Sie die URL des vCenter Server-Webclients.

Option	Beschreibung
URL mit vSphere-Diensten bereitstellen	Um diese Option verwenden zu können, müssen Sie mithilfe der vCloud-API vCloud Director für die Verwendung des vSphere Lookup Service konfigurieren.
vSphere Web Client-URL	Um diese Option verwenden zu können, müssen Sie die URL des vSphere Web Client eingeben. Beispiel: https://example.vmware.com/vsphere-client.

- 9 Klicken Sie auf **Weiter**.
- 10 (Optional) Überspringen Sie das Hinzufügen der NSX Manager-Instanz, die der vCenter Server-Instanz zugeordnet ist, und schließen Sie die Registrierung ab.

Wenn vCloud Director diese vCenter Server-Instanz mit einer NSX-T Manager-Instanz verwenden soll, müssen Sie die vCenter Server-Instanz allein hinzufügen.

Hinweis Sie können die zugeordnete NSX Manager-Instanz nicht zu einem späteren Zeitpunkt hinzufügen. Sie können die Registrierung aufheben und die vCenter Server-Instanz zusammen mit der ihr zugeordneten NSX Manager-Instanz erneut anhängen.

- a Deaktivieren Sie auf der Seite **NSX-V Manager-Einstellungen** die Umschaltoption **Einstellungen konfigurieren** und klicken Sie auf **Weiter**.
- b Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Registrierungsdaten und klicken Sie auf **Fertigstellen**.

(Optional) Hinzufügen der verknüpften NSX Manager-Instanz

Wenn vCloud Director diese vCenter Server-Instanz mit der ihr zugeordneten NSX Manager-Instanz verwenden soll, müssen Sie NSX Manager-Zugriffsdaten hinzufügen.

Verfahren

- 1 Lassen Sie auf der Seite **NSX-V Manager-Einstellungen** die Umschaltoption **Einstellungen konfigurieren** aktiviert.

- 2 Geben Sie die URL der NSX Manager-Instanz ein.

Wenn der Standardport verwendet wird, können Sie die Portnummer überspringen. Wenn ein benutzerdefinierter Port verwendet wird, fügen Sie die Portnummer hinzu.

Beispiel: **https://FQDN_or_IP_address: <custom_port_number>**.

- 3 Geben Sie den Benutzernamen und das Kennwort für das NSX-Administratorkonto ein..
- 4 (Optional) Um VDC-übergreifende Netzwerke für die von dieser vCenter Server-Instanz gestützten virtuellen Datencenter zu ermöglichen, aktivieren Sie die Umschaltoption **VDC-übergreifende Netzwerke** und geben Sie die Bereitstellungseigenschaften für die Steuerungs-VM und einen Namen für den Netzwerkanbieter-Bereich ein.

Die Bereitstellungseigenschaften der Steuerungs-VM dienen zur Bereitstellung einer Appliance auf der NSX Manager-Instanz für Komponenten von VDC-übergreifenden Netzwerken, wie z. B. einem globalen Router.

Option	Beschreibung
Ressourcenpoolpfad	Der hierarchische Pfad zu einem bestimmten Ressourcenpool in der vCenter Server-Instanz, beginnend mit dem Cluster <i>Cluster/Übergeordnetes Element des Ressourcenpools/Zielressource</i> . Beispielsweise TestbedCluster1/mgmt-rp . Alternativ hierzu können Sie die MoRef-ID (Managed Object Reference) des Ressourcenpools eingeben. Beispielsweise resgroup-1476 .
Datenspeichername	Der Name des Datenspeichers zum Hosten der Appliance-Dateien. Zum Beispiel shared-disk-1 .
Verwaltungsschnittstelle	Der Name des Netzwerks in vCenter Server oder der Portgruppe, das bzw. die für die HA-DLR-Management-Schnittstelle verwendet wird. Zum Beispiel TestbedPG1 .
Netzwerkanbieter-Bereich	Entspricht der Netzwerk-Fehlerdomäne in den Netzwerktopologien der Datencenter-Gruppen. Zum Beispiel boston-fault1 . Informationen zur Verwaltung von VDC-übergreifenden Gruppen finden Sie im <i>Handbuch für das vCloud Director Mandantenportal</i> .

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

Nächste Schritte

- [Zuweisen des NSX-Lizenzschlüssels in vCenter Server](#).
- Informationen zum Erstellen eines virtuellen Provider-Datencenters finden Sie im *vCloud Director-Administratorhandbuch*.

Zuweisen des NSX-Lizenzschlüssels in vCenter Server

Nachdem Sie eine vCenter Server-Instanz zusammen mit der ihr zugeordneten NSX Manager-Instanz angehängt haben, müssen Sie mittels vSphere Client einen Lizenzschlüssel für die NSX Manager-Instanz zuweisen, die vCloud Director-Netzwerke unterstützt.

Voraussetzungen

Dieser Vorgang ist Systemadministratoren vorbehalten.

Verfahren

- 1 Wählen Sie in einem vSphere-Client, der mit dem vCenter Server-System verbunden ist, die Option **Startseite > Lizenzierung**.
- 2 Wählen Sie die Option **Ressource**, um die Berichtansicht anzuzeigen.
- 3 Klicken Sie mit der rechten Maustaste auf das NSX Manager-Objekt und wählen Sie **Lizenzschlüssel bearbeiten**.
- 4 Wählen Sie die Option **Neuen Lizenzschlüssel zuweisen** und klicken Sie dann auf **Schlüssel eingeben**.
- 5 Geben Sie den Lizenzschlüssel ein, geben Sie bei Bedarf eine Beschriftung für den Schlüssel ein und klicken Sie dann auf **OK**.


Verwenden Sie den Lizenzschlüssel für NSX Manager, den Sie beim Erwerb von vCloud Director erhalten haben. Sie können diesen Lizenzschlüssel in mehreren vCenter Server-Instanzen verwenden.

- 6 Klicken Sie auf **OK**.

Registrieren einer NSX-T Manager-Instanz

Sie können eine NSX-T Manager-Instanz bei vCloud Director registrieren, damit vCloud Director deren Netzwerkressourcen verwenden kann. Ein virtuelles Provider-Datencenter kann Netzwerkressourcen entweder von NSX Data Center for vSphere oder von NSX-T Data Center verwenden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **NSX-T Manager** und klicken Sie dann auf **Hinzufügen**.
- 3 Wenn Sie über eine Multisite-vCloud Director-Bereitstellung verfügen, wählen Sie im Dropdown-Menü **Site** die Site aus, der Sie diese NSX-T Manager-Instanz hinzufügen möchten, und klicken Sie auf **Weiter**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die NSX-T Manager-Instanz in vCloud Director ein.

- 5 Geben Sie die URL der NSX-T Manager-Instanz ein.

Beispiel: **https://FQDN_or_IP_address.**

- 6 Geben Sie den Benutzernamen und das Kennwort für das NSX-T Manager-Administratorkonto ein.

- 7 Klicken Sie auf **Speichern**.


Nächste Schritte

Informationen zum Erstellen eines virtuellen Provider-Datencenters, das von NSX-T Data Center gestützt wird, finden Sie unter *vCloud API-Programmierhandbuch für Dienstleister* unter <https://code.vmware.com>.

Anzeigen der vCenter Server-Instanzen

Sie können eine Liste der vCenter Server-Instanzen auf allen Sites in Ihrer vCloud Director-Installation anzeigen. Sie können sehen, wie vCloud Director jede vCenter Server-Instanz verwendet.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter**.

Ergebnisse

Eine Liste aller angehängten vCenter Server-Instanzen wird angezeigt. Die Liste enthält die folgenden Informationen für jede vCenter Server-Instanz.


	Beschreibung
Name	Der Name der vCenter Server-Instanz in vCloud Director.
Zustand	Aktiviert oder deaktiviert. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren einer vCenter Server-Instanz .
Verbindung	Mit vCloud Director verbunden oder nicht verbunden. Weitere Informationen finden Sie unter Erneutes Verbinden einer vCenter Server-Instanz .
VC-Host	FQDN der vCenter Server-Instanz.
Version	Die vCenter Server-Version.
Dienstleister	Für die Verwendung durch virtuelle Datencenter veröffentlicht oder nicht veröffentlicht.
Mandant	Für die Verwendung als Software-Defined Data Center (SDDC) veröffentlicht oder nicht veröffentlicht.
Standort	Der vCloud Director-FQDN für den Standort, zu dem die vCenter Server-Instanz gehört.

Bearbeiten der vCenter Server-Einstellungen

Wenn die Verbindungseinstellungen für eine angehängte vCenter Server-Instanz geändert werden oder wenn Sie den Namen und die Beschreibung der Instanz in vCloud Director ändern möchten, können Sie diese Einstellungen bearbeiten.

Sie können die Einstellungen ändern, die Sie beim Hinzufügen der vCenter Server-Instanz konfiguriert haben. Weitere Informationen finden Sie unter [Hinzufügen der vCenter Server-Instanz](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter** und klicken Sie dann auf den Namen der vCenter Server-Instanz, die Sie ändern möchten.
- 3 Klicken Sie in der oberen rechten Ecke des Abschnitts **Info zu vCenter** auf **Bearbeiten**.
- 4 Bearbeiten Sie die vCenter Server-Einstellungen und klicken Sie auf **Speichern**.


Nächste Schritte

Wenn Sie die Verbindungsinformationen geändert haben, müssen Sie [Erneutes Verbinden einer vCenter Server-Instanz](#).

Aktivieren oder Deaktivieren einer vCenter Server-Instanz

Bevor Sie eine Wartung durchführen oder die Registrierung einer vCenter Server-Instanz aufheben, müssen Sie die vCenter Server-Zielinstanz deaktivieren. Um die Ressourcen für virtuelle Datacenter in vCloud Director bereitzustellen, müssen Sie die vCenter Server-Instanz aktivieren.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der vCenter Server-Zielinstanz und klicken Sie dann auf **Aktivieren** oder **Deaktivieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Erneutes Verbinden einer vCenter Server-Instanz

Wenn eine vCenter Server-Instanz als „getrennt“ angezeigt wird oder wenn Sie die Verbindungseinstellungen geändert haben, können Sie versuchen, die Verbindung zurückzusetzen.

Hinweis Während der Einrichtung der neuen Verbindung ist die vCenter Server-Instanz für Vorgänge nicht verfügbar.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der vCenter Server-Zielinstanz und klicken Sie dann auf **Erneut verbinden**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Aktualisieren einer vCenter Server-Instanz

Um in der vCloud Director-Datenbank die Informationen über die zugrunde liegenden vCenter Server-Ressourcen zu aktualisieren, müssen Sie die vCenter Server-Instanz aktualisieren.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der vCenter Server-Zielinstanz und klicken Sie auf **Aktualisieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Aktualisieren der Speicherrichtlinien einer vCenter Server-Instanz

Um in der vCloud Director-Datenbank die Informationen über die VM-Speicherrichtlinien in der zugrunde liegenden vSphere-Umgebung zu aktualisieren, müssen Sie die Speicherrichtlinien der vCenter Server-Instanz aktualisieren.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter**.

- 3 Klicken Sie auf das Optionsfeld neben dem Namen der vCenter Server-Zielinstanz und klicken Sie dann auf **Richtlinien aktualisieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.


Aufheben der Registrierung einer vCenter Server-Instanz

Um die Verwendung der Ressourcen einer vCenter Server-Instanz zu beenden, können Sie diese vCenter Server-Instanz aus Ihrer vCloud Director-Installation entfernen.

Voraussetzungen

- Deaktivieren Sie die vCenter Server-Instanz. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren einer vCenter Server-Instanz](#).
- Löschen Sie alle virtuellen Provider-Datencenter, die Ressourcenpools aus dieser vCenter Server-Instanz verwenden. Weitere Informationen finden Sie unter [Löschen eines virtuellen Provider-Datencenters](#).

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der vCenter Server-Zielinstanz und klicken Sie auf **Registrierung aufheben**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Bearbeiten der NSX Manager-Einstellungen

Wenn die Verbindungseinstellungen für eine registrierte NSX Manager-Instanz geändert werden oder wenn Sie den Namen und die Beschreibung der Instanz in vCloud Director ändern möchten, können Sie diese Einstellungen bearbeiten.

Sie können die Einstellungen ändern, die Sie beim Hinzufügen der NSX Manager-Instanz konfiguriert haben. Weitere Informationen finden Sie unter [\(Optional\) Hinzufügen der verknüpften NSX Manager-Instanz](#).

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter** und klicken Sie auf den Namen der vCenter Server-Instanz, die der NSX Manager-Zielinstanz zugeordnet ist.
- 3 Klicken Sie in der oberen rechten Ecke des Abschnitts **Info zu NSX-V Manager** auf **Bearbeiten**.
- 4 Bearbeiten Sie die vCenter Server-Einstellungen und klicken Sie auf **Speichern**.

Bearbeiten der NSX-T Manager-Einstellungen

Wenn die Verbindungseinstellungen für eine registrierte NSX-T Manager-Instanz geändert werden oder wenn Sie den Namen und die Beschreibung der Instanz in vCloud Director ändern möchten, können Sie diese Einstellungen bearbeiten.

Sie können die Einstellungen ändern, die Sie beim Hinzufügen der vCenter Server-Instanz konfiguriert haben. Weitere Informationen finden Sie unter [Registrieren einer NSX-T Manager-Instanz](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **NSX-T Manager** und klicken Sie dann auf den Namen der NSX-T Manager-Instanz, die Sie ändern möchten.
- 3 Klicken Sie in der oberen rechten Ecke der Registerkarte **Allgemein** auf **Bearbeiten**.
- 4 Bearbeiten Sie die NSX-T Manager-Einstellungen und klicken Sie auf **Speichern**.


Löschen einer NSX-T Manager-Instanz

Um die Verwendung der Ressourcen einer NSX-T Manager-Instanz zu beenden, können Sie diese vCenter Server-Instanz aus Ihrer vCloud Director-Installation entfernen.

Voraussetzungen

Löschen Sie alle virtuellen Provider-Datencenter, die Ressourcen aus dieser NSX-T Manager-Instanz verwenden. Weitere Informationen finden Sie unter [Löschen eines virtuellen Provider-Datencenters](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **NSX-T Manager**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der NSX-T Manager-Instanz, die Sie entfernen möchten, und klicken Sie auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **Löschen**.

Ressourcenlisten für mehrere Standorte

Wenn Sie mit vCloud Director-Bereitstellungen an mehreren Standorten arbeiten, können Sie Ressourcenlisten anzeigen, die Informationen zu Objekten von allen verbundenen Sites enthalten.

Um das Navigieren durch vSphere und Cloud-Ressourcen vom Service Provider Admin Portal aus zu erleichtern, gibt es ab Version 9.7 in vCloud Director Ressourcenlisten für mehrere Standorte.

Sie können auf die Ressourcenlisten über die Menüs **vSphere-Ressourcen** und **Cloud-Ressourcen** zugreifen.

Sie können auf detaillierte Informationen zu Objekten von den verschiedenen Sites zugreifen und auch Objekte auf der lokalen Site und auf Remote-Sites erstellen.

vSphere-Ressourcenlisten für mehrere Standorte werden für vCenter Server-Instanzen, NSX-T Manager-Instanzen, Ressourcenpools, Datenspeicher, Hosts, Distributed Switches, Portgruppen, isolierte Elemente und Speicherrichtlinien unterstützt.

Cloud-Ressourcenlisten für mehrere Standorte werden für Organisations-VDCs, Organisations-VDC-Vorlagen, Anbieter-VDCs, Cloud-Zellen, Edge-Gateways, externe Netzwerke und Netzwerkpools unterstützt.

Hinweis Multisite-Organisationslisten werden nicht unterstützt.

Verwalten von virtuellen Provider-Datencentern

4

Wenn Sie ein virtuelles Provider-Datencenter erstellt haben, können Sie seine Eigenschaften ändern, das virtuelle Datencenter deaktivieren oder löschen sowie seine Speicherrichtlinien und Ressourcenpools verwalten.

Um ein virtuelles Provider-Datencenter zu erstellen, müssen Sie entweder die vCloud Director Web Console oder die vCloud API verwenden. Informationen zur Verwendung der vCloud Director Web Console finden Sie im *vCloud Director-Administratorhandbuch*. Informationen zur Verwendung der vCloud API finden Sie im *vCloud API-Programmierhandbuch für Dienstleister*.

Dieses Kapitel enthält die folgenden Themen:


- [Aktivieren oder Deaktivieren eines virtuellen Provider-Datencenters](#)
- [Löschen eines virtuellen Provider-Datencenters](#)
- [Bearbeiten der allgemeinen Einstellungen eines virtuellen Provider-Datencenters](#)
- [Zusammenführen von virtuellen Provider-Datencentern](#)
- [Anzeigen der virtuellen Organisations-Datencenter eines virtuellen Provider-Datencenters](#)
- [Anzeigen der Datenspeicher in einem virtuellen Provider-Datencenter](#)
- [Anzeigen der externen Netzwerke in einem virtuellen Provider-Datencenter](#)
- [Verwalten der VM-Speicherrichtlinien auf einem virtuellen Provider-Datencenter](#)
- [Verwalten der Ressourcenpools in einem virtuellen Provider-Datencenter](#)
- [Bearbeiten der Metadaten für ein virtuelles Provider-Datencenter](#)

Aktivieren oder Deaktivieren eines virtuellen Provider-Datencenters

Um alle vorhandenen Organisations-VDCs, die die Ressourcen eines virtuellen Provider-Datencenters verwenden, zu deaktivieren, können Sie dieses virtuelle Provider-Datencenter deaktivieren. Sie können keine virtuellen Organisations-Datencenter erstellen, die die Ressourcen eines deaktivierten virtuellen Provider-Datencenters verwenden.

Laufende vApps und eingeschaltete virtuelle Maschinen werden weiterhin in den vorhandenen virtuellen Organisations-Datencentern ausgeführt, die von diesem Provider-VDC unterstützt werden, aber Sie können keine zusätzlichen vApps oder virtuellen Maschinen erstellen oder starten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des virtuellen Provider-Datencenters auf dem Ziel und klicken Sie auf **Aktivieren** oder **Deaktivieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Löschen eines virtuellen Provider-Datencenters


Um die Ressourcen eines virtuellen Provider-Datencenters aus vCloud Director zu entfernen, können Sie dieses virtuelle Provider-Datencenter löschen.

Die zugrunde liegenden Ressourcen in vSphere bleiben hiervon unberührt.

Voraussetzungen

- Deaktivieren Sie das virtuelle Provider-Datencenter auf dem Ziel. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren eines virtuellen Provider-Datencenters](#).
- Löschen Sie alle Organisations-VDCs, die Ressourcen aus diesem virtuellen Provider-Datencenter verwenden. Weitere Informationen finden Sie unter [Löschen eines virtuellen Organisations-Datencenters](#).


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des virtuellen Provider-Datencenters, das Sie entfernen möchten, und klicken Sie auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Bearbeiten der allgemeinen Einstellungen eines virtuellen Provider-Datencenters

Sie können den Namen und die Beschreibung eines virtuellen Provider-Datencenters ändern. Wenn der unterstützende Ressourcenpool eine höhere virtuelle Hardwareversion unterstützt, können Sie ein Upgrade auf die höchste virtuelle Hardware durchführen, die von einem virtuellen Provider-Datencenter unterstützt wird.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und klicken Sie auf den Namen des virtuellen Provider-Datencenters, das Sie ändern möchten.
- 3 Klicken Sie auf der Registerkarte **Konfigurieren > Allgemein** in der oberen rechten Ecke auf **Bearbeiten**.
- 4 (Optional) Ändern Sie den Namen und die Beschreibung des virtuellen Provider-Datencenters.
- 5 (Optional) Wählen Sie im Dropdown-Menü die höchste Hardwareversion aus, die von diesem virtuellen Provider-Datencenter unterstützt wird, und klicken Sie auf **Speichern**.

Die höchste Version, die Sie auswählen können, hängt von den ESXi-Hosts im Ressourcenpool ab, die das virtuelle Provider-Datencenter stützen.

Hinweis Sie können nur ein Upgrade der von einem virtuellen Provider-Datencenter unterstützten Hardwareversion durchführen. Sie können kein Downgrade der Hardwareversion durchführen.

- 6 Klicken Sie auf **Speichern**.


Zusammenführen von virtuellen Provider-Datencentern

Um die Ressourcen von zwei virtuellen Provider-Datencentern zu kombinieren, können Sie diese virtuellen Provider-Datencenter in einem einzigen virtuellen Provider-Datencenter zusammenführen.

Voraussetzungen

- Die Provider-VDCs im Ziel gehören zur selben Site.
- Die Provider-VDCs im Ziel enthalten nur elastische Organisations-VDCs.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des virtuellen Provider-Datencenters, das Sie entfernen möchten, und klicken Sie auf **Zusammenführen**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen des virtuellen Provider-Datencenters, mit dem die Ressourcen zusammengeführt werden sollen, und klicken Sie auf **Zusammenführen**.

Anzeigen der virtuellen Organisations-Datencenter eines virtuellen Provider-Datencenters

Sie können eine Liste der virtuellen Organisations-Datencenter anzeigen, die Ressourcen aus einem virtuellen Provider-Datencenter verwenden.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Organisations-VDCs**.

Ergebnisse

Die Liste der virtuellen Organisations-Datencenter, die die Ressourcen aus diesem Provider-VDC nutzen, wird angezeigt. Für jedes Organisations-VDC enthält die Liste Informationen zu Status, Zustand, Zuweisungsmodell, Organisation, vCenter Server-Instanz, Anzahl der Netzwerke, Anzahl der vApps, Anzahl der Speicherrichtlinien und Anzahl der Ressourcenpools.


Nächste Schritte

- Sie können die Ansicht des virtuellen Organisations-Datencenters im vCloud Director Tenant Portal durch Klicken auf das **Pop-out**-Symbol () neben dem Namen des gewünschten virtuellen Organisations-Datencenters aufrufen.
- Durch Klicken auf das Optionsfeld neben dem Namen eines virtuellen Organisations-Datencenters können Sie Verwaltungsvorgänge durchführen, die den in [Kapitel 6 Verwalten von virtuellen Organisations-Datencentern](#) beschriebenen Vorgängen ähneln.

Anzeigen der Datenspeicher in einem virtuellen Provider-Datencenter

Sie können Details zu den Datenspeichern anzeigen, die die Speicherkapazität für ein virtuelles Provider-Datencenter bereitstellen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Datenspeicher**.


Eine Liste aller Datenspeicher im virtuellen Provider-Datencenter wird angezeigt. Die Liste enthält die folgenden Informationen für jeden Datenspeicher.

Titel	Beschreibung
Name	Der Name des Datenspeichers
Zustand	Aktiviert oder deaktiviert
Typ	Der Typ des vom Datenspeicher verwendeten Dateisystems, entweder Virtual Machine File System (VMFS) oder Network File System (NFS).
Genutzt	Der durch Dateien von virtuellen Maschinen (einschließlich Protokolldateien, Snapshots und den virtuellen Festplatten) belegte Speicherplatz im Datenspeicher. Wenn eine virtuelle Maschine eingeschaltet ist, sind im belegten Speicherplatz auch Protokolldateien berücksichtigt.
Bereitgestellt	Der Speicherplatz im Datenspeicher, der virtuellen Maschinen gesichert zur Verfügung steht. Wenn virtuelle Maschinen Thin Provisioning verwenden, wird ein Teil des bereitgestellten Platzes möglicherweise nicht verwendet und andere virtuelle Maschinen können über diesen ungenutzten Platz verfügen. Dieser Wert kann größer als die tatsächliche Datenspeicherkapazität sein, wenn Thin Provisioning verwendet wird.
Angeforderter Speicher	<p>Bereitgestellter Speicherplatz, der nur von vCloud Director-Objekten im Datenspeicher verwendet wird. Dazu gehören:</p> <ul style="list-style-type: none"> ■ In vCloud Director bereitgestellte virtuelle Maschinen ■ Katalogelemente (Vorlagen und Mediendateien) ■ NSX Edges ■ Verwendete und nicht verwendete Anforderungen an die Arbeitsspeicherauslagerung für virtuelle Maschinen <p>Dieser Wert umfasst nicht den von Schatten-VMs oder Zwischenfestplatten angeforderten Speicherplatz in einer verknüpften Klonstruktur.</p>
vCenter	Die dem Datenspeicher zugeordnete vCenter Server-Instanz.

Anzeigen der externen Netzwerke in einem virtuellen Provider-Datencenter

Sie können eine Liste der externen Netzwerke anzeigen, auf die ein virtuelles Provider-Datencenter zugreifen kann.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.

3 Klicken Sie auf die Registerkarte **Externe Netzwerke**.

Ergebnisse

Sie können eine Liste der verfügbaren externen Netzwerke mit Informationen zu den Gateway-CIDR-Einstellungen und der IP-Poolnutzung anzeigen.

Verwalten der VM-Speicherrichtlinien auf einem virtuellen Provider-Datencenter

Sie können VM-Speicherrichtlinien für ein virtuelles Provider-Datencenter hinzufügen, aktivieren, deaktivieren und entfernen. Sie können auch Metadaten für eine VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter hinzufügen, bearbeiten und löschen.

Hinzufügen einer VM-Speicherrichtlinie zu einem virtuellen Provider-Datencenter


Sie können eine VM-Speicherrichtlinie einem virtuellen Provider-Datencenter hinzufügen. Danach können Sie zur Unterstützung der hinzugefügten Speicherrichtlinie von diesem virtuellen Provider-Datencenter gestützte virtuelle Organisations-Datencenter konfigurieren.

Wichtig vCloud Director unterstützt keine VM-Speicherrichtlinien für hostbasierte Datendienste wie Verschlüsselung und Storage I/O Control.

Voraussetzungen

- Ihr vSphere-Administrator hat die Ziel-VM-Speicherrichtlinie erstellt. Weitere Informationen zur speicherrichtlinienbasierten Verwaltung (Storage Policy Based Management – SPBM) finden Sie in der *vSphere Storage*-Dokumentation.
- [Aktualisieren der Speicherrichtlinien einer vCenter Server-Instanz](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf der Registerkarte **Speicherrichtlinien** auf **Hinzufügen**.
- 4 Wählen Sie eine oder mehrere Speicherrichtlinien aus, die Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**.

Wenn Sie * **(Alle)** auswählen, fügt vCloud Director dynamisch Datenspeicher hinzu oder entfernt sie, wenn Datenspeicher zu den Datenspeicher-Clustern des virtuellen Provider-Datencenters hinzugefügt bzw. daraus entfernt werden.


Nächste Schritte

Konfigurieren Sie virtuelle Organisations-Datencenter, die vom virtuellen Provider-Datencenter gestützt werden, damit die Speicherrichtlinie unterstützt wird. Weitere Informationen finden Sie unter [Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC](#).

Aktivieren oder Deaktivieren einer VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter

Nachdem Sie eine VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter deaktiviert haben, können dessen Organisations-VDCs diese VM-Speicherrichtlinie nicht mehr verwenden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Speicherrichtlinien**.
- 4 Klicken Sie auf das Optionsfeld neben der Ziel-VM-Speicherrichtlinie und klicken Sie dann auf **Aktivieren** oder **Deaktivieren**.
- 5 Klicken Sie zur Bestätigung auf **OK**.


Löschen einer VM-Speicherrichtlinie aus einem virtuellen Provider-Datencenter

Sie können eine VM-Speicherrichtlinie aus einem virtuellen Provider-Datencenter löschen.

Voraussetzungen

Deaktivieren Sie die Ziel-VM-Speicherrichtlinie. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren einer VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter](#).

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Speicherrichtlinien**.
- 4 Klicken Sie auf das Optionsfeld neben der Ziel-VM-Speicherrichtlinie und klicken Sie auf **Entfernen**.
- 5 Klicken Sie zur Bestätigung auf **Entfernen**.

Bearbeiten der Metadaten für eine VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter

Sie können Metadaten für eine Speicherrichtlinie in einem virtuellen Provider-Datencenter hinzufügen, bearbeiten und löschen.

Mithilfe von Objektmetadaten können Sie benutzerdefinierte *Namen=Wert*-Paare mit einer Speicherrichtlinie in einem Provider-VDC verknüpfen. Sie können Objektmetadaten in Filterausdrücken der vCloud-API-Abfrage verwenden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Speicherrichtlinien**.
- 4 Klicken Sie auf das Optionsfeld neben der Ziel-VM-Speicherrichtlinie und anschließend auf **Metadaten**.
- 5 Klicken Sie auf **Bearbeiten**.
- 6 (Optional) Um ein Schlüssel-Wert-Paar hinzuzufügen, klicken Sie auf **Hinzufügen**, geben Sie einen Namen und einen Wert ein und wählen Sie einen Typ für das neue Schlüssel-Wert-Paar aus.
- 7 (Optional) Um ein Schlüssel-Wert-Paar zu bearbeiten, geben Sie einen neuen Namen und einen Wert ein und wählen Sie einen neuen Typ für das Schlüssel-Wert-Paar aus.
- 8 (Optional) Um ein Schlüssel-Wert-Paar zu entfernen, klicken Sie am rechten Ende der Zeile auf das Symbol **Löschen**.
- 9 Klicken Sie auf **Speichern** und dann auf **OK**.

Verwalten der Ressourcenpools in einem virtuellen Provider-Datencenter

Sie können sekundäre Ressourcenpools in einem virtuellen Provider-Datencenter hinzufügen, aktivieren, deaktivieren und trennen. Der primäre Ressourcenpool in einem virtuellen Provider-Datencenter kann nicht deaktiviert oder getrennt werden.

Hinzufügen eines Ressourcenpools zu einem virtuellen Provider-Datencenter

Sie können einem virtuellen Provider-Datencenter mindestens einen sekundären Ressourcenpool hinzufügen, sodass die virtuellen Datencenter der Organisation für die nutzungsbasierte Bezahlung (Pay-As-You-Go) und den Zuweisungspool erweitert werden können.


Wenn Rechenressourcen von mehreren Ressourcenpools gestützt werden, können sie für weitere virtuelle Maschinen erweitert werden.

Sie können Ressourcenpools hinzufügen, die von vSphere-Clustern, die optimal für das Hosten von NSX Edges mit VLAN-Uplinks konfiguriert sind, gestützt werden. vCloud Director kann Metadaten verwenden, um anzugeben, dass das System Organisations-VDC-Edge-Gateways in Ressourcenpools ablegen muss, denen diese Cluster zugrunde liegen. Weitere Informationen finden Sie im VMware Knowledgebase-Artikel <https://kb.vmware.com/kb/2151398>.

Voraussetzungen

Ihr vSphere-Administrator hat den sekundären Ziel-Ressourcenpool in der vCenter Server-Instanz erstellt, die den primären Ressourcenpool des virtuellen Provider-Datencenters stützt.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf der Registerkarte **Ressourcenpools** auf **Hinzufügen**.
- 4 Wählen Sie mindestens einen hinzuzufügenden Ressourcenpool aus und klicken Sie auf **Hinzufügen**.

Ergebnisse

vCloud Director fügt den Ressourcenpool hinzu, der vom virtuellen Provider-Datencenter verwendet werden soll, sodass alle von diesem virtuellen Provider-Datencenter gestützten virtuellen Organisations-Datencenter nach dem Pay-As-You-Go- und Zuweisungspool-Modell elastisch werden.

vCloud Director fügt außerdem einen System-VDC-Ressourcenpool unter dem neuen Ressourcenpool hinzu. Dieser Ressourcenpool wird für die Erstellung von Systemressourcen verwendet, wie z. B. NSX Edge-VMs und virtuellen Maschinen, die als Vorlage für verknüpfte Klone fungieren.

Wichtig Bearbeiten und löschen Sie den System-VDC-Ressourcenpool nicht.


Aktivieren oder Deaktivieren eines Ressourcenpools in einem virtuellen Provider-Datencenter

Wenn Sie einen Ressourcenpool deaktivieren, sind die Speicher- und Rechenressourcen des Ressourcenpools nicht mehr für das virtuelle Provider-Datencenter verfügbar.

Bei Prozessen, die bereits ausgeführt werden, wird die Verwendung von Ressourcen aus dem deaktivierten Ressourcenpool nicht beendet.

Hinweis Der primäre Ressourcenpool in einem virtuellen Provider-Datencenter kann nicht deaktiviert werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Ressourcenpools**.
- 4 Klicken Sie auf das Optionsfeld neben dem Zielressourcenpool und klicken Sie auf **Aktivieren** oder **Deaktivieren**.
- 5 Klicken Sie zur Bestätigung auf **OK**.


Trennen eines Ressourcenpools von einem virtuellen Provider-Datencenter

Wenn ein virtuelles Provider-Datencenter über mehr als einen Ressourcenpool verfügt, können Sie einen sekundären Ressourcenpool vom virtuellen Provider-Datencenter trennen. Der primäre Ressourcenpool kann nicht vom virtuellen Provider-Datencenter getrennt werden.

Voraussetzungen

- Deaktivieren Sie den gewünschten Ressourcenpool im virtuellen Provider-Datencenter. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren eines Ressourcenpools in einem virtuellen Provider-Datencenter](#).
- Migrieren Sie alle virtuellen Maschinen von diesem Ressourcenpool zu einem aktivierten Ressourcenpool. Informationen zum Migrieren von virtuellen Maschinen zwischen Ressourcenpools in einem virtuellen Provider-Datencenter finden Sie im *vCloud Director-Administratorhandbuch*.
- Stellen Sie alle Netzwerke, die von dem deaktivierten Ressourcenpool betroffen sind, erneut bereit.
- Stellen Sie alle Edge-Gateways, die von dem deaktivierten Ressourcenpool betroffen sind, erneut bereit.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Ressourcenpools**.


- 4 Klicken Sie auf das Optionsfeld neben dem Zielressourcenpool und dann auf **Trennen**.
- 5 Klicken Sie zur Bestätigung auf **OK**.

Bearbeiten der Metadaten für ein virtuelles Provider-Datencenter

Sie können Metadaten für ein virtuelles Provider-Datencenter hinzufügen, bearbeiten und löschen.

Mithilfe von Objektmetadaten können Sie benutzerdefinierte *Namen=Wert*-Paare mit einem virtuellen Provider-Datencenter verknüpfen. Sie können Objektmetadaten in vCloud-API-Abfragefilterausdrücken verwenden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf der Registerkarte **Konfigurieren > Metadaten** in der oberen rechten Ecke auf **Bearbeiten**.
- 4 (Optional) Um ein Schlüssel-Wert-Paar hinzuzufügen, klicken Sie auf **Hinzufügen**, geben Sie einen Namen und einen Wert ein und wählen Sie einen Typ für das neue Schlüssel-Wert-Paar aus.
- 5 (Optional) Um ein Schlüssel-Wert-Paar zu bearbeiten, geben Sie einen neuen Namen und einen Wert ein und wählen Sie einen neuen Typ für das Schlüssel-Wert-Paar aus.
- 6 (Optional) Um ein Schlüssel-Wert-Paar zu entfernen, klicken Sie am rechten Ende der Zeile auf das Symbol **Löschen**.
- 7 Klicken Sie auf **Speichern** und dann auf **OK**.

Verwalten von Organisationen

5

Mithilfe des vCloud Director Service Provider Admin Portal können Sie vCloud Director-Organisationen erstellen, konfigurieren und verwalten.

Verwenden Sie das vCloud Director Service Provider Admin Portal zum Verwalten von Organisationen, Festlegen von Richtlinien zur Bestimmung des Ressourcenverbrauchs durch Benutzer in einer Organisation sowie zum Veröffentlichen und Freigeben von Katalogen.

Dieses Kapitel enthält die folgenden Themen:

- [Wissenswertes über Leases](#)
- [Erstellen einer Organisation](#)
- [Konfigurieren von Katalogen für eine Organisation](#)
- [Konfigurieren von Richtlinien für eine Organisation](#)

Wissenswertes über Leases

Beim Erstellen von Organisationen müssen u. a. Leases angegeben werden. Leases ermöglichen eine grundlegende Steuerung der Speicher- und Rechenressourcen, indem festgelegt wird, wie lange vApps maximal ausgeführt und wie lange vApps und vApp-Vorlagen gespeichert werden dürfen.

Der Zweck von Laufzeit-Leases besteht darin, zu verhindern, dass inaktive vApps Rechenressourcen verbrauchen. Wenn beispielsweise ein Benutzer eine vApp startet und anschließend verreist, ohne sie anzuhalten, verbraucht die vApp fortlaufend Ressourcen.

Eine Laufzeit-Lease beginnt zu dem Zeitpunkt, an dem der Benutzer eine vApp startet. Wenn die Laufzeit-Lease abläuft, hält vCloud Director die vApp an.


Der Zweck von Speicher-Leases besteht darin, zu verhindern, dass nicht verwendete vApps und vApp-Vorlagen Speicherressourcen verbrauchen. Eine vApp-Speicher-Lease beginnt zu dem Zeitpunkt, an dem der Benutzer eine vApp anhält. Speicher-Leases haben keine Auswirkungen auf ausgeführte vApps. Eine vApp-Vorlagen-Speicher-Lease beginnt, wenn der Benutzer die vApp-Vorlage einer vApp oder einem Arbeitsbereich hinzufügt oder sie herunterlädt, kopiert oder verschiebt.

Bei Ablauf der Speicher-Lease kennzeichnet vCloud Director die vApp bzw. vApp-Vorlage als abgelaufen oder löscht sie entsprechend den festgelegten Organisationsrichtlinien.

Erstellen einer Organisation

Sie können eine neue Organisation über das vCloud Director Service Provider Admin Portal erstellen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.

Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.
- 2 Zum Erstellen einer neuen Organisation klicken Sie auf die Schaltfläche **+Hinzufügen**.
Das Dialogfeld **Neue Organisation** wird geöffnet.
- 3 Geben Sie die folgenden Werte ein.


Option	Beschreibung
Name der Organisation	Der eindeutige Bezeichner, der die URL für den Zugriff auf das Mandantenportal der Organisation bildet.
Vollständiger Name der Organisation	Der vollständige Name der Organisation.
Beschreibung	Eine optionale Beschreibung für die Organisation.


- 4 Klicken Sie auf die Schaltfläche **Erstellen**, um den Erstellvorgang abzuschließen.

Konfigurieren von Katalogen für eine Organisation

Sie können die Vorgehensweise einer Organisation zur Freigabe von Dienstkatalogen konfigurieren.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.

Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.
- 2 Verwenden Sie die Listenleiste () auf der linken Seite jedes Elements, um die Aktionen anzuzeigen, die Sie für jede Organisation durchführen können.
- 3 Klicken Sie auf **Kataloge**.
Das Dialogfeld **Katalogeinstellungen** der Organisation wird geöffnet.

4 Konfigurieren Sie die folgenden Optionen für Freigabe und Veröffentlichung.

Option	Beschreibung
Gemeinsame Nutzung	Ermöglicht Organisationsadministratoren, Kataloge dieser Organisation für andere Organisationen in dieser Instanz von vCloud Director freizugeben. Wenn Sie diese Option nicht auswählen, können Organisationsadministratoren nach wie vor Kataloge innerhalb der Organisation freigeben.
Veröffentlichung in externen Katalogen zulassen	Ermöglicht Organisationsadministratoren, Kataloge für Organisationen außerhalb dieser Instanz von vCloud Director zu veröffentlichen.
Abonnieren von externen Katalogen zulassen	Ermöglicht Organisationsadministratoren, Kataloge außerhalb dieser Instanz von vCloud Director zu abonnieren.


Konfigurieren von Richtlinien für eine Organisation


Leases, Kontingente und Grenzwerte beschränken die Möglichkeit von Benutzern in der Organisation zur Nutzung von Speicher- und Prozessorressourcen. Bearbeiten Sie diese Einstellungen, um zu verhindern, dass einzelne Benutzer eine Ressource der Organisation erschöpfend oder ausschließlich nutzen.

Voraussetzungen

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

Verfahren

- Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.

Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.
- Verwenden Sie die Listenleiste () auf der linken Seite jedes Elements, um die Aktionen anzuzeigen, die Sie für jede Organisation durchführen können.
- Klicken Sie auf **Richtlinien**, um die Leases, Kontingente, Ressourcengrenzwerte und Kennwortrichtlinien für die Organisation zu bearbeiten.
- Konfigurieren Sie vApp-Leases mit den folgenden Einstellungen.

Option	Beschreibung
Maximaler Laufzeit-Lease	Gibt an, wie lange vApps ausgeführt werden können, bevor sie automatisch beendet werden.
Maximaler Speicher-Lease	Gibt an, wie lange beendete vApps verfügbar sind, bevor sie automatisch bereinigt werden.
Speicher bereinigen	Gibt an, wie vApps verarbeitet werden, nachdem sie beendet und bereinigt wurden.

5 Konfigurieren Sie Leases von vApp-Vorlagen mit den folgenden Einstellungen.

Option	Beschreibung
Maximaler Speicher-Lease	Gibt an, wie lange vApp-Vorlagen verfügbar sind, bevor sie automatisch bereinigt werden.
Speicher bereinigen	Gibt an, wie abgelaufene vApp-Vorlagen nach deren Bereinigung verarbeitet werden.

6 Konfigurieren Sie Kontingente mit den folgenden Einstellungen.

Option	Beschreibung
Kontingent aller VMs	Gesamtzahl der verfügbaren VMs, die ein Benutzer in dieser Organisation speichern kann.
Kontingent ausgeführter VMs	Gesamtzahl der VMs, die ein Benutzer in dieser Organisation einschalten kann.

7 Konfigurieren Sie Grenzwerte mit den folgenden Einstellungen.

Option	Beschreibung
Anzahl ressourcenintensiver Vorgänge pro Benutzer	Geben Sie die maximale Anzahl von gleichzeitigen ressourcenintensiven Vorgängen pro Benutzer an oder wählen Sie Systemgrenzwert übernehmen aus.
Anzahl ressourcenintensiver Vorgänge, die in die Warteschlange gestellt werden, pro Benutzer	Geben Sie die maximale Anzahl von ressourcenintensiven Vorgängen, die in die Warteschlange gestellt werden, pro Benutzer an oder wählen Sie Systemgrenzwert übernehmen aus.
Anzahl ressourcenintensiver Vorgänge pro Organisation	Geben Sie die maximale Anzahl von gleichzeitigen ressourcenintensiven Vorgängen pro Organisation an oder wählen Sie Systemgrenzwert übernehmen aus.
Anzahl ressourcenintensiver Vorgänge, die in die Warteschlange gestellt werden, pro Organisation	Geben Sie die maximale Anzahl von ressourcenintensiven Vorgängen, die in die Warteschlange gestellt werden, pro Organisation an oder wählen Sie Systemgrenzwert übernehmen aus.
Anzahl gleichzeitiger Verbindungen pro VM	Geben Sie die maximale Anzahl von gleichzeitigen Konsolenverbindungen pro virtueller Maschine an oder wählen Sie Systemgrenzwert übernehmen aus.
Anzahl virtueller Datacenter pro Organisation	Geben Sie die maximale Anzahl virtueller Datacenter pro Organisation ein oder wählen Sie Systemkontingent übernehmen aus.

8 Konfigurieren Sie Kennwortrichtlinien mit den folgenden Einstellungen.

Option	Beschreibung
Kontosperrung aktiviert	Benutzerkontosperrung wird nach mehreren ungültigen Anmeldeversuchen aktiviert.
Ungültige Anmeldungen vor der Sperrung	Anzahl der ungültigen Anmeldeversuche vor Sperrung des Benutzerkontos.
Kontosperrungsintervall	Der Zeitraum, während dessen ein gesperrtes Benutzerkonto nicht angemeldet werden kann.

Verwalten von virtuellen Organisations-Datencentern

6

Um Ressourcen für eine Organisation bereitzustellen, erstellen Sie ein oder mehrere virtuelle Organisations-Datencenter für diese Organisation. Nachdem Sie ein virtuelles Organisations-Datencenter erstellt haben, können Sie seine Eigenschaften bearbeiten, das virtuelle Datencenter deaktivieren oder löschen sowie sein Zuweisungsmodell, den Speicher und die Netzwerkeinstellungen verwalten.

Dieses Kapitel enthält die folgenden Themen:

- Funktionsweise von Zuweisungsmodellen
- Grundlegendes zu Computing-Richtlinien
- Erstellen eines virtuellen Organisations-Datencenters
- Aktivieren oder Deaktivieren eines virtuellen Organisations-Datencenters
- Löschen eines virtuellen Organisations-Datencenters
- Ändern des Namens und der Beschreibung eines virtuellen Organisations-Datencenters.
- Ändern der Zuweisungsmodelleinstellungen eines virtuellen Organisations-Datencenters
- Ändern der Speichereinstellungen eines virtuellen Organisations-Datencenters
- Bearbeiten der Netzwerkeinstellungen eines Organisations-VDCs
- Ändern der Metadaten für ein virtuelles Organisations-Datencenter
- Anzeigen der Ressourcenpools eines virtuellen Organisations-Datencenters
- Verwalten der Distributed Firewall in einem virtuellen Organisations-Datencenter

Funktionsweise von Zuweisungsmodellen

Ein Zuweisungsmodell legt fest, wie und wann die zugewiesenen VDC-Computing- und Arbeitsspeicherressourcen des virtuellen Provider-Datencenters (VDC) an das Organisations-VDC übergeben werden.

Die folgende Tabelle zeigt die vSphere-Einstellungen für die Ressourcenverteilung auf der VM- oder Ressourcenpoolebene basierend auf dem Zuweisungsmodell des Organisations-VDC.

	Flex-Zuweisungsmodell	Elastisches Zuweisungspool-Modell	Nicht elastisches Zuweisungspool-Modell	Pay-As-You-Go-Modell	Reservierungspool-Modell
Elastisch	Basierend auf der Organisations-VDC-Konfiguration.	Ja	Nein	Ja	Nein
vCPU-Geschwindigkeit	Wenn ein VM-CPU-Grenzwert in einer VDC-Computing-Richtlinie nicht definiert ist, kann sich die vCPU-Geschwindigkeit auf den CPU-Grenzwert der VM innerhalb des VDC auswirken.	Auswirkungen auf die Anzahl der laufenden vCPUs im Organisations-VDC.	Nicht anwendbar	Auswirkungen auf den VM-CPU-Grenzwert	Nicht anwendbar
CPU-Grenzwert des Ressourcenpools	CPU-Grenzwert des Organisations-VDC, aufgeteilt basierend auf der Anzahl der VMs im Ressourcenpool.	CPU-Zuweisung des Organisations-VDC	CPU-Zuweisung des Organisations-VDC	Unbegrenzt	CPU-Zuweisung des Organisations-VDC
Ressourcenpool-CPU-Reservierung	Die CPU-Reservierung des Organisations-VDC wird basierend auf der Anzahl der VMs im Ressourcenpool aufgeteilt. Die CPU-Reservierung des Organisations-VDC entspricht der CPU-Zuweisung des Organisations-VDC multipliziert mit der CPU-Garantie.	Summe der eingeschalteten VMs, entspricht der CPU-Garantie multipliziert mit der vCPU-Geschwindigkeit und mit der Anzahl der vCPUs.	CPU-Zuweisung des Organisations-VDC multipliziert mit der CPU-Garantie	Keine, erweiterbar	CPU-Zuweisung des Organisations-VDC
Arbeitsspeichergrenzwert für Ressourcenpool	Der Arbeitsspeichergrenzwert des Organisations-VDC wird basierend auf der Anzahl der VMs im Ressourcenpool aufgeteilt.	Unbegrenzt	RAM-Zuweisung des Organisations-VDC	Unbegrenzt	RAM-Zuweisung des Organisations-VDC

	Flex-Zuweisungsmodell	Elastisches Zuweisungspool-Modell	Nicht elastisches Zuweisungspool-Modell	Pay-As-You-Go-Modell	Reservierungspool-Modell
Arbeitsspeicherreservierung für Ressourcenpool	Die RAM-Reservierung des Organisations-VDC wird basierend auf der Anzahl der VMs im Ressourcenpool aufgeteilt. Die RAM-Reservierung des Organisations-VDC entspricht der RAM-Zuweisung des VDC multipliziert mit der RAM-Garantie.	Summe der RAM-Garantie multipliziert mit dem vRAM aller eingeschalteten VMs im Ressourcenpool. Die RAM-Reservierung des Ressourcenpools ist erweiterbar.	RAM-Zuweisung des Organisations-VDC multipliziert mit der RAM-Garantie	Keine, erweiterbar	RAM-Zuweisung des Organisations-VDC
VM-CPU-Grenzwert	Basierend auf der VDC-Computing-Richtlinie der VM.	Unbegrenzt	Unbegrenzt	vCPU-Geschwindigkeit multipliziert mit der Anzahl der vCPUs	Benutzerdefiniert
CPU-Reservierung der VM	Basierend auf der VDC-Computing-Richtlinie der VM.	0	0	Entspricht der CPU-Geschwindigkeit multipliziert mit der vCPU-Geschwindigkeit und der Anzahl der vCPUs.	Benutzerdefiniert
VM-RAM-Grenzwert	Basierend auf der VDC-Computing-Richtlinie der VM.	Unbegrenzt	Unbegrenzt	vRAM	Benutzerdefiniert
VM-RAM-Reservierung	Basierend auf der VDC-Computing-Richtlinie der VM.	0	Entspricht dem vRAM multipliziert mit der RAM-Garantie plus RAM-Overhead.	Entspricht dem vRAM multipliziert mit der RAM-Garantie plus RAM-Overhead.	Benutzerdefiniert

Vorgeschlagene Verwendung der Zuweisungsmodelle

Jedes Zuweisungsmodell kann für verschiedene Ebenen der Leistungssteuerung und -verwaltung verwendet werden.

Die folgende Tabelle enthält Informationen über die vorgeschlagene Verwendung jedes Zuweisungsmodells.

Zuweisungsmodell	Vorgeschlagene Verwendung
Flex-Zuweisungsmodell	Mit dem Flex-Zuweisungsmodell können Sie eine differenzierte Leistungssteuerung auf der Arbeitslastebene erreichen. Mithilfe des Flex-Zuweisungsmodells können vCloud Director- Systemadministratoren die Elastizität der einzelnen Organisations-VDCs verwalten. Das Flex-Zuweisungsmodell verwendet die richtlinienbasierte Verwaltung von Arbeitslasten. Mit dem Flex-Zuweisungsmodell können Cloud-Anbieter den Arbeitsspeicher-Overhead in einem Organisations-VDC besser steuern und eine strenge Burst-Kapazitätsnutzung für Mandanten erzwingen.
Zuweisungspool-Zuweisungsmodell	Verwenden Sie das Zuweisungspool-Zuweisungsmodell für langlebige, stabile Arbeitslasten, bei denen Mandanten eine feste Computing-Ressourcennutzung abonnieren und Cloud-Anbieter die Computing-Ressourcenkapazität im Voraus planen und verwalten können. Das Zuweisungspool-Zuweisungsmodell ist optimal für Arbeitslasten mit unterschiedlichen Leistungsanforderungen. Beim Zuweisungspool-Zuweisungsmodell nutzen alle Arbeitslasten die zugewiesenen Ressourcen aus den Ressourcenpools von vCenter Server gemeinsam. Unabhängig davon, ob Sie die Elastizität aktivieren oder deaktivieren, erhalten Mandanten eine begrenzte Menge an Computing-Ressourcen. Mit dem Zuweisungspool-Zuweisungsmodell aktivieren oder deaktivieren Cloud-Anbieter die Elastizität auf Systemebene. Die Einstellung gilt für alle Organisations-VDCs des Zuweisungspools. Wenn Sie die nicht elastische Zuweisungspool-Zuweisung verwenden, reserviert das Organisations-VDC vorab den VDC-Ressourcenpool und Mandanten können vCPUs, aber keinen Arbeitsspeicher überbelegen. Wenn Sie die elastische Poolzuweisung verwenden, reserviert das Organisations-VDC keine Computing-Ressourcen vorab und die Kapazität kann sich über mehrere Cluster erstrecken. Cloud-Anbieter verwalten die Überbelegung von physischen Computing-Ressourcen, und Mandanten können vCPUs und Arbeitsspeicher nicht überbelegen.
Pay-As-You-Go	Verwenden Sie das Pay-As-You-Go-Modell, wenn Sie Computing-Ressourcen nicht im Voraus in vCenter Server zuweisen müssen. Reservierungen, Grenzwerte und Anteile werden auf jede Arbeitslast angewendet, die Mandanten im VDC bereitstellen. Mit dem Pay-As-You-Go-Zuweisungsmodell erhält jede Arbeitslast im Organisations-VDC denselben Prozentsatz der konfigurierten Computing-Ressourcen, die reserviert sind. Für vCloud Director ist die CPU-Geschwindigkeit aller vCPUs für jede Arbeitslast gleich und Sie können die CPU-Geschwindigkeit nur auf der Organisations-VDC-Ebene definieren. Aus Sicht der Leistung werden die Arbeitslasten gleich behandelt, da die Reservierungseinstellungen einzelner Arbeitslasten nicht geändert werden können. Das Pay-As-You-Go-Zuweisungsmodell ist optimal für Mandanten, die Arbeitslasten mit unterschiedlichen Leistungsanforderungen zur Ausführung innerhalb desselben Organisations-VDC benötigen. Aufgrund der Elastizität ist das Pay-As-You-Go-Modell für generische, kurzlebige Arbeitslasten geeignet, die zu selbstskalierenden Anwendungen gehören. Bei Pay-As-You-Go können Mandanten Spitzen im Computing-Ressourcenbedarf innerhalb eines Organisations-VDC handhaben.
Reservierungspool	Verwenden Sie das Reservierungspool-Zuweisungsmodell, wenn Sie eine differenzierte Kontrolle über die Leistung von Arbeitslasten benötigen, die im Organisations-VDC ausgeführt werden. Aus Sicht des Cloud-Anbieters erfordert das Reservierungspool-Zuweisungsmodell eine Vorabzuweisung aller Computing-Ressourcen in vCenter Server. Das Reservierungspool-Zuweisungsmodell ist nicht elastisch. Das Reservierungspool-Zuweisungsmodell eignet sich optimal für Arbeitslasten, die auf Hardware ausgeführt werden, die für einen bestimmten Mandanten vorgesehen ist. In solchen Fällen können Mandantenbenutzer die Nutzung und die Überbelegung von Computing-Ressourcen verwalten.

Flex-Zuweisungsmodell

Ab vCloud Director 9.7 können **Systemadministratoren** virtuelle Organisations-Datencenter (VDC) unter Verwendung des Flex-Zuweisungsmodells erstellen. Mit der Kombination aus Flex-Zuweisung und VDC-Computing-Richtlinien können **Systemadministratoren** die CPU- und RAM-Nutzung sowohl auf VDC-Ebene als auch auf der Ebene der einzelnen virtuellen Maschine (VM)

steuern. Das Flex-Zuweisungsmodell unterstützt alle Zuweisungskonfigurationen, die in den vorhandenen Zuweisungsmodellen verfügbar sind.

Wenn Sie ein nicht-Flex-Organisations-VDC in vCloud Director 9.7 erstellen, können Sie das Organisations-VDC für die Verwendung des Flex-Zuweisungsmodells neu konfigurieren. Wenn ein Organisations-VDC mit einer vCloud Director-Version vor 9.7 erstellt wird, können Sie die Organisations-Datencenter nicht neu konfigurieren, um das Flex-Zuweisungsmodell zu verwenden.

Beim Erstellen eines Flex-Organisations-VDC steuern die **Systemadministratoren** die folgenden Attribute des Organisations-VDC:

- Aktivieren oder deaktivieren Sie die Funktion des elastischen Pools.
- Arbeitsspeicher-Overhead ein- oder ausschließen.
- Geben Sie eine Standard-VDC-Computing-Richtlinie für das Organisations-VDC an.
- Arbeitsspeicher- und CPU-Zuweisung und Garantie
- Netzwerkkontingent
- Speicherprofil

Als **vCloud Director-Systemadministrator** können Sie ein Flex-Organisations-VDC als elastisch oder nicht elastisch konfigurieren. Wenn für Flex-Organisations-VDCs die elastische Poolfunktion aktiviert ist, umfasst und nutzt das Organisations-VDC alle Ressourcenpools, die mit seinem Provider-VDC verknüpft sind. Wenn Sie in vCloud Director 9.7 ein nicht elastisches Organisations-VDC in ein elastisches Organisations-VDC konvertieren, können Sie dasselbe Organisations-VDC nicht wieder in ein nicht elastisches zurückkonvertieren.

Das Flex-Zuweisungsmodell unterstützt die Funktionen von Organisations-VDC-Computing-Richtlinien und weist keine der Einschränkungen anderer Zuweisungsmodelle auf. Im Flex-Zuweisungsmodell hängt die VM-Computing-Ressourcenzuweisung von den Organisations-VDC-Computing-Richtlinien ab. Wenn Sie keine VDC-Computing-Richtlinie für ein Organisations-VDC definieren, hängt die Zuweisung der Computing-Ressourcen vom Organisations-VDC-Zuweisungsmodell ab. Unter Verwendung der Kombination aus dem Flex-Zuweisungsmodell und den Computing-Richtlinien des Organisations-VDC kann ein einzelnes Organisations-VDC VMs aufnehmen, die eine allen anderen Zuweisungsmodellen gemeinsame Konfiguration verwenden. Weitere Informationen finden Sie unter [Grundlegendes zu Computing-Richtlinien](#).

Um ein Flex-Organisations-VDC zu erstellen, können Sie das vCloud Director Service Provider Admin Portal oder die vCloud API verwenden. Informationen zur vCloud-API finden Sie unter *vCloud API-Programmierhandbuch für Dienstleister*.

Zuweisungspool-Zuweisungsmodell

Mit dem Zuweisungspool-Zuweisungsmodell wird ein Prozentsatz der Ressourcen, die Sie aus dem Provider-VDC zuweisen, dem Organisations-VDC zugesichert. Sie können den Prozentsatz für CPU und Arbeitsspeicher angeben. Dieser Prozentsatz wird als Faktor für den garantierten Prozentsatz bezeichnet. Hiermit können Sie Ressourcen überbelegen.

Ab vCloud Director 5.1.2 können Systemadministratoren Organisations-VDCs mit Zuweisungspool so konfigurieren, dass sie elastisch oder nicht elastisch sind. Elastizität ist eine globale Einstellung, die alle Organisations-VDCs mit Zuweisungspool betrifft. Informationen zum Ändern allgemeiner Systemeinstellungen finden Sie im *vCloud Director-Administratorhandbuch*.

Standardmäßig ist bei Organisations-VDCs mit Zuweisungspool ein elastischer Zuweisungspool aktiviert. Bei Systemen, die von vCloud Director 5.1 aktualisiert wurden und über Organisations-VDCs mit Zuweisungspool verfügen, bei denen sich virtuelle Maschinen über mehrere Ressourcenpools erstrecken, ist standardmäßig ein elastischer Zuweisungspool aktiviert.

Wenn bei Zuweisungspool-VDCs die Funktionalität des elastischen Zuweisungspools aktiviert ist, erstreckt sich das Organisations-VDC über alle Ressourcenpools, die seinem Provider-VDC zugeordnet sind, und verwendet sie. Die vCPU-Frequenz ist daher jetzt ein obligatorischer Parameter für einen Zuweisungspool.

Legen Sie die vCPU-Frequenz und den Faktor für den garantierten Prozentsatz so fest, dass genügend virtuelle Maschinen im Organisations-VDC bereitgestellt werden können, ohne dass die CPU zu einem Engpass führt.

Beim Erstellen einer virtuellen Maschine wird diese vom Platzierungsmodul in dem Provider-VDC-Ressourcenpool platziert, der die Anforderungen der virtuellen Maschine am besten erfüllt. Für dieses Organisations-VDC wird ein Unterressourcenpool unter dem Ressourcenpool des Provider-VDCs erstellt und die virtuelle Maschine wird unter diesem Unterressourcenpool platziert.

Wenn die virtuelle Maschine eingeschaltet wird, überprüft das Platzierungsmodul den Ressourcenpool des Provider-VDCs, um sicherzustellen, dass die Kapazität zum Einschalten der virtuellen Maschine ausreicht. Wenn dies nicht der Fall ist, verschiebt das Platzierungsmodul die virtuelle Maschine in einen Provider-VDC-Ressourcenpool mit ausreichenden Ressourcen zum Ausführen der virtuellen Maschine. Es wird ein Unterressourcenpool für das Organisations-VDC erstellt, falls noch keiner vorhanden ist.

Der Unterressourcenpool wird mit ausreichenden Ressourcen zum Ausführen der neuen virtuellen Maschine konfiguriert. Die Speicherreservierung des Unterressourcenpools wird um die Größe des für die virtuelle Maschine konfigurierten Speichers multipliziert mit dem prozentualen Garantiefaktor für das Organisations-VDC erhöht. Die CPU-Reservierung des Unterressourcenpools wird um die Anzahl von für die virtuelle Maschine konfigurierten vCPUs multipliziert mit dem auf der Ebene des Organisations-VDC festgelegten Faktor für den garantierten Prozentsatz für CPU erhöht. Wenn die elastische Zuweisungspoolfunktion aktiviert ist, wird die Arbeitsspeichergrenze des Unterressourcenpools um die konfigurierte Arbeitsspeichergröße der virtuellen Maschine erhöht, und die CPU-Grenze des Unterressourcenpools wird um die Anzahl der vCPUs, mit denen die virtuelle Maschine konfiguriert ist, multipliziert mit der auf der Organisations-VDC-Ebene angegebenen vCPU-Frequenz erhöht. Die virtuelle Maschine wird neu konfiguriert, um den Arbeitsspeicher und die CPU-Reservierung auf null zu setzen, und das Platzierungsmodul platziert die virtuelle Maschine im Ressourcenpool eines Provider-VDCs.

Beim Zuweisungsmodell der elastischen Poolzuweisung werden die Grenzwerte nur von vCloud Director überwacht und verwaltet. Wenn die elastische Funktion deaktiviert ist, wird der Ressourcenpool-Grenzwert zusätzlich festgelegt.

Die Vorzüge des Zuweisungspoolmodells bestehen darin, dass eine virtuelle Maschine die Ressourcen einer virtuellen Maschine im selben Unterressourcenpool, die sich im Leerlauf befindet, nutzen kann. Mit diesem Modell können neue Ressourcen genutzt werden, die dem Provider-VDC hinzugefügt werden.

In seltenen Fällen wird eine virtuelle Maschine beim Einschalten aufgrund von Ressourcenmangel in dem Ressourcenpool, dem die virtuelle Maschine ursprünglich bei der Erstellung zugewiesen wurde, einem anderen Ressourcenpool zugewiesen. Diese Änderung kann zu geringfügigen Kosten für das Verschieben der Festplattendateien der virtuellen Maschine in einen neuen Ressourcenpool führen.

Wenn die Funktionalität des elastischen Zuweisungspools deaktiviert ist, ähnelt das Verhalten von Organisations-VDCs mit Zuweisungspool dem Zuweisungspool-Modell in vCloud Director 1.5. In diesem Modell ist die vCPU-Frequenz nicht konfigurierbar. Die Zusicherung über Kapazitätsgrenzen hinaus wird durch Festlegen des Prozentsatzes der zugesicherten Ressourcen gesteuert.

Standardmäßig beziehen virtuelle Maschinen ihre Reservierungs-, Grenzwert- und Anteileneinstellungen in einem Zuweisungspool-VDC von den Einstellungen des VDCs. Zum Erstellen oder für die Neukonfiguration einer virtuellen Maschine mit benutzerdefinierten Ressourcenzuteilungseinstellungen für CPU und Speicher können Sie die vCloud-API verwenden. Weitere Informationen finden Sie im *vCloud API-Programmierhandbuch für Dienstleister*.

Zuweisungsmodell Pay-As-You-Go

Mit dem Zuweisungsmodell Pay-As-You-Go werden Ressourcen erst zugesichert, wenn Benutzer vApps im Organisations-VDC erstellen. Sie können Ressourcen überbelegen, indem Sie den Prozentsatz der garantierten Ressourcen angeben. Sie können ein Pay-As-You-Go-Organisations-VDC „elastisch“ machen, indem Sie mehrere Ressourcenpools zu seinem Provider-VDC hinzufügen.

Die der Organisation zugesicherten Ressourcen werden auf der Ebene virtueller Maschinen angewendet.

Wenn eine virtuelle Maschine eingeschaltet wird und der ursprüngliche Ressourcenpool die virtuelle Maschine nicht aufnehmen kann, überprüft das Platzierungsmodul den Ressourcenpool und weist die virtuelle Maschine einem anderen Ressourcenpool zu. Wenn für den Ressourcenpool kein Unterressourcenpool vorhanden ist, wird von vCloud Director ein Unterressourcenpool mit unbegrenztem Grenzwert und der Rate null erstellt. Die Rate der virtuellen Maschine wird auf den Grenzwert multipliziert mit ihren zugesicherten Ressourcen gesetzt und das Platzierungsmodul platziert die virtuelle Maschine im Ressourcenpool eines Provider-VDCs.

Der Vorteil des Pay-As-You-Go-Modells besteht darin, dass damit neue Ressourcen genutzt werden können, die dem Provider-VDC hinzugefügt werden.

In seltenen Fällen wird eine virtuelle Maschine beim Einschalten aufgrund von Ressourcenmangel in dem Ressourcenpool, dem die virtuelle Maschine ursprünglich bei der Erstellung zugewiesen wurde, einem anderen Ressourcenpool zugewiesen. Diese Änderung kann zu geringfügigen Kosten für das Verschieben der Festplattendateien der virtuellen Maschine in einen neuen Ressourcenpool führen.

Beim Pay-As-You-Go-Modell werden keine Ressourcen im Voraus reserviert, es kann also vorkommen, dass eine virtuelle Maschine wegen fehlender Ressourcen nicht eingeschaltet werden kann. Virtuelle Maschinen, die mit diesem Modell arbeiten, können auch nicht die Ressourcen von virtuellen Maschinen desselben Unterressourcenpools nutzen, die sich im Leerlauf befinden, da Ressourcen auf der Ebene virtueller Maschinen festgelegt werden.

Standardmäßig beziehen virtuelle Maschinen ihre Reservierungs-, Grenzwert- und Anteileinstellungen in einem Pay-As-You-Go-VDC von den Einstellungen des VDCs. Zum Erstellen oder für die Neukonfiguration einer virtuellen Maschine mit benutzerdefinierten Ressourcenzuteilungseinstellungen für CPU und Speicher können Sie die vCloud-API verwenden. Weitere Informationen finden Sie im *vCloud API-Programmierhandbuch für Dienstleister*.

Reservierungspool-Zuweisungsmodell

Mit dem Reservierungspool-Zuweisungsmodell werden alle von Ihnen zugewiesenen Ressourcen sofort dem Organisations-VDC zugesichert. Die Benutzer in der Organisation können die Überbelegung steuern, indem sie Reservierungs-, Grenzwert- und Prioritätseinstellungen für einzelne virtuelle Maschinen festlegen.

Da in diesem Modell nur ein Ressourcenpool und ein Unterressourcenpool vorhanden sind, wird der Ressourcenpool einer virtuellen Maschine vom Platzierungsmodul beim Einschalten nicht neu zugeordnet. Die Rate und das Limit der virtuellen Maschine werden nicht geändert.

Mit dem Reservierungspoolmodell sind Quellen immer verfügbar, wenn sie benötigt werden. Dieses Modell bietet auch eine genaue Kontrolle über die Rate, den Grenzwert und die Anteile von virtuellen Maschinen und ermöglicht so bei sorgfältiger Planung eine optimale Nutzung der reservierten Ressourcen. Informationen zum Konfigurieren der Ressourcenzuteilungseinstellungen für virtuelle Maschinen in Reservierungspool-VDCs finden Sie im *vCloud Air – Virtual Private Cloud OnDemand – Benutzerhandbuch*.

Bei diesem Modell erfolgt die Reservierung immer im primären Cluster. Wenn dort nicht genügend Ressourcen zum Erstellen eines Organisations-VDCs vorhanden sind, schlägt das Erstellen des Organisations-VDCs fehl.

Weitere Einschränkungen dieses Modells bestehen darin, dass es nicht elastisch ist und Benutzer der Organisation Freigaben, Raten und Limits für virtuelle Maschinen festlegen können, die nicht optimal sind und zu einer zu geringen Auslastung der Ressourcen führen.

Grundlegendes zu Computing-Richtlinien

Ab vCloud Director 9.7 können Sie die Ressourcenzuteilung und die Platzierung der virtuellen Maschine (VM) mithilfe von Computing-Richtlinien steuern. Basierend auf dem Geltungsbereich

und der Funktion gibt es zwei Typen von Computing-Richtlinien – Computing-Richtlinien für virtuelle Provider-Datencenter (VDC) und VDC-Computing-Richtlinien.

Provider-VDC-Computing-Richtlinie

Eine Provider-VDC-Computing-Richtlinie definiert VM-Host-Affinitätsregeln, die sich direkt auf die Platzierung von Mandantenarbeitslasten auswirken. Für Mandantenbenutzer sind die Provider-VDC-Computing-Richtlinien nicht sichtbar.

Der Geltungsbereich der Provider-VDC-Computing-Richtlinien ist die Provider-VDC-Ebene.

VDC-Computing-Richtlinie

Eine VDC-Computing-Richtlinie steuert die Computing-Merkmale einer VM auf Organisations-VDC-Ebene. Da für Mandantenbenutzer die Provider-VDC-Computing-Richtlinien nicht sichtbar sind, können Sie die VM-Host-Affinitätsregeln für die Mandantennutzung anzeigen, indem Sie auf die Provider-VDC-Computing-Richtlinie innerhalb der VDC-Computing-Richtlinie verweisen.

Computing-Richtlinien für virtuelle Provider-Datencenter

Mithilfe der Computing-Richtlinien des Provider-VDC können vCloud Director-**Systemadministratoren** VM-Gruppen und logische VM-Gruppen für Mandanten zur Verfügung stellen.

Computing-Richtlinien des Provider-VDC können eine Sammlung folgender Elemente enthalten:

- VM-Gruppen, die ähnliche VMs enthalten. Jede VM-Gruppe gehört zu einem anderen Cluster.
- Logische VM-Gruppen, die für unterschiedliche Funktionalitäten geeignet sind.
- Sowohl VM-Gruppen als auch logische VM-Gruppen.

Provider-VDC-Computing-Richtlinien und logische VM-Gruppen

Ein **Systemadministrator** kann Mandanten mithilfe von VM-Gruppen und logischen VM-Gruppen VM-Host-Affinitätsregeln für vSphere DRS (Distributed Resource Schedule) zur Verfügung stellen. DRS-VM-Host-Affinitätsregeln werden auf Anbieterebene in vCloud Director als VM-Gruppen verfügbar gemacht. VM-Host-Affinitätsregeln sind an einen bestimmten Cluster gebunden. Da sich elastische Anbieter-VDCs über mehrere vSphere-Cluster erstrecken können, stellen logische VM-Gruppen die Abstraktion von DRS-VM-Host-Affinitätsregeln bereit, die über mehrere Cluster hinweg funktioniert, indem an Cluster gebundene VM-Gruppen gruppiert werden, die logisch äquivalent sind. Um logische VM-Gruppen zu verwalten, verwenden Sie vCloud OpenAPI. Informationen zur vCloud OpenAPI finden Sie in *Erste Schritte mit vCloud OpenAPI* unter <https://code.vmware.com>.

Um VM-Host-Affinitätsregeln verfügbar zu machen, fügen Sie VM-Gruppen und logische VM-Gruppen zu einer Provider-VDC-Computing-Richtlinie hinzu und erstellen einen Verweis zwischen der Provider-VDC-Computing-Richtlinie und einer VDC-Computing-Richtlinie.

Im Kontext von Provider-VDC-Computing-Richtlinien weisen logische VM-Gruppen eine AND-Beziehung untereinander auf.

Mit Computing-Richtlinien des Provider-VDC und logischen VM-Gruppen können **vCloud Director-Systemadministratoren** Mandantenbenutzern innerhalb eines Organisations-VDC mehrere VM-Gruppen zur Verfügung stellen. Betrachten Sie beispielsweise eine Umgebung, die zwei Cluster enthält: *cluster1* und *cluster2*. In *cluster1* befindet sich der Host *SQL_host_1*, während sich in *cluster2* die Hosts *SQL_fast_host* und *Fast_host* befinden.

- 1 In *cluster1* erstellen Sie *SQL_host_group1* und *VM_group1*.
Sie erstellen eine positive Affinität zwischen *VM_group1* und *SQL_host_group1*.
- 2 Sie erstellen in *cluster2* vier Gruppen.
 - Sie erstellen *SQL_host_group2* und *VM_group2*
Sie erstellen eine positive Affinität zwischen *VM_group2* und *SQL_host_group2*.
 - Sie erstellen *fast_host_group* und *VM_group3*.
Sie erstellen eine positive Affinität zwischen *VM_group3* und *fast_host_group*.

Sie erstellen die *PVDC_compute_policy1*, die aus *logical_VM_group1* und *logical_VM_group2* besteht. Die *logical_VM_group1* umfasst *VM_group1* und *VM_group2*. Die *logical_VM_group2* umfasst *VM_group3*.

Sie erstellen und veröffentlichen die VDC-Computing-Richtlinie *SQL_and_fast* für ein Organisations-VDC und fügen einen Verweis auf *PVDC_compute_policy1* hinzu. Wenn Sie einen Verweis zwischen der VDC-Computing-Richtlinie *SQL_and_fast* und der *PVDC_compute_policy1* erstellen, stellen Sie den Mandantenbenutzern innerhalb des Organisations-VDC Informationen zu logischen VM-Gruppen und VM-Gruppen zur Verfügung. Wenn ein Mandant daher die VDC-Computing-Richtlinie *SQL_and_fast* auf eine VM anwendet, fügt das Platzierungsmodul die VM zum *SQL_fast_host* innerhalb von *cluster2* hinzu.

Der Workflow lautet wie folgt.

- 1 Ein **vCenter Server-Administrator** erstellt Hostgruppen mithilfe des vSphere Client.
Weitere Informationen finden Sie unter *Erstellen einer Host-DRS-Gruppe (MSCS)* in der *Dokumentation zu VMware vSphere ESXi und vCenter Server*.
- 2 Ein **vCenter Server-Administrator** oder ein **vCloud Director-Systemadministrator** erstellt VM-Gruppen.
Weitere Informationen finden Sie unter *Erstellen oder Aktualisieren einer VM-Gruppe* im *vCloud Director-Administratorhandbuch*.
- 3 Ein **vCloud Director-Systemadministrator** erstellt die entsprechenden Affinitätsregeln zwischen VM-Gruppen und Hostgruppen.
Weitere Informationen finden Sie unter *Verwalten von VM-Host-Affinitätsregeln* im *vCloud Director-Administratorhandbuch*.
- 4 Ein **vCloud Director-Systemadministrator** gruppiert logisch äquivalente VM-Gruppen mithilfe der vCloud OpenAPI in logischen VM-Gruppen.

- 5 Ein **vCloud Director-Systemadministrator** erstellt eine Provider-VDC-Computing-Richtlinie und fügt die logischen VM-Gruppen mithilfe der vCloud OpenAPI hinzu.
- 6 Ein **vCloud Director-Systemadministrator** erstellt eine VDC-Computing-Richtlinie, die auf die Provider-VDC-Computing-Richtlinie verweist, und veröffentlicht die VDC-Computing-Richtlinie für ein Organisations-VDC unter Verwendung der vCloud OpenAPI.

Wenn ein Mandant eine VM im Organisations-VDC erstellt und die VDC-Computing-Richtlinie auswählt, fügt vCloud Director die VM zur VM-Gruppe hinzu, auf die in der VDC-Computing-Richtlinie verwiesen wird. Daher erstellt vCloud Director die VM auf dem entsprechenden Host.

Provider-VDC-Computing-Richtlinien und VM-Gruppen

Eine Provider-VDC-Computing-Richtlinie kann keine oder eine VM-Gruppe aus jedem Cluster besitzen. Beispielsweise kann die Provider-VDC-Computing-Richtlinie *oracle_license* die VM-Gruppen *oracle_license1* und *oracle_license2* umfassen, wobei die VM-Gruppe *oracle_license1* zum Cluster *oracle_cluster1* und die VM-Gruppe *oracle_license2* zum Cluster *oracle_cluster2* gehört.

Wenn Sie einer virtuellen Maschine eine Provider-VDC-Computing-Richtlinie zuweisen, fügt das Platzierungsmodul diese VM der entsprechenden VM-Gruppe des Clusters hinzu, auf dem sie sich befindet. Wenn Sie z. B. eine virtuelle Maschine auf Cluster *oracle_cluster1* bereitstellen möchten und die Provider-VDC-Computing-Richtlinie *oracle_license* dieser virtuellen Maschine zuweisen, fügt das Platzierungsmodul die virtuelle Maschine der VM-Gruppe *oracle_license1* hinzu.

Der Workflow lautet wie folgt.

- 1 Ein **Systemadministrator** erstellt eine oder mehrere Provider-VDC-Computing-Richtlinien mithilfe der vCloud OpenAPI.
- 2 Ein **Systemadministrator** erstellt eine oder mehrere VDC-Computing-Richtlinien mithilfe der vCloud OpenAPI.

Eine VDC-Computing-Richtlinie kann keiner oder einer Provider-VDC-Computing-Richtlinie zugeordnet werden. VDC-Computing-Richtlinien haben einen eindeutigen Namen und eine eindeutige Provider-VDC-Computing-Richtlinie.

- 3 Ein **Systemadministrator** veröffentlicht die VDC-Computing-Richtlinie für eine oder mehrere Organisations-VDCs mithilfe der vCloud OpenAPI.

Mandanten können nur die VDC-Computing-Richtlinien sehen, die für ihre Organisations-VDCs veröffentlicht wurden. Provider-VDC-Computing-Richtlinien sind nicht auf Mandantenebene verfügbar.

- 4 Mandanten können die vCloud-API oder das vCloud Director-Mandantenportal verwenden, um einer VM eine Organisations-VDC-Computing-Richtlinie zuzuweisen, wenn eine VM erstellt oder aktualisiert wird.

Anfangs enthält das System keine Provider-VDC-Computing-Richtlinien, und jedes Organisations-VDC enthält nur eine Standard-Computing-Richtlinie, die nicht mit einer Provider-VDC-Computing-Richtlinie verknüpft ist.

Zum Erstellen und Verwalten von Anbieter- und globalen VDC-Computing-Richtlinien müssen Sie die vCloud OpenAPI verwenden. Weitere Informationen finden Sie in *Erste Schritte mit vCloud OpenAPI* unter <https://code.vmware.com>.

Computing-Richtlinien für virtuelle Datacenter

Computing-Richtlinien für das virtuelle Datacenter (VDC) steuern die physische Computing-Ressourcenzuweisung für Mandantenarbeitslasten. Um physische Ressourcen basierend auf bestimmten Arbeitslastanforderungen zuzuweisen, können Mandantenbenutzer zwischen einer standardmäßigen und benutzerdefinierten VDC-Computing-Richtlinien auswählen.

Eine VDC-Computing-Richtlinie gruppiert Attribute, die die Computing-Ressourcenzuweisung für virtuelle Maschinen innerhalb eines Organisations-VDC definieren. Die Computing-Ressourcenzuweisung umfasst CPU- und Arbeitsspeicherzuweisung, Reservierungen, Grenzwerte und Anteile.

vCloud Director **-Systemadministratoren** erstellen und verwalten Computing-Richtlinien auf globaler Ebene und können einzelne Computing-Richtlinien für ein oder mehrere Organisations-VDCs veröffentlichen. Wenn Sie eine VDC-Computing-Richtlinie für ein Organisations-VDC veröffentlichen, wird die Richtlinie für die Benutzer in der Organisation verfügbar. Beim Erstellen und Verwalten von virtuellen Maschinen im Organisations-VDC können **Mandantenadministratoren** die verfügbaren VDC-Computing-Richtlinien zu virtuellen Maschinen zuweisen. **Mandantenadministratoren** und Benutzer im Organisations-VDC können die spezifische Konfiguration einer VDC-Computing-Richtlinie nicht einsehen.

Mit VDC-Computing-Richtlinien können Cloud-Anbieter benannte CPU- und Arbeitsspeicher-Nutzungsprofile definieren, die Mandanten den virtuellen Maschinen innerhalb eines Organisations-VDC zuordnen können. Die Verwendung von VDC-Computing-Richtlinien ist ein Mechanismus, mit dem Cloud-Anbieter differenzierte Dienstebenen definieren und anbieten können, z. B. ein CPU-intensives Profil oder ein Profil mit hoher Arbeitsspeicherauslastung. Mit VDC-Computing-Richtlinien können Cloud-Anbieter auch die CPU- und Arbeitsspeichernutzung von virtuellen Maschinen in einem Organisations-VDC begrenzen oder einschränken.

Mit VDC-Computing-Richtlinien können vCloud Director-Systemadministratoren die folgenden Aspekte der Computing-Ressourcennutzung auf der Ebene der virtuellen Maschine steuern:

- Anzahl der vCPUs und vCPU-Taktgeschwindigkeiten
- Größe des Arbeitsspeichers, der der virtuellen Maschine zugeteilt ist
- Arbeitsspeicher- und CPU-Reservierung, -Grenzwert und -Anteile

Attribute von Computing-Richtlinien für virtuelle Datacenter

Wenn Sie eine VDC-Computing-Richtlinie (Virtual Data Center – virtuelles Datacenter) erstellen, können Sie eine Teilmenge aller verfügbaren Attribute angeben. Das einzige obligatorische Attribut ist der Name der VDC-Computing-Richtlinie.

Die folgende Tabelle listet alle Attribute auf, die Sie innerhalb einer VDC-Computing-Richtlinie definieren können.

Tabelle 6-1. VDC-Computing-Richtlinienattribute

VDC-Computing-Richtlinienattribut	API-Parameter	Beschreibung
Name	name	Obligatorischer Parameter, der als Bezeichner für die VDC-Computing-Richtlinie verwendet wird.
Description	description	Stellt eine kurze Beschreibung der VDC-Computing-Richtlinie dar.
vCPU Speed	cpuSpeed	Definiert die vCPU-Geschwindigkeit einer virtuellen Maschine (VM) in MHz.
Memory	memory	Definiert den für eine VM konfigurierten Arbeitsspeicher in MB. Wenn ein Mandant die VDC-Computing-Richtlinie einer VM zuweist, erhält die VM die Menge an Arbeitsspeicher, die durch dieses Attribut definiert wird.
Number of vCPUs	cpuCount	Definiert die Anzahl der für eine VM konfigurierten vCPUs. Wenn ein Mandant die VDC-Computing-Richtlinie einer VM zuweist, erhält die VM die durch dieses Attribut definierte Anzahl von vCPUs.
Cores per Socket	coresPerSocket	Die Anzahl der Kerne pro Socket für eine VM. Die Anzahl der vCPUs, die in der VDC-Computing-Richtlinie definiert ist, muss durch die Anzahl der Kerne pro Socket teilbar sein. Wenn die Anzahl der vCPUs nicht durch die Anzahl der Kerne pro Socket teilbar ist, wird die Anzahl der Kerne pro Socket ungültig.
Memory Reservation Guarantee	memoryReservationGuarantee	Definiert die reservierte Menge an Arbeitsspeicher, die für eine VM konfiguriert ist. Der Wert des Attributs liegt zwischen 0 und 1. Mit einem Wert von 0 für die Arbeitsspeicher-Reservierungsgarantie wird definiert, dass keine Arbeitsspeichergarantie vorhanden ist. Der Wert eins definiert 100 % reservierten Arbeitsspeicher.
CPU Reservation Guarantee	cpuReservationGuarantee	Legt fest, wie viele CPU-Ressourcen einer VM reserviert sind. Die zugewiesene CPU für eine VM entspricht der Anzahl der vCPUs multipliziert mit der vCPU-Geschwindigkeit in MHz. Der Wert des Attributs liegt zwischen 0 und eins. Mit einem Wert von 0 für die CPU-Reservierungsgarantie wird angegeben, dass keine CPU-Reservierung vorhanden ist. Der Wert 1 definiert 100 % reservierte CPU.
CPU Limit	cpuLimit	Definiert den CPU-Grenzwert in MHz für eine VM. Der Wert minus eins (-1) definiert, dass kein CPU-Grenzwert vorhanden ist. Wenn er in der VDC-Computing-Richtlinie nicht definiert ist, ist der CPU-Grenzwert gleich der zugewiesenen CPU für die VM.
Memory Limit	memoryLimit	Definiert den Arbeitsspeichergrenzwert in MB für eine VM. Der Wert minus eins (-1) definiert, dass kein Arbeitsspeichergrenzwert vorhanden ist. Wenn er in der VDC-Computing-Richtlinie nicht definiert ist, entspricht der Arbeitsspeichergrenzwert dem zugewiesenen Arbeitsspeicher für die VM.
CPU Shares	cpuShares	Definiert die Anzahl der CPU-Anteile für eine VM. Wenn sie in der VDC-Computing-Richtlinie nicht definiert sind, werden normale Anteile auf die VM angewendet.
Memory Shares	memoryShares	Definiert die Anzahl der Arbeitsspeicheranteile für eine VM. Wenn sie in der VDC-Computing-Richtlinie nicht definiert sind, werden normale Anteile auf die VM angewendet.

Tabelle 6-1. VDC-Computing-Richtlinienattribute (Fortsetzung)

VDC-Computing-Richtlinienattribut	API-Parameter	Beschreibung
Extra Configurations	extraConfigs	Stellt eine Zuordnung zwischen Schlüssel-Wert-Paaren dar, die als zusätzliche Konfigurationswerte auf eine VM angewendet werden.
Provider VDC Compute Policy	pvdccomputePolicy	Definiert den Verweis der VDC-Computing-Richtlinie auf eine Provider-VDC-Computing-Richtlinie.

Arbeiten mit Computing-Richtlinien für virtuelle Datacenter

vCloud Director generiert eine Standard-Computing-Richtlinie für alle virtuellen Datacenter (VDCs). Die Standard-VDC-Computing-Richtlinie enthält nur einen Namen und eine Beschreibung und alle verbleibenden Attribute für VDC-Computing-Richtlinien sind leer.

Sie können auch eine andere VDC-Computing-Richtlinie als Standardrichtlinie für ein Organisations-VDC definieren. Die Standard-VDC-Computing-Richtlinie steuert die Ressourcenzuweisung und die Nutzung der virtuellen Maschinen (VMs), die Mandanten im Organisations-VDC erstellen, es sei denn, ein Mandant weist der VM eine andere spezifische VDC-Computing-Richtlinie zu.

Um die maximalen Computing-Ressourcen zu begrenzen, die Mandanten einzelnen VMs innerhalb eines Organisations-VDC zuweisen können, können Cloud-Anbieter eine maximale VDC-Computing-Richtlinie definieren. Wenn sie einem Organisations-VDC zugewiesen ist, fungiert die maximale VDC-Computing-Richtlinie als Obergrenze für die Computing-Ressourcenkonfiguration für alle VMs innerhalb des Organisations-VDC. Die maximale VDC-Computing-Richtlinie steht Mandantenbenutzern beim Erstellen einer VM nicht zur Verfügung. Wenn Sie eine VDC-Computing-Richtlinie als maximale VDC-Computing-Richtlinie definieren, kopiert vCloud Director intern den Inhalt der Richtlinie und verwendet den kopierten Inhalt als maximale VDC-Computing-Richtlinie. Infolgedessen hängt das Organisations-VDC nicht von der anfänglich verwendeten VDC-Computing-Richtlinie ab.

Wenn Sie mehrere VDC-Computing-Richtlinien für ein Organisations-VDC veröffentlichen, können Mandantenbenutzer zwischen allen benutzerdefinierten Richtlinien und der Standardrichtlinie auswählen, wenn sie VMs im Organisations-VDC erstellen und verwalten.

Zu den verfügbaren VDC-Computing-Richtlinienvorgängen für Cloud-Anbieter gehören:

- Eine VDC-Computing-Richtlinie erstellen.
- Eine VDC-Computing-Richtlinie für ein oder mehrere Organisations-VDCs veröffentlichen.
- Die Veröffentlichung einer VDC-Computing-Richtlinie für ein Organisations-VDC rückgängig machen.
- Eine VDC-Computing-Richtlinie löschen.

Benutzer mit dem Recht **ORG_VDC_MANAGE_COMPUTE_POLICIES** können VDC-Computing-Richtlinien erstellen, aktualisieren und veröffentlichen. Um VDC-Computing-Richtlinien zu erstellen, verwenden Sie die vCloud API.

In der folgenden Tabelle sind die verfügbaren VDC-Computing-Richtlinienvorgänge für Mandantenbenutzer aufgeführt.

Tabelle 6-2. VDC-Computing-Richtlinienvorgänge für Mandantenbenutzer

Vorgang	Beschreibung
Einer VM während der VM-Erstellung eine VDC-Computing-Richtlinie zuweisen.	Mandantenbenutzer, die zum Erstellen von VMs in einem Organisations-VDC berechtigt sind, können optional VDC-Computing-Richtlinien zu VMs zuweisen. Infolgedessen steuern die in der VDC-Computing-Richtlinie definierten Parameter die CPU- und Arbeitsspeichernutzung der VM. Das Zuweisen einer VDC-Computing-Richtlinie ist für Mandanten während der VM-Erstellung nicht erforderlich. Wenn ein Mandant nicht explizit eine VDC-Computing-Richtlinie für die Zuweisung zu einer VM wählt, wird die Standard-VDC-Richtlinie auf die VM angewendet. Mandantenbenutzer können einer VM während der VM-Erstellung mithilfe des vCloud Director-Mandantenportals eine VDC-Computing-Richtlinie zuweisen.
Einer vorhandenen VM eine VDC-Computing-Richtlinie zuweisen.	Mandantenbenutzer, die zur Verwaltung von VMs in einem Organisations-VDC berechtigt sind, können die Zuordnung zwischen einer VM und einer VDC-Computing-Richtlinie aktualisieren. Infolgedessen konfiguriert das System die VM neu, um Computing-Ressourcen zu nutzen, wie in der neuen VDC-Computing-Richtlinie angegeben. Mandantenbenutzer können mithilfe des vCloud Director-Mandantenportals einer vorhandenen VM eine VDC-Computing-Richtlinie zuweisen.

Mithilfe von VDC-Computing-Richtlinien können Cloud-Anbieter die Nutzung von Computing-Ressourcen für alle VMs innerhalb eines Organisations-VDC beispielsweise auf drei vordefinierte Größen einschränken, z. B. *kleine Größe*, *mittlere Größe* und *große Größe*. Der Workflow lautet wie folgt.

- 1 Ein **Systemadministrator** erstellt drei VDC-Computing-Richtlinien mit den folgenden Attributen:

Name	Attribute
Kleine Größe	<ul style="list-style-type: none"> ■ Beschreibung: VM-Richtlinie für kleine Größen ■ Name: kleine Größe ■ Arbeitsspeicher: 1024 ■ Anzahl an vCPUs: 1
Mittlere Größe	<ul style="list-style-type: none"> ■ Beschreibung: VM-Richtlinie für mittlere Größen ■ Name: mittlere Größe ■ Arbeitsspeicher: 2048 ■ Anzahl an vCPUs: 2
Große Größe	<ul style="list-style-type: none"> ■ Beschreibung: VM-Richtlinie für große Größen ■ Name: große Größe ■ Arbeitsspeicher: 4096 ■ Anzahl an vCPUs: 4

- 2 Veröffentlichen Sie die neuen VDC-Computing-Richtlinien in einem Organisations-VDC.

Durch das Veröffentlichen einer VDC-Computing-Richtlinie in einem Organisations-VDC ist die Richtlinie für Mandantenbenutzer im Organisations-VDC verfügbar.

- 3 Definieren Sie optional eine der VDC-Computing-Richtlinien als Standard-VDC-Richtlinie für das Organisations-VDC.

Wenn Sie eine Standardrichtlinie für das Organisations-VDC definieren und die Mandantenbenutzer während der Erstellung einer VM keine andere Richtlinie angeben, wird die Standardrichtlinie auf die VM angewendet.

Um VDC-Computing-Richtlinien anzuzeigen oder zu ändern, müssen Sie die vCloud API verwenden.


Erstellen eines virtuellen Organisations-Datencenters

Um einer Organisation Ressourcen zuzuweisen, müssen Sie ein virtuelles Organisations-Datencenter erstellen. Ein virtuelles Organisations-Datencenter erhält seine Ressourcen von einem virtuellen Provider-Datencenter. Eine Organisation kann über mehrere virtuelle Organisations-Datencenter verfügen.

Voraussetzungen

Erstellen Sie ein virtuelles Provider-Datencenter. Weitere Informationen dazu finden Sie im *vCloud Director-Administratorhandbuch*.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie dann auf **Neu**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für das neue virtuelle Organisations-Datencenter ein.
- 4 (Optional) Um das neue virtuelle Organisations-Datencenter bei der Erstellung zu deaktivieren, deaktivieren Sie die Umschaltoption **Organisations-VDC aktivieren**.

Benutzer können keine vApps auf einem deaktivierten virtuellen Organisations-Datencenter bereitstellen.

- 5 Klicken Sie auf **Weiter**.
- 6 Aktivieren Sie das Optionsfeld neben dem Namen der Organisation, der Sie dieses virtuelle Datencenter hinzufügen möchten, und klicken Sie auf **Weiter**.
- 7 Aktivieren Sie das Optionsfeld neben dem Namen des virtuellen Provider-Datencenters, von dem das virtuelle Organisations-Datencenter Computing- und Speicherressourcen erhalten soll, und klicken Sie auf **Weiter**.

Die Liste der virtuellen Provider-Datencenter zeigt alle aktivierten virtuellen Provider-Datencenter am Standort mit Informationen zu den verfügbaren Ressourcen an. In der Liste „Netzwerke“ werden Informationen zu den für das ausgewählte virtuelle Provider-Datencenter verfügbaren Netzwerken angezeigt.

- 8 Wählen Sie ein Zuweisungsmodell für dieses virtuelle Organisations-Datencenter aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Zuweisungspool	Ein Prozentsatz der von Ihnen über das virtuelle Provider-Datencenter zugewiesenen Ressourcen wird dem virtuellen Organisations-Datencenter zugesichert. Sie können den Prozentsatz für CPU und Arbeitsspeicher angeben.
Pay-As-You-Go	Ressourcen werden erst zugesichert, wenn Benutzer in dem virtuellen Organisations-Datencenter vApps erstellen.
Reservierungspool	Alle von Ihnen zugeteilten Ressourcen werden dem virtuellen Organisations-Datencenter sofort zugesichert.
Flex	Sie können die Ressourcennutzung sowohl auf der Ebene des VDC als auch auf der Ebene der einzelnen virtuellen Maschine steuern. Das Flex-Zuweisungsmodell unterstützt die Funktionen der Organisations-VDC-Computing-Richtlinien. Das Flex-Zuweisungsmodell unterstützt alle Zuweisungskonfigurationen, die in den anderen Zuweisungsmodellen verfügbar sind.

- 9 Konfigurieren Sie die Zuweisungseinstellungen für das Zuweisungsmodell, das Sie ausgewählt haben, und klicken Sie auf **Weiter**.

Option	Beschreibung	Zuweisungsmodell
Elastizität	Aktivieren oder deaktivieren Sie die Funktion des elastischen Pools. Ein elastisches Organisations-VDC umfasst und verwendet alle dem Provider-VDC zugewiesenen Ressourcenpools.	Flex
VM-Arbeitsspeicher-Overhead einschließen	Arbeitsspeicher-Overhead ein- oder ausschließen.	Flex
CPU-Zuweisung	Die maximale CPU-Menge, die Sie den virtuellen Maschinen zuweisen möchten, die in diesem virtuellen Organisations-Datencenter ausgeführt werden.	<ul style="list-style-type: none"> ■ Zuweisungspool ■ Reservierungspool ■ Flex
Zulassen, dass CPU-Ressourcen den reservierten Wert überschreiten	Um diesem virtuellen Organisations-Datencenter unbegrenzte CPU-Ressourcen zur Verfügung zu stellen, aktivieren Sie diese Umschaltoption.	Reservierungspool
CPU-Kontingent	Die maximale CPU-Nutzung für dieses virtuelle Organisations-Datencenter.	<ul style="list-style-type: none"> ■ Pay-As-You-Go ■ Flex
Garantierte CPU-Ressourcen	Der Prozentsatz der CPU-Ressourcen, den Sie für eine virtuelle Maschine garantieren möchten, die in diesem virtuellen Organisations-Datencenter ausgeführt wird. Sie können die Überbelegung von CPU-Ressourcen steuern, indem Sie weniger als 100 Prozent garantieren. Bei einem Zuweisungspool-Zuweisungsmodell bestimmt der garantierte Prozentsatz auch, welcher Prozentsatz der CPU-Zuweisung für dieses virtuelle Organisations-Datencenter zugesichert werden soll.	<ul style="list-style-type: none"> ■ Zuweisungspool ■ Pay-As-You-Go ■ Flex

Option	Beschreibung	Zuweisungsmodell
vCPU-Geschwindigkeit	Die vCPU-Geschwindigkeit. Den virtuellen Maschinen im virtuellen Organisations-Datencenter wird dieser Wert in GHz pro vCPU zugeteilt.	<ul style="list-style-type: none"> ■ Pay-As-You-Go ■ Flex
Arbeitsspeicherzuweisung	Die maximale Menge an Arbeitsspeicher, die Sie den virtuellen Maschinen zuweisen möchten, die im virtuellen Organisations-Datencenter ausgeführt werden.	<ul style="list-style-type: none"> ■ Zuweisungspool ■ Reservierungspool
Arbeitsspeicherkontingent	Die maximale Menge an Arbeitsspeichernutzung für dieses virtuelle Organisations-Datencenter.	<ul style="list-style-type: none"> ■ Pay-As-You-Go ■ Flex
Garantierte Arbeitsspeicherressourcen	<p>Der Prozentsatz der Arbeitsspeicherressourcen, der den virtuellen Maschinen im virtuellen Organisations-Datencenter garantiert werden soll. Sie können Ressourcen überbelegen, indem Sie weniger als 100 Prozent garantieren.</p> <p>Bei einem Zuweisungspool-Zuweisungsmodell bestimmt der garantierte Prozentsatz auch, welcher Prozentsatz der Arbeitsspeicherzuweisung für dieses virtuelle Organisations-Datencenter zugesichert werden soll.</p>	<ul style="list-style-type: none"> ■ Zuweisungspool ■ Pay-As-You-Go ■ Flex
Maximale Anzahl der VMs	Die maximale Anzahl virtueller Maschinen, die im virtuellen Organisations-Datencenter vorhanden sein dürfen.	<ul style="list-style-type: none"> ■ Zuweisungspool ■ Pay-As-You-Go ■ Reservierungspool ■ Flex

- 10** Konfigurieren Sie die Speichereinstellungen für dieses virtuelle Organisations-Datencenter und klicken Sie auf **Weiter**.

Die Liste enthält die aktivierten Speicherrichtlinien für das virtuelle Provider-Quelldatencenter.

- a Aktivieren Sie die Kontrollkästchen für eine oder mehrere Speicherrichtlinien, die Sie zu diesem virtuellen Organisations-Datencenter hinzufügen möchten.
- b (Optional) Um die Menge der zugewiesenen Speicherkapazität für eine ausgewählte Speicherrichtlinie zu begrenzen, wählen Sie **Begrenzt** aus dem Dropdown-Menü in der Zelle **Zuteilungstyp** aus und geben Sie die maximale Kapazität in der Zelle **Zugeteilter Speicher** ein.
- c (Optional) Um die Standardspeicherrichtlinie zu ändern, wählen Sie aus dem Dropdown-Menü **Standardinstanziierungsrichtlinie** die Ziel-Standardspeicherrichtlinie aus.
vCloud Director verwendet die Standardspeicherrichtlinie für alle VM-Bereitstellungsvorgänge, bei denen keine Speicherrichtlinie auf der VM- oder vApp-Vorlagenebene angegeben wurde.
- d (Optional) Um Thin Provisioning für virtuelle Maschinen im virtuellen Organisations-Datencenter zu aktivieren, aktivieren Sie die Umschaltoption **Thin Provisioning**.
- e (Optional) Um Fast Provisioning für virtuelle Maschinen im virtuellen Organisations-Datencenter zu deaktivieren, deaktivieren Sie die Umschaltoption **Fast Provisioning**.

- 11 Konfigurieren Sie die Netzwerkpooleinstellungen für dieses virtuelle Organisations-Datencenter und klicken Sie auf **Weiter**.

vCloud Director verwendet den Netzwerkpool zum Erstellen von vApp-Netzwerken und internen VDC-Organisationsnetzwerken.

- Um das Hinzufügen eines Netzwerkpools zu diesem Zeitpunkt zu überspringen, deaktivieren Sie die Umschaltoption **Netzwerkpool verwenden**.
- Um einen Netzwerkpool zu konfigurieren, aktivieren Sie das Optionsfeld neben dem Namen des gewünschten Netzwerkpools und geben Sie das Kontingent für dieses virtuelle Organisations-Datencenter ein.


Das Kontingent ist die maximale Anzahl der bereitgestellten Netzwerke im virtuellen Organisations-Datencenter, die von diesem Netzwerkpool unterstützt werden. Darf die Anzahl der verfügbaren Netzwerke für den ausgewählten Netzwerkpool nicht überschreiten.

- 12 Überprüfen Sie die Seite **Bereit zum Abschließen** und klicken Sie auf **Beenden**.

Aktivieren oder Deaktivieren eines virtuellen Organisations-Datencenters

Um zu verhindern, dass zusätzliche vApps und virtuelle Maschinen Computing- und Speicherressourcen eines virtuellen Organisations-Datencenters verwenden, können Sie dieses virtuelle Organisations-Datencenter deaktivieren. Laufende vApps und eingeschaltete virtuelle Maschinen laufen weiter, aber Sie können weder neue vApps oder virtuelle Maschinen erstellen noch zusätzliche starten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf **Aktivieren** oder **Deaktivieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Löschen eines virtuellen Organisations-Datencenters


Um alle Ressourcen eines virtuellen Organisations-Datencenters aus einer Organisation zu entfernen, können Sie dieses virtuelle Organisations-Datencenter löschen. Dieser Vorgang hat im virtuellen Provider-Quelldatencenter keine Auswirkungen auf die Ressourcen.

Wichtig Durch diesen Vorgang werden das virtuelle Organisations-Datencenter und alle zugehörigen VMs, vApps, VDC-Organisationsnetzwerke und Edge-Gateways dauerhaft entfernt.

Voraussetzungen

Wenn Sie bestimmte VMs, vApps, vApp-Vorlagen oder Mediendateien behalten möchten, die zum virtuellen Organisations-Zieldatacenter gehören, verschieben Sie sie in ein anderes virtuelles Organisations-Datencenter.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des virtuellen Organisations-Datencenters, das Sie entfernen möchten, und klicken Sie auf **Löschen**.
- 4 Wenn dieses virtuelle Organisations-Datencenter Ressourcen enthält, wie z. B. VMs, vApps, VDC-Organisationsnetzwerke und Edge-Gateways, aktivieren Sie das Kontrollkästchen für jeden Ressourcentyp, um dessen Entfernung zu bestätigen.
- 5 Klicken Sie zur Bestätigung auf **Löschen**.

Ändern des Namens und der Beschreibung eines virtuellen Organisations-Datencenters.

Wenn Ihre vCloud Director-Installation ausgeweitet wird, besteht möglicherweise der Bedarf, einem bestehenden virtuellen Organisations-Datencenter einen aussagekräftigeren Namen oder eine Beschreibung zuzuweisen.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf der Registerkarte **Allgemein** in der oberen rechten Ecke auf **Bearbeiten**.
- 4 Geben Sie einen neuen Namen und eine neue Beschreibung ein und klicken Sie auf **Speichern**.

Ändern der Zuweisungsmodelleinstellungen eines virtuellen Organisations-Datencenters

Sie können das Zuweisungsmodell für ein virtuelles Organisations-Datencenter nicht ändern, jedoch können Sie die Zuweisungseinstellungen des Zuweisungsmodells ändern, das beim Erstellen des virtuellen Organisations-Datencenters festgelegt wurde.

Sie können die Zuweisungseinstellungen für das Zuweisungsmodell ändern, das Sie während der Erstellung des virtuellen Organisations-Datencenters konfiguriert haben. Weitere Informationen finden Sie unter [Schritt 9](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf der Registerkarte **Zuweisung** in der oberen rechten Ecke auf **Bearbeiten**.
- 4 Bearbeiten Sie die Einstellungen für das Zuweisungsmodell und klicken Sie auf **Speichern**.


Ändern der Speichereinstellungen eines virtuellen Organisations-Datencenters

Sie können die Speichereinstellungen ändern, die Sie während der Erstellung des virtuellen Organisations-Datencenters konfiguriert haben.

Ändern der VM-Bereitstellungseinstellungen eines Organisations-VDC

Sie können die Einstellungen für Thin und Fast Provisioning der virtuellen Maschine ändern, die Sie während der Erstellung des Organisations-VDC konfiguriert haben.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf der Registerkarte **Speicher** in der oberen rechten Ecke auf **Bearbeiten**.
- 4 (Optional) Ändern Sie die Einstellung für Thin Provisioning.
 - Zum Deaktivieren von Thin Provisioning für virtuelle Maschinen im Organisations-VDC deaktivieren Sie die Umschaltfläche **Thin Provisioning**.
 - Zum Aktivieren von Thin Provisioning für virtuelle Maschinen im Organisations-VDC aktivieren Sie die Umschaltfläche **Thin Provisioning**.
- 5 (Optional) Ändern Sie die Einstellung für Fast Provisioning.
 - Zum Aktivieren von Fast Provisioning für virtuelle Maschinen im Organisations-VDC aktivieren Sie die Umschaltfläche **Fast Provisioning**.
 - Um Fast Provisioning für virtuelle Maschinen im virtuellen Organisations-Datencenter zu deaktivieren, deaktivieren Sie die Umschaltoption **Fast Provisioning**.
- 6 Klicken Sie auf **Bearbeiten**.


Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC

Sie können ein Organisations-VDC so konfigurieren, dass eine VM-Speicherrichtlinie unterstützt wird, die Sie zuvor dem virtuellen Datacenter des zugrunde liegenden Provider-VDC hinzugefügt haben.

Voraussetzungen

Sie haben die Ziel-VM-Speicherrichtlinie dem virtuellen Provider-Quelldatencenter hinzugefügt. Weitere Informationen finden Sie unter [Hinzufügen einer VM-Speicherrichtlinie zu einem virtuellen Provider-Datencenter](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf die Registerkarte **Speicher** und dann auf **Hinzufügen**.
Sie können eine Liste der verfügbaren zusätzlichen Speicherrichtlinien im virtuellen Provider-Quelldatencenter anzeigen.
- 4 Aktivieren Sie die Kontrollkästchen für eine oder mehrere Speicherrichtlinien, die Sie hinzufügen möchten, und klicken Sie auf **Hinzufügen**.

Ändern der Standardspeicherrichtlinie für ein virtuelles Organisations-Datencenter


Sie können die Standardspeicherrichtlinie ändern, die Sie während der Erstellung eines virtuellen Organisations-Datencenters konfiguriert haben.

vCloud Director verwendet die Standardspeicherrichtlinie für alle VM-Bereitstellungsvorgänge, bei denen keine Speicherrichtlinie auf der VM- oder vApp-Vorlagenebene angegeben wurde.

Voraussetzungen

- Die Ziel-Standardspeicherrichtlinie wird dem virtuellen Organisations-Datencenter hinzugefügt. Weitere Informationen finden Sie unter [Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC](#).
- Die Ziel-Standardspeicherrichtlinie ist auf dem virtuellen Organisations-Datencenter aktiviert. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren einer Speicherrichtlinie in einem virtuellen Organisations-Datencenter](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.


- 3 Klicken Sie auf die Registerkarte **Speicher**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen der gewünschten Standardspeicherrichtlinie und dann auf **Als Standard festlegen**.
- 5 Klicken Sie zur Bestätigung auf **OK**.

Bearbeiten des Grenzwerts einer Speicherrichtlinie für ein virtuelles Organisations-Datencenter

Sie können den Grenzwert der zugewiesenen Speicherkapazität ändern, den Sie während der Erstellung eines virtuellen Organisations-Datencenters für eine Speicherrichtlinie konfiguriert haben.

Sie können die zugewiesene Speicherkapazität als unbegrenzt festlegen oder eine maximale Menge an zugeteilter Speicherkapazität für eine Speicherrichtlinie in einem virtuellen Organisations-Datencenter konfigurieren.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf die Registerkarte **Speicher**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen der gewünschten Speicherrichtlinie und dann auf **Grenzwert bearbeiten**.
- 5 Konfigurieren Sie die Grenzwerteinstellung für diese Speicherrichtlinie.
 - Um einen Grenzwert festzulegen, aktivieren Sie das obere Optionsfeld und geben Sie die maximale Menge an Speicherressourcen für diese Speicherrichtlinie in diesem virtuellen Organisations-Datencenter ein.
 - Um keinen Grenzwert festzulegen, wählen Sie das Optionsfeld **Unbegrenzt** aus.
- 6 Klicken Sie auf **Bearbeiten**.

Ändern der Metadaten für eine VM-Speicherrichtlinie in einem virtuellen Organisations-Datencenter

Sie können Metadaten für eine Speicherrichtlinie in einem virtuellen Organisations-Datencenter hinzufügen, bearbeiten und löschen.

Mithilfe von Objektmetadaten können Sie benutzerdefinierte *Namen=Wert*-Paare mit einer Speicherrichtlinie in einem virtuellen Organisations-Datencenter verknüpfen. Sie können Objektmetadaten in vCloud-API-Abfragefilterausdrücken verwenden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf die Registerkarte **Speicher**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen der gewünschten Speicherrichtlinie und dann auf **Metadaten**.
- 5 Klicken Sie auf **Bearbeiten**.
- 6 (Optional) Um ein Schlüssel-Wert-Paar hinzuzufügen, klicken Sie auf **Hinzufügen**, geben Sie einen Namen und einen Wert ein und wählen Sie einen Typ für das neue Schlüssel-Wert-Paar aus.
- 7 (Optional) Um ein Schlüssel-Wert-Paar zu bearbeiten, geben Sie einen neuen Namen und einen Wert ein und wählen Sie einen neuen Typ für das Schlüssel-Wert-Paar aus.
- 8 (Optional) Um ein Schlüssel-Wert-Paar zu entfernen, klicken Sie am rechten Ende der Zeile auf das Symbol **Löschen**.
- 9 Klicken Sie auf **Speichern** und dann auf **OK**.

Aktivieren oder Deaktivieren einer Speicherrichtlinie in einem virtuellen Organisations-Datencenter


Um zu verhindern, dass zusätzliche vApps und virtuelle Maschinen eine Speicherrichtlinie eines virtuellen Organisations-Datencenters verwenden, können Sie diese Speicherrichtlinie im Organisations-VDC deaktivieren. Laufende vApps und eingeschaltete virtuelle Maschinen laufen weiter, aber Sie können unter dieser Speicherrichtlinie keine zusätzlichen vApps oder virtuellen Maschinen erstellen oder starten.

Die Standardspeicherrichtlinie kann nicht deaktiviert werden.

Voraussetzungen

Wenn Sie die Standardspeicherrichtlinie deaktivieren möchten, finden Sie weitere Informationen unter [Ändern der Standardspeicherrichtlinie für ein virtuelles Organisations-Datencenter](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf die Registerkarte **Speicher**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen der gewünschten Speicherrichtlinie und klicken Sie dann auf **Aktivieren** oder **Deaktivieren**.

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


Löschen einer Speicherrichtlinie aus einem virtuellen Organisations-Datencenter

Um zu verhindern, dass ein virtuelles Organisations-Datencenter eine Speicherrichtlinie verwendet, können Sie diese Speicherrichtlinie aus dem virtuellen Organisations-Datencenter entfernen. Laufende vApps und eingeschaltete virtuelle Maschinen laufen weiter, aber Sie können unter dieser Speicherrichtlinie keine zusätzlichen vApps oder virtuellen Maschinen erstellen oder starten.

Voraussetzungen

Deaktivieren Sie die Speicherrichtlinie, die Sie entfernen möchten. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren einer Speicherrichtlinie in einem virtuellen Organisations-Datencenter](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf die Registerkarte **Speicher**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen der gewünschten Speicherrichtlinie und dann auf **Entfernen**.
- 5 Klicken Sie zur Bestätigung auf **Entfernen**.

Bearbeiten der Netzwerkeinstellungen eines Organisations-VDCs

Sie können den Netzwerkpool ändern, von dem aus neue Netzwerke in einem virtuellen Organisations-Datencenter bereitgestellt werden. Sie können auch eine Option aktivieren, mit der Organisations-VDCs für VDC-übergreifende Netzwerke verwendet werden können.


Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die zur Erstellung von vApp-Netzwerken, gerouteten VDC-Organisationsnetzwerken und internen VDC-Organisationsnetzwerken verwendet werden. Sie können den Netzwerkpool für neue Netzwerke ändern. Vorhandene Netzwerke verwenden weiterhin die alten Netzwerkpools.

Bei Nutzung von Organisations-VDCs, die für VDC-übergreifende Netzwerke aktiviert sind, können Organisationsbenutzer mit entsprechenden Rechten Datencenter-Gruppen und ausgeweitete Layer 2-Netzwerke in diesen Gruppen erstellen.

Voraussetzungen

Wenn Sie VDC-übergreifende Netzwerke für ein Organisations-VDC aktivieren möchten, stellen Sie sicher, dass Sie Cross-vCenter NSX für das stützende virtuelle Provider-Datencenter konfiguriert haben.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf der Registerkarte **Netzwerkpool** in der oberen rechten Ecke auf **Bearbeiten**.
Sie können die Anzahl der Netzwerke sehen, die von diesem Organisations-VDC genutzt werden.
- 4 (Optional) Konfigurieren Sie die Netzwerkpooleinstellungen für dieses Organisations-VDC.
 - Wenn Sie keinen Netzwerkpool für dieses Organisations-VDC wünschen, deaktivieren Sie die Umschaltoption **Netzwerkpool verwenden**.
 - Wenn Sie einen Netzwerkpool für dieses Organisations-VDC konfigurieren möchten, führen Sie die folgenden Schritte aus:
 - a Aktivieren Sie die Umschaltoption **Netzwerkpool verwenden**.
Sie können eine Liste der verfügbaren Netzwerkpools mit Informationen zu deren Verwendung, verfügbaren Netzwerken und Kapazität anzeigen.
 - b Wählen Sie das Optionsfeld neben dem Namen des Zielressourcenpools aus.
 - c Konfigurieren Sie das Kontingent für diesen Netzwerkpool in diesem virtuellen Organisations-Datencenter.
Das Kontingent ist die maximale Anzahl der bereitgestellten Netzwerke. Darf die Anzahl der verfügbaren Netzwerke für den ausgewählten Netzwerkpool nicht überschreiten.
- 5 Um VDC-übergreifende Netzwerke für dieses Organisations-VDC zu aktivieren, aktivieren Sie die Umschaltoption **VDC-übergreifende Netzwerke**.
- 6 Klicken Sie auf **Speichern**.

Ergebnisse


Im vCloud Director-Mandantenportal werden die für VDC-übergreifende Netzwerke aktivierten virtuellen Datencenter auf der Liste der Datencenter für das Erstellen einer Datencenter-Gruppe aufgeführt. Informationen über das Erstellen von Datencenter-Gruppen finden Sie im *Handbuch für das vCloud Director Mandantenportal*.

Ändern der Metadaten für ein virtuelles Organisations-Datencenter

Sie können Metadaten für ein virtuelles Organisations-Datencenter hinzufügen, bearbeiten und löschen.

Mithilfe von Objektmetadaten können Sie benutzerdefinierte *Namen=Wert*-Paare mit einem virtuellen Organisations-Datencenter verknüpfen. Sie können Objektmetadaten in vCloud-API-Abfragefilterausdrücken verwenden.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf die Registerkarte **Metadaten**.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 (Optional) Um ein Schlüssel-Wert-Paar hinzuzufügen, klicken Sie auf **Hinzufügen**, geben Sie einen Namen und einen Wert ein und wählen Sie einen Typ für das neue Schlüssel-Wert-Paar aus.
- 6 (Optional) Um ein Schlüssel-Wert-Paar zu bearbeiten, geben Sie einen neuen Namen und einen Wert ein und wählen Sie einen neuen Typ für das Schlüssel-Wert-Paar aus.
- 7 (Optional) Um ein Schlüssel-Wert-Paar zu entfernen, klicken Sie am rechten Ende der Zeile auf das Symbol **Löschen**.
- 8 Klicken Sie auf **Speichern** und dann auf **OK**.

Anzeigen der Ressourcenpools eines virtuellen Organisations-Datencenters

Sie können eine Liste der vCenter Server-Ressourcenpools anzeigen, die ein virtuelles Organisations-Datencenter verwendet.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs** und klicken Sie auf den Namen des Organisations-VDCs.
- 3 Klicken Sie auf die Registerkarte **Ressourcenpools**.

Ergebnisse

Sie können eine Tabelle mit den Ressourcenpools anzeigen, die vom virtuellen Organisations-Datencenter verwendet werden, und die vCenter Server-Instanz, zu der jeder Ressourcenpool gehört.

Verwalten der Distributed Firewall in einem virtuellen Organisations-Datencenter

Um Layer-3- und Layer-2-Netzwerksicherheit in einem virtuellen Organisations-Datencenter bereitzustellen, können Sie Regeln für die Distributed Firewall in diesem Organisations-VDC aktivieren und erstellen. Mit den Distributed Firewall-Regeln können Sie den Datenverkehr zwischen virtuellen Maschinen in einem virtuellen Organisations-Datencenter schützen.

vCloud Director unterstützt Dienste für verteilte Firewalls in von NSX Data Center for vSphere gestützten Organisations-VDCs.

Zum Erstellen der Regeln für Distributed Firewalls können Sie verschiedene Gruppierungsobjekte und Sicherheitsgruppen verwenden. Weitere Informationen erhalten Sie unter [Benutzerdefiniertes Gruppieren von Objekten](#) und [Arbeiten mit Sicherheitsgruppen](#).


Informationen zum Schützen des Datenverkehrs an und von einem Edge-Gateway finden Sie unter [Verwalten einer Edge-Gateway-Firewall](#).

Aktivieren der Distributed Firewall eines Organisations-VDCs

Bevor Sie die Einstellungen für die Distributed Firewall in einem virtuellen Organisations-Datencenter verwalten können, müssen Sie die Distributed Firewall in diesem Organisations-VDC aktivieren.

vCloud Director unterstützt Dienste für verteilte Firewalls in von NSX Data Center for vSphere gestützten Organisations-VDCs.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4 Aktivieren Sie auf der Registerkarte **Distributed Firewall > Allgemein** die Umschaltoption **Distributed Firewall aktivieren**.

Ergebnisse

Sie können die Standard-Firewallregeln anzeigen, die zulassen, dass der gesamte Layer-2- und Layer-3-Datenverkehr über das Organisations-VDC geleitet wird.

- Auf der Registerkarte **Distributed Firewall > Allgemein** können Sie die standardmäßige Distributed Firewall-Regel für Layer-3-Datenverkehr mit dem Namen „Standardregel ‚Zulassen‘“ sehen.
- Auf der Registerkarte **Distributed Firewall > Ethernet** können Sie die standardmäßige Distributed Firewall-Regel für Layer-2-Datenverkehr mit dem Namen „Standardregel ‚Zulassen‘“ sehen.

Hinzufügen einer Distributed Firewall-Regel


Sie fügen eine Distributed Firewall-Regel zuerst dem Bereich des virtuellen Datacenters der Organisation (Organisations-VDC) hinzu. Anschließend können Sie den Bereich einschränken, auf den Sie die Regel anwenden möchten. Mit der Distributed Firewall können Sie auf Quell- und Zielebene für jede Regel mehrere Objekte hinzufügen und so die Gesamtanzahl der hinzuzufügenden Firewallregeln verringern.

Informationen zu den vordefinierten Diensten und Dienstgruppen, die Sie in einer Regel verwenden können, finden Sie unter [Anzeigen der für Firewallregeln verfügbaren Dienste](#) und [Anzeigen der für Firewallregeln verfügbaren Dienstgruppen](#).

Voraussetzungen


- [Aktivieren der Distributed Firewall eines Organisations-VDCs](#)
- 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.

- 4 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.

- 5 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.

- 6 Klicken Sie in die Zelle **Name** und geben Sie einen Namen ein.
- 7 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	<p>Gilt für Regeln, die auf der Registerkarte Allgemein definiert sind.</p> <p>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.</p>
Auf das Plusymbol (+) klicken	<p>Über das Plusymbol (+) 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>

8 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>

9 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 Zielpports ein oder Beliebig 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.

10 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.

11 Wählen Sie in der Zelle **Richtung** der neuen Regel aus, ob die Regel auf eingehenden Datenverkehr, ausgehenden Datenverkehr oder beides angewendet wird.

- 12 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.
- 13 Markieren Sie die Zelle **Angewendet auf** und definieren Sie mithilfe des Plussymbols (+) den Objektbereich, auf den diese Regel anwendbar ist.

Hinweis Wenn die Regel in den Zellen **Quelle** und **Ziel** virtuelle Maschinen enthält, müssen Sie die virtuellen Quell- und Zielfirewall-Regeln der Zelle **Angewendet auf** der Regel hinzufügen, damit die Regel ordnungsgemäß funktioniert.



- 14 Klicken Sie auf **Änderungen speichern**.

Bearbeiten einer Distributed Firewall-Regel

Verwenden Sie in einer vCloud Director-Umgebung zum Ändern einer vorhandenen Distributed Firewall-Regel eines virtuellen Organisations-Datencenters den Bildschirm **Distributed Firewall**.

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

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4 Führen Sie eine der folgenden Aktionen aus, um Distributed Firewall-Regeln zu verwalten:
 - Deaktivieren Sie eine Regel durch Klicken auf das grüne Häkchen in der Zelle **Nein**.
Das grüne Häkchen verwandelt sich in ein rotes Deaktiviert-Symbol. Wenn die Regel deaktiviert ist und Sie die Regel aktivieren möchten, klicken Sie auf das rote Deaktiviert-Symbol.
 - Bearbeiten Sie einen Regelnamen, indem Sie auf die Zelle **Name** doppelklicken und den neuen Namen eingeben.
 - Ändern Sie die Einstellungen für eine Regel, z. B. die Quell- oder Aktionseinstellungen, indem Sie die entsprechende Zelle auswählen und die angezeigten Steuerelemente verwenden.
 - Löschen Sie eine Regel, indem Sie sie auswählen und oberhalb der Regeltabelle auf die Schaltfläche **Löschen** () klicken.
 - Verschieben Sie eine Regel in der Regeltabelle nach oben oder unten, indem Sie die Regel auswählen und oberhalb der Regeltabelle auf eine der Schaltflächen mit dem Pfeil nach oben oder unten klicken.
- 5 Klicken Sie auf **Änderungen speichern**.

Benutzerdefiniertes Gruppieren von Objekten

Die NSX-Software in der vCloud Director-Umgebung bietet die Möglichkeit, Sätze und Gruppen von bestimmten Entitäten zu definieren, die Sie dann beim Angeben weiterer netzwerkbezogener Konfigurationen verwenden können, z. B. in Firewallregeln.

Erstellen eines IP Sets zur Verwendung in Firewallregeln und bei der DHCP-Relay-Konfiguration

Bei einem IP Set handelt es sich um eine Gruppe von IP-Adressen, die Sie auf Organisations-VDC-Ebene erstellen können. Sie können ein IP Set als Quelle oder Ziel in einer Firewallregel oder in einer DHCP-Relay-Konfiguration verwenden.

Ein IP Set erstellen Sie auf der Seite **Gruppierungsobjekte**. Um diese Seite zu öffnen, müssen Sie entweder zu den Einstellungen der Distributed Firewall des Organisations-VDC oder zu den Diensteinstellungen eines zum Organisations-VDC gehörenden Edge-Gateways navigieren.


Verfahren

- 1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ol style="list-style-type: none"> a Wählen Sie im Hauptmenü (☰) die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Organisations-VDCs. c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. d Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Diensteinstellungen eines Edge-Gateways im Organisations-VDC	<ol style="list-style-type: none"> a Wählen Sie im Hauptmenü (☰) die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Edge-Gateways. c Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. d Klicken Sie auf die Registerkarte 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 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 erstellen ein MAC Set mithilfe der Seite **Gruppierungsobjekte**. Zum Öffnen dieser Seite müssen Sie entweder zu den Distributed Firewall-Einstellungen des Organisations-VDC oder den Dienstinstellungen eines Edge-Gateways navigieren, das zum Organisations-VDC gehört.


Verfahren

- 1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ol style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Organisations-VDCs. c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. d Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Dienstinstellungen eines Edge-Gateways im Organisations-VDC	<ol style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Edge-Gateways. c Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. d Klicken Sie auf die Registerkarte 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 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 mithilfe der Seite **Gruppierungsobjekte** anzeigen. Zum Öffnen dieser Seite müssen Sie entweder zu den Distributed Firewall-Einstellungen des Organisations-VDC oder den Diensteinstellungen eines Edge-Gateways navigieren, das zum Organisations-VDC gehört.

Verfahren

- 1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ol style="list-style-type: none"> Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. Klicken Sie im linken Bereich auf Organisations-VDCs. Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Diensteinstellungen eines Edge-Gateways im Organisations-VDC	<ol style="list-style-type: none"> Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. Klicken Sie im linken Bereich auf Edge-Gateways. Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. Klicken Sie auf die Registerkarte 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 mithilfe der Seite **Gruppierungsobjekte** anzeigen. Zum Öffnen dieser Seite müssen Sie entweder zu den Distributed Firewall-Einstellungen des Organisations-VDC oder den Diensteinstellungen eines Edge-Gateways navigieren, das zum Organisations-VDC gehört.

Verfahren

1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Organisations-VDCs. c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. d Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Diensteseinstellungen eines Edge-Gateways im Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Edge-Gateways. c Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. d Klicken Sie auf die Registerkarte 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.

Arbeiten mit Sicherheitsgruppen

Eine Sicherheitsgruppe ist eine Sammlung von Objekten oder Gruppierungsobjekten, wie z. B. virtuelle Maschinen, VDC-Organisationsnetzwerke oder Sicherheitstags.

Sicherheitsgruppen können dynamische Mitgliedschaftskriterien basierend auf Sicherheitstags, VM-Name, Name des VM-Gastbetriebssystems oder Name des VM-Gasthosts aufweisen. Beispielsweise werden alle virtuellen Maschinen mit dem Sicherheitstag „Web“ automatisch zu einer bestimmten Sicherheitsgruppe hinzugefügt, die für Webserver vorgesehen ist. Nach dem Erstellen einer Sicherheitsgruppe wird eine Sicherheitsrichtlinie auf diese Gruppe angewendet.

Erstellen einer Sicherheitsgruppe



Sie können benutzerdefinierte Sicherheitsgruppen erstellen.

Voraussetzungen

Wenn Sie Sicherheits-Tags mit Sicherheitsgruppen verwenden möchten, nutzen Sie das Verfahren unter [Erstellen und Zuweisen von Sicherheitstags](#).

Verfahren

1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.

- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4 Klicken Sie auf die Registerkarte **Gruppierungsobjekte > Sicherheitsgruppen**.
- 5 Klicken Sie auf die Schaltfläche **Erstellen** ().
- 6 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.
- 7 (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**.
- 8 (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.
- 9 (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.

10 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.




Ergebnisse

Die Sicherheitsgruppe kann jetzt in Regeln, z. B. in Firewallregeln, verwendet werden.

Bearbeiten einer Sicherheitsgruppe

Sie können benutzerdefinierte Sicherheitsgruppen bearbeiten.

Verfahren

- 1** Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2** Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3** Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4** Klicken Sie auf die Registerkarte **Gruppierungsobjekte > Sicherheitsgruppen**.
- 5** Wählen Sie die Sicherheitsgruppe aus, die Sie bearbeiten möchten.
Die Details für die Sicherheitsgruppe werden unter der Liste der Sicherheitsgruppen angezeigt.
- 6** (Optional) Bearbeiten Sie den Namen und die Beschreibung der Sicherheitsgruppe.
- 7** (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**.
- 8** (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**.

- 9 (Optional) Löschen Sie eine dynamische Mitgliedergruppe durch einen Klick auf das Symbol **Löschen** (✕) neben der Mitgliedergruppe, die Sie löschen möchten.
- 10 (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.
- 11 (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.
- 12 Klicken Sie auf **Änderungen speichern**.
Die Änderungen an der Sicherheitsgruppe werden gespeichert.

Löschen einer Sicherheitsgruppe

Sie können eine benutzerdefinierte Sicherheitsgruppe löschen.

Verfahren

- 1 Wählen Sie im Hauptmenü (≡) die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4 Klicken Sie auf die Registerkarte **Gruppierungsobjekte > Sicherheitsgruppen**.
- 5 Wählen Sie die Sicherheitsgruppe aus, die Sie löschen möchten.

6 Klicken Sie auf die Schaltfläche **Löschen** ().

7 Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Ergebnisse

Die Sicherheitsgruppe wird gelöscht.

Arbeiten mit Sicherheitstags

Sicherheitstags sind Beschriftungen, die einer virtuellen Maschine oder einer Gruppe von virtuellen Maschinen zugeordnet werden können. Sicherheitstags sind zur Verwendung mit Sicherheitsgruppen konzipiert. Nachdem Sie die Sicherheitstags erstellt haben, ordnen Sie sie einer Sicherheitsgruppe zu, die in Firewallregeln verwendet werden kann. Sie können ein benutzerdefiniertes Sicherheitstag erstellen, bearbeiten oder zuweisen. Sie können auch anzeigen, für welche virtuellen Maschinen oder Sicherheitsgruppen ein bestimmtes Sicherheitstag angewendet wird.


Ein allgemeiner Anwendungsfall für Sicherheitstags ist die dynamische Gruppierung von Objekten, um Firewallregeln zu vereinfachen. Beispielsweise können Sie mehrere verschiedene Sicherheitstags basierend auf dem Typ der Aktivität erstellen, deren Auftreten Sie für eine bestimmte virtuelle Maschine erwarten. Erstellen Sie ein Sicherheitstag für Datenbankserver und ein Sicherheitstag für E-Mail-Server. Anschließend wenden Sie das entsprechende Tag auf virtuelle Maschinen an, die Datenbankserver oder E-Mail-Server enthalten. Später können Sie das Tag einer Sicherheitsgruppe zuweisen, eine Firewallregel dafür schreiben und verschiedene Sicherheitseinstellungen in Abhängigkeit davon anwenden, ob auf der 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4 Klicken Sie auf die Registerkarte **Sicherheitstags**.

5 Klicken Sie auf die Schaltfläche **Erstellen** () und geben Sie einen Namen für das Sicherheitstag ein.

6 (Optional) Geben Sie eine Beschreibung für das Sicherheitstag ein.

7 (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.

8 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.

2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.

3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.

- 4 Klicken Sie auf die Registerkarte **Sicherheitstags**.
- 5 Wählen Sie in der Liste der Sicherheitstags das Sicherheitstag aus, das Sie bearbeiten möchten, und klicken Sie auf die Schaltfläche **Bearbeiten** ().
- 6 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.
- 7 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.
- 8 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.

- 4 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**.
- 5 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4 Klicken Sie auf die Registerkarte **Sicherheitstags**.
- 5 Wählen Sie aus der Liste der Sicherheitstags das Sicherheitstag aus, das Sie bearbeiten möchten.
- 6 Klicken Sie auf die Schaltfläche **Bearbeiten** ()
- 7 Bearbeiten Sie den Namen und die Beschreibung der Sicherheitstags.

- 8 Weisen Sie das Tag den virtuellen Maschinen zu, die Sie auswählen, oder entfernen Sie die Zuweisung von den ausgewählten virtuellen Maschinen.
- 9 Klicken Sie zum Speichern der Änderungen auf **Behalten**.

Nächste Schritte

Wenn Sie ein Sicherheitstag bearbeiten, müssen Sie möglicherweise auch eine zugeordnete Sicherheitsgruppe oder Firewallregeln bearbeiten. Weitere Informationen zu Sicherheitsgruppen finden Sie unter [Arbeiten mit Sicherheitsgruppen](#).

Löschen eines Sicherheitstags

Sie können ein benutzerdefiniertes Sicherheitstag löschen.

Sie können ein Sicherheitstag löschen, wenn sich die Funktion oder Umgebung der virtuellen Maschine ändert. Wenn Sie z. B. ein Sicherheitstag für Oracle-Datenbanken haben, jedoch einen anderen Datenbankserver verwenden möchten, können Sie das Sicherheitstag entfernen, sodass für Oracle-Datenbanken geltende Firewallregeln nicht mehr für die virtuelle Maschine ausgeführt werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- 4 Klicken Sie auf die Registerkarte **Sicherheitstags**.
- 5 Wählen Sie aus der Liste der Sicherheitstags das Sicherheitstag aus, das Sie löschen möchten.
- 6 Klicken Sie auf die Schaltfläche **Löschen** ()
- 7 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](#).

Verwalten von Edge-Gateways

7

Ein Edge-Gateway stellt für ein virtuelles Organisations-Datencenter-Netzwerk mit Routing die Konnektivität zu anderen Netzwerken her und kann Dienste wie Lastenausgleich, Netzwerkadressübersetzung (NAT) und eine Firewall bereitstellen. vCloud Director unterstützt IPv4- und IPv6-Edge-Gateways.

Edge-Gateways erfordern NSX Data Center for vSphere. Weitere Informationen finden Sie unter *Administratorhandbuch für NSX*.

Ab vCloud Director 9.7 werden die Computing-Arbeitslast und die Netzwerkarbeitslast durch die Verwendung unterschiedlicher vSphere-Ressourcenpools und Speicherrichtlinien isoliert. Edge-Gateways befinden sich auf Edge-Clustern, die Sie zuvor erstellen müssen. Weitere Informationen finden Sie unter [Arbeiten mit Edge-Clustern](#).

Sie können Legacy-Edge-Gateways zu den entsprechenden Edge-Clustern migrieren, indem Sie diese Edge-Gateways erneut bereitstellen. Weitere Informationen finden Sie unter [Edge-Gateway erneut bereitstellen](#).

Wichtig Ab Version 9.7 unterstützt vCloud Director nur erweiterte Edge-Gateways. Sie müssen jedes ältere, nicht erweiterte Edge-Gateway in ein erweitertes Gateway konvertieren. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/66767>.

Dieses Kapitel enthält die folgenden Themen:

- [Arbeiten mit Edge-Clustern](#)
- [Hinzufügen eines Edge-Gateways](#)
- [Konfigurieren von Edge-Gateway-Diensten](#)
- [Anzeigen der Netzwerknutzung und der IP-Zuweisungen auf einem Edge-Gateway](#)
- [Bearbeiten der Edge-Gateway-Eigenschaften](#)
- [Edge-Gateway erneut bereitstellen](#)
- [Löschen eines Edge-Gateways](#)
- [Statistiken und Protokolle für ein Edge-Gateway](#)
- [Aktivieren des SSH-Befehlszeilenzugriffs auf ein Edge-Gateway](#)

Arbeiten mit Edge-Clustern

Um die Computing-Arbeitslasten von den Netzwerkarbeitslasten zu isolieren, führt vCloud Director 9.7 das Edge-Cluster-Objekt ein. Ein Edge-Cluster besteht aus einem vSphere-Ressourcenpool und einer Speicherrichtlinie, die nur für VDC-Organisations-Edge-Gateways verwendet werden. Virtuelle Provider-Datencenter können keine Ressourcen verwenden, die für Edge-Cluster reserviert sind, und Edge-Cluster können keine Ressourcen verwenden, die für virtuelle Provider-Datencenter reserviert sind.

Edge-Cluster stellen eine dedizierte L2-Broadcast-Domäne bereit, die die VLAN-Ausbreitung reduziert und die Netzwerksicherheit und -isolierung sicherstellt. Beispielsweise kann der Edge-Cluster zusätzliche VLANs für das Peering mit physischen Routern enthalten.

Sie können eine beliebige Anzahl von Edge-Clustern erstellen. Sie können einem Organisations-VDC einen Edge-Cluster als primären oder sekundären Edge-Cluster zuweisen.

- Der primäre Edge-Cluster für ein Organisations-VDC wird für die Haupt-Edge-Appliance eines VDC-Organisations-Edge-Gateways verwendet.
- Der sekundäre Edge-Cluster für ein Organisations-VDC wird für die Standby-Edge-Appliance verwendet, wenn sich ein Edge-Gateway im HA-Modus befindet.

Unterschiedliche Organisations-VDCs können Edge-Cluster gemeinsam nutzen oder eigene dedizierte Edge-Cluster aufweisen.

Mit der Version vCloud Director 9.7 ist der alte Prozess für die Verwendung von Metadaten zur Steuerung der Edge-Gateway-Platzierung veraltet. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/2151398>.

Sie können Legacy-Edge-Gateways auf neu erstellte Edge-Cluster migrieren, indem Sie diese Edge-Gateways erneut bereitstellen. Weitere Informationen finden Sie unter [Edge-Gateway erneut bereitstellen](#).

Vorbereiten Ihrer Umgebung für einen Edge-Cluster

- 1 Erstellen Sie in vSphere den Ressourcenpool für den Ziel-Edge-Cluster.

Wenn ein virtuelles Organisations-Datencenter einen VLAN-Netzwerkpool verwendet, müssen sich der VLAN-Netzwerkpool und der Edge-Cluster für dieses virtuelle Organisations-Datencenter auf demselben vSphere Distributed Switch befinden.

- 2 Wenn ein virtuelles Organisations-Datencenter einen VXLAN-Netzwerkpool verwendet, fügen Sie in NSX den Edge-Cluster zur VXLAN-Transportzone hinzu und synchronisieren Sie anschließend den VXLAN-Netzwerkpool in vCloud Director.
- 3 Erstellen Sie in vSphere das Edge-Cluster-Speicherprofil.

Erstellen und Verwalten von Edge-Clustern

Nachdem Sie Ihre Umgebung vorbereitet haben, müssen Sie zum Erstellen und Verwalten von Edge-Clustern die vCloud OpenAPI EdgeClusters-Methoden verwenden. Weitere Informationen finden Sie unter *Erste Schritte mit vCloud OpenAPI* auf <https://code.vmware.com>.

Für das Anzeigen von Edge-Clustern ist das Recht **Edge-Cluster anzeigen** erforderlich. Zum Erstellen, Aktualisieren und Löschen von Edge-Clustern ist das Recht **Edge-Cluster verwalten** erforderlich.

Wenn Sie einen Edge-Cluster erstellen, geben Sie den Namen, den vSphere-Ressourcenpool und den Namen des Speicherprofils an.

Nachdem Sie einen Edge-Cluster erstellt haben, können Sie seinen Namen und seine Beschreibung ändern. Nachdem Sie die zugehörigen Edge-Gateways gelöscht oder verschoben haben, können Sie einen Edge-Cluster löschen.

Zuweisen eines Edge-Clusters zu einem Organisations-VDC

Nachdem Sie einen Edge-Cluster erstellt haben, können Sie diesen Edge-Cluster einem Organisations-VDC zuweisen, indem Sie das Netzwerkprofil des Organisations-VDCs aktualisieren. Sie können einem Organisations-VDC einen Edge-Cluster als primären oder sekundären Edge-Cluster zuweisen.

Wenn Sie keinen sekundären Edge-Cluster zuweisen, wird die Standby-Edge-Appliance eines Edge-Gateways im HA-Modus auf dem primären Edge-Cluster bereitgestellt, aber auf einem anderen Host als dem Host, auf dem die primäre Edge-Appliance ausgeführt wird.

Um Organisations-VDC-Netzwerkprofile zu aktualisieren, anzuzeigen und zu löschen, müssen Sie die vCloud OpenAPI VdcNetworkProfile-Methoden verwenden. Weitere Informationen finden Sie unter *Erste Schritte mit vCloud OpenAPI* auf <https://code.vmware.com>.

Überlegungen:

- Die primären und sekundären Edge-Cluster müssen sich auf demselben vSphere Distributed Switch befinden.
- Wenn das Organisations-VDC einen VXLAN-Netzwerkpool verwendet, muss die NSX-Transportzone den Computing- und den Edge-Cluster umfassen.
- Wenn das Organisations-VDC einen VLAN-Netzwerkpool verwendet, müssen sich die Edge-Cluster und die Computing-Cluster auf demselben vSphere Distributed Switch befinden.

Wenn Sie den primären oder sekundären Edge-Cluster eines Organisations-VDC erneut aktualisieren, um ein vorhandenes Edge-Gateway in den neuen Cluster zu verschieben, müssen Sie dieses Edge-Gateway erneut bereitstellen. Weitere Informationen finden Sie unter [Edge-Gateway erneut bereitstellen](#)

Hinzufügen eines 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.

Ab vCloud Director 9.7 werden Edge-Gateways auf Edge-Clustern bereitgestellt, die Sie zuvor erstellt und dem Organisations-VDC zugewiesen haben.


Sie können ein IPv4- oder IPv6-Edge-Gateway hinzufügen, das eine Verbindung mit einem oder mehreren externen Netzwerken herstellt.

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

Voraussetzungen

- Informationen zu den Systemanforderungen für die Bereitstellung eines Edge-Gateways finden Sie im *Administratorhandbuch für NSX*.
- Wenn Sie das Edge-Gateway auf einem dedizierten Edge-Cluster bereitstellen möchten, erstellen Sie einen Edge-Cluster und weisen Sie diesen dem Organisations-VDC zu. Weitere Informationen finden Sie unter [Arbeiten mit Edge-Clustern](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie dann auf **Neu**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des Organisations-VDCs, in dem Sie das Edge-Gateway erstellen möchten, und klicken Sie auf **Weiter**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für das neue Edge-Gateway ein.
- 5 Sie können jede der folgenden allgemeinen Edge-Gateway-Einstellungen aktivieren oder deaktiviert lassen.

Allgemeine Einstellung	Beschreibung
Distributed Routing	Konfiguriert das Edge-Gateway für die Bereitstellung von verteiltem logischen Routing.
FIPS-Modus	Konfiguriert das Edge-Gateway für die Verwendung des NSX-FIPS-Modus.
Hochverfügbarkeit	Aktiviert automatisches Failover auf ein Sicherungs-Edge-Gateway.

- 6 Wählen Sie die Edge-Gateway-Konfiguration für Ihre Systemressourcen aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Kompakt	Benötigt weniger Arbeitsspeicher- und Rechenressourcen.
Groß	Bietet eine größere Kapazität und eine höhere Leistung als mit der Option „Kompakt“. Große und sehr große Konfigurationen bieten exakt dieselben Sicherheitsfunktionen.
Sehr groß	Wird für Umgebungen verwendet, die über einen Lastausgleichsdienst mit einer großen Anzahl gleichzeitiger Sitzungen verfügen.
Vollständig-4	Wird für Umgebungen mit hohem Durchsatz verwendet. Erfordert eine hohe Verbindungsrate.

- 7 Wählen Sie ein oder mehrere Subnetze aus den externen Netzwerken aus, mit denen das Edge-Gateway eine Verbindung herstellen kann, und klicken Sie auf **Weiter**.

Wenn Sie dem Organisations-VDC einen Edge-Cluster zugewiesen haben, enthält die angezeigte Liste die externen Netzwerke, auf die dieser Edge-Cluster zugreifen kann.

- 8 (Optional) Konfigurieren Sie ein Netzwerk als Standard-Gateway.
- Aktivieren Sie die Umschloption **Standard-Gateway konfigurieren**.
 - Aktivieren Sie das Optionsfeld neben dem Namen des externen Zielnetzwerks und aktivieren Sie das Optionsfeld neben der Ziel-IP-Adresse.
 - (Optional) Aktivieren Sie die Umschloption **Standard-Gateway für DNS-Relay verwenden**.
- 9 Klicken Sie auf **Weiter**.
- 10 Sie können jede der folgenden erweiterten Edge-Gateway-Einstellungen aktivieren oder deaktiviert lassen. Klicken Sie anschließend auf **Weiter**.

Erweiterte Einstellung	Beschreibung
IP-Einstellungen	Sie können manuell eine IP-Adresse für jedes Subnetz auf dem Edge-Gateway angeben.
Unterzuweisung von IP-Pools	Sie können mehrere statische IP-Pools aus den verfügbaren IP-Pools jedes externen Netzwerks auf dem Edge-Gateway unterzuweisen.
Ratengrenzwerte	Sie können den Grenzwert für die eingehende und die ausgehende Rate für jedes aktivierte externe Netzwerk des Edge-Gateways konfigurieren.

- 11 (Optional) Wenn Sie eine oder mehrere erweiterte Einstellungen in [Schritt Schritt 10](#) aktiviert haben, konfigurieren Sie jede aktivierte Einstellung.

Erweiterte Einstellung	Schritte
IP-Einstellungen	<p>Geben Sie für jedes Netzwerk auf dem Edge-Gateway in der Zelle IP-Adressen eine IP-Adresse ein und klicken Sie auf Weiter.</p> <p>Wenn Sie für ein Netzwerk keine IP-Adresse eingeben, weist das System diesem Netzwerk eine beliebige IP-Adresse zu.</p>
Unterzuweisung von IP-Pools	<ol style="list-style-type: none"> Klicken Sie auf das Optionsfeld neben dem Namen eines externen Netzwerks und anschließend auf Bearbeiten. Sie können die verfügbaren IP-Pools für dieses externe Netzwerk und die aktuellen unterzugewiesenen IP-Pools anzeigen, sofern diese konfiguriert sind. Bearbeiten Sie die unterzugewiesenen IP-Pools für dieses externe Netzwerk und klicken Sie auf Speichern. Sie können IP-Adressen und Bereiche aus den Bereichen der verfügbaren IP-Pools hinzufügen. Klicken Sie auf Speichern. Das System kombiniert überlappende IP-Bereiche. Klicken Sie auf Weiter. <p>Hinweis Die Zuweisung von IP-Adressen zu einem Edge-Gateway ist ein Prozess, bei dem der Anbieter dem Gateway den Besitz von IP-Adressen zuweist. vCloud Director konfiguriert die entsprechende Gateway-Schnittstelle mit den sekundären Adressen automatisch während des Zuteilungsvorgangs. Wenn eine oder mehrere der IP-Adressen außerhalb von vCloud Director verwendet werden, kann dies zu IP-Adressenkonflikten führen.</p>
Ratengrenzwerte	<p>Aktivieren Sie für jedes externe Netzwerk auf dem Edge-Gateway die Umschaltoption Aktivieren, geben Sie die Grenzwerte in die Zellen Eingehende Rate und Ausgehende Rate ein und klicken Sie auf Weiter.</p>

- 12 Überprüfen Sie die Seite **Bereit zum Abschließen** und klicken Sie auf **Beenden**.

Konfigurieren von Edge-Gateway-Diensten

Sie können auf einem Edge-Gateway Dienste wie DHCP, Firewall, NAT (Network Address Translation, Netzwerkadressübersetzung) und VPN konfigurieren.

Verwalten einer Edge-Gateway-Firewall

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

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

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

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

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

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

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


Hinzufügen einer Firewallregel für Edge-Gateways

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

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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:

- a Wählen Sie das Dienstprotokoll aus.
- b Geben Sie die Portnummern für die Quell- und Zielports oder **Beliebig** an.
- c Klicken Sie auf **Behalten**.

- 8 Konfigurieren Sie in der Zelle **Aktion** der neuen Regel die Aktion für die Regel.

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

- 9 Klicken Sie auf **Änderungen speichern**.


Der Speichervorgang kann eine Minute dauern.

Ändern der Firewallregeln für Edge-Gateways

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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**.

Anwenden von Syslog-Servereinstellungen auf ein Edge-Gateway

Wenn Sie die Protokollierung für eine oder mehrere Edge-Gateway-Firewallregeln aktiviert haben, stellt das Edge-Gateway eine Verbindung mit dem Syslog-Server her. Wenn Sie ein Edge-Gateway vor der anfänglichen Konfiguration des Syslog-Servers erstellt oder die Syslog-Servereinstellungen geändert haben, müssen Sie die Syslog-Servereinstellungen für dieses Edge-Gateway synchronisieren.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend auf **Syslog synchronisieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Verwalten des DHCP-Protokolls für Edge-Gateways

Sie konfigurieren die Edge-Gateways, um virtuellen Maschinen, die mit den zugeordneten VDC-Organisationsnetzwerken verbunden sind, DHCP-Dienste (Dynamic Host Configuration Protocol) bereitzustellen.

Wie in der [NSX-Dokumentation](#) beschrieben, gehören zu den Funktionen eines NSX-Edge-Gateways IP-Adresspools, die 1:1-Zuordnung statischer IP-Adressen und eine externe DNS-Server-Konfiguration. Die Bindung statischer IP-Adressen basiert auf der verwalteten Objekt- und Schnittstellen-ID der anfordernden virtuellen Client-Maschine.

Der DHCP-Dienst verfährt für ein NSX Edge-Gateway wie folgt:

- Überwacht die interne Schnittstelle des Edge-Gateways zum Zweck der DHCP-Erkennung.
- Verwendet die IP-Adresse der internen Schnittstelle des Edge-Gateways als standardmäßige Gateway-Adresse für alle Clients.

- Die Broadcast- und Subnetzmaskenwerte der internen Schnittstelle werden für das Containernetzwerk verwendet.

In den folgenden Situationen müssen Sie den DHCP-Dienst auf denjenigen virtuellen Client-Maschinen neu starten, die über von DHCP zugewiesene IP-Adressen verfügen:

- Sie haben einen DHCP-Pool, ein Standard-Gateway oder einen DNS-Server geändert bzw. gelöscht.
- Sie haben die interne IP-Adresse der Edge-Gateway-Instanz geändert.

Hinweis Wenn die DNS-Einstellungen eines für DHCP konfigurierten Edge-Gateways geändert werden, stellt das Edge-Gateway möglicherweise keine DHCP-Dienste mehr bereit. Wenn dieser Fall eintritt, verwenden Sie die Option **Status des DHCP-Diensts** auf dem Bildschirm „DHCP-Pools“, um DHCP auf dem Edge-Gateway zu deaktivieren und erneut zu aktivieren. Weitere Informationen finden Sie unter [Hinzufügen eines DHCP-IP-Pools](#).


Hinzufügen eines DHCP-IP-Pools

Sie können die für einen DHCP-Dienst eines erweiterten Edge-Gateways benötigten IP-Pools konfigurieren. DHCP automatisiert die Zuweisung von IP-Adressen zu virtuellen Maschinen, die mit VDC-Organisationsnetzwerken verbunden sind.

Wie in der *Administratordokumentation für NSX* beschrieben, benötigt der DHCP-Dienst einen Pool von IP-Adressen. Ein IP-Pool ist ein sequenzieller Bereich von IP-Adressen innerhalb des Netzwerks. Virtuelle Maschinen, die durch das Edge-Gateway geschützt werden und keine Adressbindung aufweisen, werden einer IP-Adresse aus diesem Pool zugewiesen. Bereiche eines IP-Pools können sich nicht mit anderen Bereichen überschneiden. Daher kann eine IP-Adresse nur zu einem IP-Pool gehören.


Hinweis Es muss mindestens ein DHCP-IP-Pool konfiguriert werden, damit der DHCP-Dienststatus aktiviert wird.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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.
Standard-Gateway	Geben Sie die Adresse des Standard-Gateways ein. Wenn Sie die IP-Adresse des Standard-Gateways nicht eingeben, wird die interne Schnittstelle der Edge-Gateway-Instanz als Standard-Gateway verwendet.
Subnetzmaske	Geben Sie die Subnetzmaske der Edge-Gateway-Schnittstelle ein.
Lease läuft nie ab	Aktivieren Sie diese Option, um die Bindung der aus diesem Pool zugewiesenen IP-Adressen an deren zugewiesene virtuelle Maschinen dauerhaft beizubehalten. Wenn Sie diese Option auswählen, wird die Lease-Zeit auf „Unendlich“ festgelegt.
Lease-Zeit (Sekunden)	Zeitdauer (in Sekunden), die die über DHCP zugewiesenen IP-Adressen für die Clients geleast werden. Die standardmäßige Lease-Zeit beträgt einen Tag (86.400 Sekunden). Hinweis Wenn Sie Lease läuft nie ab auswählen, können Sie keine Lease-Zeit angeben.

- 5 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

vCloud Director aktualisiert das Edge-Gateway, sodass DHCP-Dienste bereitgestellt werden.



Hinzufügen von DHCP-Bindungen

Wenn Sie über auf einer virtuellen Maschine ausgeführte Dienste verfügen, deren IP-Adresse nicht geändert werden soll, können Sie die MAC-Adresse der virtuellen Maschine an die IP-Adresse binden. Die IP-Adresse, die Sie binden, darf sich mit keinem DHCP-IP-Pool überschneiden.

Voraussetzungen

Sie verfügen über die MAC-Adressen für die virtuellen Maschinen, für die Sie Bindungen einrichten möchten.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Domännennamen des DNS-Servers ein.
DNS automatisch konfigurieren	Aktivieren Sie diese Option, um die DNS-Dienstkonfiguration für diese DNS-Bindung zu verwenden. Wenn sie aktiviert ist, werden Primärer Namensserver und Sekundärer Namensserver auf Automatisch festgelegt.
Primärer Namensserver	Wenn Sie DNS automatisch konfigurieren nicht auswählen, geben Sie die IP-Adresse des primären DNS-Servers ein. Diese IP-Adresse wird für die Auflösung von Hostnamen in IP-Adressen verwendet.

Option	Beschreibung
Sekundärer Namensserver	Wenn Sie DNS automatisch konfigurieren nicht auswählen, geben Sie die IP-Adresse des sekundären DNS-Servers ein. Diese IP-Adresse wird für die Auflösung von Hostnamen in IP-Adressen verwendet.
Standard-Gateway	Geben Sie die Adresse des Standard-Gateways ein. Wenn Sie die IP-Adresse des Standard-Gateways nicht eingeben, wird die interne Schnittstelle der Edge-Gateway-Instanz als Standard-Gateway verwendet.
Lease läuft nie ab	Aktivieren Sie diese Option, damit die IP-Adresse dauerhaft an diese MAC-Adresse gebunden wird. Wenn Sie diese Option auswählen, wird die Lease-Zeit auf „Unendlich“ festgelegt.
Lease-Zeit (Sekunden)	Zeitdauer (in Sekunden), die die über DHCP zugewiesenen IP-Adressen für die Clients geleast werden. Die standardmäßige Lease-Zeit beträgt einen Tag (86.400 Sekunden). Hinweis Wenn Sie Lease läuft nie ab auswählen, können Sie keine Lease-Zeit angeben.

3 Klicken Sie auf **Änderungen speichern**.

Konfigurieren von DHCP-Relay für Edge-Gateways

Die DHCP-Relay-Funktion, die von NSX in Ihrer vCloud Director-Umgebung bereitgestellt wird, ermöglicht Ihnen die Nutzung Ihrer vorhandenen DHCP-Infrastruktur von Ihrer vCloud Director-Umgebung aus, ohne die IP-Adressverwaltung in der vorhandenen DHCP-Infrastruktur zu unterbrechen. DHCP-Nachrichten werden von virtuellen Maschinen an die designierten DHCP-Server in Ihrer physischen DHCP-Infrastruktur übertragen. Dadurch wird ermöglicht, dass von der NSX-Software gesteuerte IP-Adressen weiter mit den IP-Adressen in den restlichen DHCP-gesteuerten Umgebungen synchronisiert bleiben.

In der DHCP-Relay-Konfiguration eines Edge-Gateways können verschiedene DHCP-Server aufgelistet werden. Anforderungen werden an alle aufgelisteten Server gesendet. Während der Übertragung der DHCP-Anforderung von den VMs fügt das Edge-Gateway der Anforderung eine Gateway-IP-Adresse hinzu. Der externe DHCP-Server verwendet diese Gateway-Adresse, um einen Pool abzugleichen und eine IP-Adresse für die Anforderung zuzuteilen. Die Gateway-Adresse muss zu einem Subnetz der Schnittstelle des Edge-Gateways gehören.

Sie können einen anderen DHCP-Server für jedes Edge-Gateway angeben und mehrere DHCP-Server auf jedem Edge-Gateway konfigurieren, um mehrere IP-Domänen zu unterstützen.

Hinweis

- DHCP-Relay unterstützt keine überlappenden IP-Adressbereiche.
 - DHCP-Relay und der DHCP-Dienst können nicht gleichzeitig auf der gleichen vNIC ausgeführt werden. Wenn ein Relay-Agent auf einer vNIC konfiguriert ist, kann kein DHCP-Pool in den Subnetzen dieser vNIC konfiguriert werden. Weitere Einzelheiten finden Sie im *NSX-Administratorhandbuch*.
-

Angeben einer DHCP-Relay-Konfiguration für ein Edge-Gateway

Die NSX-Software in Ihrer vCloud Director-Umgebung stellt dem Edge-Gateway die Funktionalität zur Relay-gestützten Weiterleitung von DHCP-Meldungen an DHCP-Server bereit, die sich außerhalb Ihres vCloud Director-Organisations-VDC befinden. Sie können die DHCP-Relay-Funktion des Edge-Gateways konfigurieren.


Wie in der *Administratordokumentation für NSX* beschrieben, können die DHCP-Server mithilfe eines vorhandenen IP Sets, eines IP-Adressblocks, einer Domäne oder einer Kombination aus diesen angegeben werden. DHCP-Meldungen werden an alle angegebenen DHCP-Server weitergeleitet.

Sie müssen auch mindestens einen DHCP-Relay-Agent konfigurieren. Ein DHCP-Relay-Agent ist eine Schnittstelle auf dem Edge-Gateway, von der aus die DHCP-Anforderungen an die externen DHCP-Server weitergeleitet werden.


Voraussetzungen


Wenn Sie mithilfe eines IP-Satzes einen DHCP-Server angeben möchten, stellen Sie sicher, dass der IP-Satz als dem Edge-Gateway zur Verfügung stehendes Gruppierungsobjekt vorhanden ist. Weitere Informationen finden Sie unter [Erstellen eines IP Sets zur Verwendung in Firewallregeln und bei der DHCP-Relay-Konfiguration](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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**.

Hinzufügen einer SNAT- oder DNAT-Regel

Sie können eine Quell-NAT- bzw. SNAT-Regel erstellen, um die Quell-IP-Adresse von einer öffentlichen in eine private IP-Adresse zu ändern oder umgekehrt. Sie können eine Ziel-NAT- bzw. DNAT-Regel erstellen, um die Ziel-IP-Adresse von einer öffentlichen in eine private IP-Adresse zu ändern oder umgekehrt.

Beim Erstellen von NAT-Regeln können Sie die ursprünglichen und übersetzten IP-Adressen mit den folgenden Formaten angeben:


- IP-Adresse – Beispiel: 192.0.2.0
- IP-Adressbereich – Beispiel: 192.0.2.0-192.0.2.24
- IP-Adresse/-Subnetzmaske – Beispiel: 192.0.2.0/24
- any

Bei der Konfiguration einer SNAT- oder DNAT-Regel auf einem Edge-Gateway in der vCloud Director-Umgebung konfigurieren Sie die Regel immer aus der Perspektive des virtuellen Datencenters Ihrer Organisation. Eine SNAT-Regel übersetzt die IP-Quelladresse von Paketen, die von einem VDC-Organisationsnetzwerk an ein externes Netzwerk oder an ein anderes VDC-Organisationsnetzwerk gesendet werden. Eine DNAT-Regel übersetzt die IP-Adresse und optional den Port von Paketen, die von einem VDC-Organisationsnetzwerk empfangen werden und aus einem externen Netzwerk oder einem anderen VDC-Organisationsnetzwerk stammen.

Voraussetzungen

Die öffentliche IP-Adresse muss bereits der Edge-Gateway-Schnittstelle, für die Sie die Regel hinzufügen möchten, hinzugefügt worden sein. Für DNAT-Regeln muss der Edge-Gateway-Schnittstelle die ursprüngliche (öffentliche) IP-Adresse hinzugefügt worden sein, für SNAT-Regeln die übersetzte (öffentliche) IP-Adresse.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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	Geben Sie die erforderliche IP-Adresse ein. Bei dieser Adresse muss es sich um die öffentliche IP-Adresse des Edge-Gateways handeln, für das Sie die DNAT-Regel konfigurieren. Im untersuchten Paket würde diese IP-Adresse oder dieser Bereich die Adressen umfassen, die als IP-Zieladresse des Pakets angezeigt werden. Bei diesen Paket-Zieladressen handelt es sich um die Adressen, die von dieser DNAT-Regel übersetzt werden.
Protokoll	Wählen Sie das Protokoll aus, auf das die Regel angewendet wird. Wenn die Regel für alle Protokolle gelten soll, wählen Sie Alle aus.
Ursprünglicher Port	(Optional) Wählen Sie den Port oder Portbereich aus, über den der eingehende Datenverkehr auf dem Edge-Gateway eine Verbindung zum internen Netzwerk herstellt, in dem die virtuellen Maschinen verbunden sind. Diese Auswahl ist nicht verfügbar, wenn Protokoll auf ICMP oder Alle festgelegt ist.
ICMP-Typ	Wenn Sie ICMP (ein Fehlerberichts- und Diagnose-Dienstprogramm für die geräteübergreifende Kommunikation von Fehlerinformationen) als Protokoll auswählen, wählen Sie im Dropdown-Menü die Option ICMP-Typ aus. ICMP-Meldungen werden anhand des Feldtyps identifiziert. Der ICMP-Typ ist standardmäßig auf „Alle“ festgelegt.
Übersetzte(r) IP/Bereich	Geben Sie die IP-Adresse oder einen Bereich von IP-Adressen ein, in die Zieladressen in eingehenden Paketen übersetzt werden. Bei diesen Adressen handelt es sich um die IP-Adressen der virtuellen Maschine(n), für die Sie DNAT konfigurieren, sodass sie Datenverkehr aus dem externen Netzwerk empfangen können.
Übersetzter Port	(Optional) Wählen Sie den Port oder Portbereich aus, zu dem eingehender Datenverkehr auf den virtuellen Maschinen im internen Netzwerk eine Verbindung herstellt. Dies sind die Ports, in die die DNAT-Regel die Übersetzung für die auf den virtuellen Maschinen eingehenden Pakete vornimmt.

Option	Beschreibung
Beschreibung	(Optional) Geben Sie eine Beschreibung ein, anhand derer die Funktionsweise dieser Regel identifiziert werden kann.
Aktiviert	Aktivieren Sie diese Option, um diese Regel zu aktivieren.
Protokollierung aktivieren	Aktivieren Sie diese Option, damit die Adressübersetzung dieser Regel protokolliert wird.

5 Konfigurieren Sie eine NAT-Quellregel (von innen nach außen).

Option	Beschreibung
Angewendet auf	Wählen Sie die Schnittstelle aus, auf die die Regel angewendet werden soll.
Ursprüngliche(r) Quell-IP/ Quellbereich	Geben Sie die ursprüngliche IP-Adresse oder einen Bereich von IP-Adressen an, die auf diese Regel angewendet werden sollen. Bei diesen Adressen handelt es sich um die IP-Adressen der virtuellen Maschinen, für die Sie die SNAT-Regel konfigurieren, damit diese Datenverkehr an das externe Netzwerk senden können.
Übersetzte(r) Quell-IP/Quellbereich	Geben Sie die erforderliche IP-Adresse ein. Bei dieser Adresse handelt es sich immer um die öffentliche IP-Adresse des Gateways, für das Sie die SNAT-Regel konfigurieren. Gibt die IP-Adresse an, in die Quelladressen (die virtuellen Maschinen) in ausgehenden Paketen übersetzt werden, wenn sie Datenverkehr an das externe Netzwerk senden.
Beschreibung	(Optional) Geben Sie eine Beschreibung ein, anhand derer die Funktionsweise dieser Regel identifiziert werden kann.
Aktiviert	Aktivieren Sie diese Option, um diese Regel zu aktivieren.
Protokollierung aktivieren	Aktivieren Sie diese Option, damit die Adressübersetzung dieser Regel protokolliert wird.

6 Klicken Sie auf **Behalten**, um die Regel der Tabelle auf dem Bildschirm hinzuzufügen.

7 Wiederholen Sie die Schritte, um weitere Regeln zu konfigurieren.

8 Klicken Sie auf **Änderungen speichern**, um die Regeln im System zu speichern.

Nächste Schritte

Fügen Sie die entsprechenden Edge-Gateway-Firewallregeln für die SNAT- oder DNAT-Regeln hinzu, die Sie soeben konfiguriert haben. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Konfiguration für erweitertes Routing

Sie können die statischen und dynamischen Routing-Funktionen konfigurieren, die von der NSX-Software für Ihre Edge-Gateways bereitgestellt werden.

Zur Aktivierung des dynamischen Routings konfigurieren Sie mit dem BGP- (Border Gateway Protocol) oder dem OSPF-Protokoll (Open Shortest Path First) ein erweitertes Edge-Gateway.

Detaillierte Informationen zu den von NSX bereitgestellten Routing-Funktionen finden Sie in der *Administratorokumentation für NSX* unter *Routing*.


Sie können für jedes erweiterte Edge-Gateway statisches und dynamisches Routing angeben. Die dynamische Routing-Funktion stellt die erforderlichen Weiterleitungsinformationen zwischen Layer-2-Broadcast-Domänen zur Verfügung. Auf diese Weise können Sie die Anzahl der Layer-2-Broadcast-Domänen verringern und die Netzwerkeffizienz und -skalierung verbessern. NSX erweitert diese Funktion auf die Speicherorte der Arbeitslasten für horizontales Routing. Diese Funktion ermöglicht mehr direkte Kommunikation zwischen virtuellen Maschinen, ohne dass hierbei der für die Erweiterung von Hops erforderliche Kosten- oder Zeitaufwand entsteht.

Angeben von Standard-Routing-Konfigurationen für das Edge-Gateway

Sie können die Standardeinstellungen für statisches und dynamisches Routing für ein Edge-Gateway angeben.

Hinweis Um alle konfigurierten Routing-Einstellungen zu entfernen, verwenden Sie die Schaltfläche **Globale Konfiguration löschen** unten im Bildschirm **Routing-Konfiguration**. Diese Aktion löscht alle auf den Unterbildschirmen aktuell angegebenen Routing-Einstellungen: Standard-Routing-Einstellungen, statische Routen, OSPF, BGP und Route Redistribution.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Plusymbol (+) verwenden, um eine neue ID einzugeben. Diese Router-ID ist die erste Uplink-IP-Adresse des Edge-Gateways, die Routen zum Kernel für dynamisches Routing überträgt.

- b Konfigurieren Sie die Protokollierung, indem Sie die Option **Protokollierung aktivieren** aktivieren und die Protokollierungsebene auswählen.
- c Klicken Sie auf **OK**.

6 Klicken Sie auf **Änderungen speichern**.

Nächste Schritte

Fügen Sie statische Routen hinzu. Weitere Informationen finden Sie unter [Hinzufügen einer statischen Route](#).

Konfigurieren Sie die Route Redistribution. Weitere Informationen finden Sie unter [Konfigurieren der Route Redistribution](#).

Konfigurieren Sie dynamisches Routing. Lesen Sie hierzu auch folgende Themen:

- [Konfigurieren des BGP-Protokolls](#)
- [Konfigurieren des OSPF-Protokolls](#)

Hinzufügen einer statischen Route



Sie können eine statische Route für ein Zielsubnetz oder einen Zielhost hinzufügen.

Wenn ECMP in der standardmäßigen Routing-Konfiguration aktiviert ist, können Sie mehrere nächste Hops in den statischen Routen angeben. Die Schritte zur Aktivierung von ECMP sind unter [Angaben von Standard-Routing-Konfigurationen für das Edge-Gateway](#) beschrieben.

Voraussetzungen

Wie in der NSX-Dokumentation beschrieben, muss die IP-Adresse des nächsten Hops der statischen Route in einem Subnetz vorhanden sein, das einer der Edge-Gateway-Schnittstellen zugeordnet ist. Andernfalls schlägt die Konfiguration dieser statischen Route fehl.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Edge-Gateways](#).

Konfigurieren des OSPF-Protokolls

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


Das NSX-Edge-Gateway unterstützt OSPF, ein internes Gateway-Protokoll, das IP-Pakete nur innerhalb einer einzelnen Routing-Domäne weiterleitet. Wie in der *Administratordokumentation für NSX* beschrieben, ermöglicht das Konfigurieren von OSPF auf einem NSX-Edge-Gateway es dem Edge-Gateway, Routen zu erlernen und anzukündigen. Das Edge-Gateway verwendet OSPF, um Informationen zum Verbindungszustand von verfügbaren Edge-Gateways zu erfassen und eine Topologiezuordnung des Netzwerks zu erstellen. Die Topologie bestimmt die Routing-Tabelle, die dem Internet Layer präsentiert wird, der Routing-Entscheidungen auf der Grundlage der in den IP-Paketen gefundenen IP-Adresse des Ziels trifft.

Daher bieten OSPF-Routing-Richtlinien einen dynamischen Vorgang des Datenverkehrs-Lastausgleichs zwischen Routen gleicher Kosten. Ein OSPF-Netzwerk ist in Routing-Bereiche aufgeteilt, um den Datenverkehr zu optimieren und die Größe der Routing-Tabellen zu begrenzen. Ein Bereich ist eine logische Sammlung von OSPF-Netzwerken, Routern und Links, die über dieselbe Bereichsidentifikation verfügen. Bereiche werden nach einer Bereichs-ID identifiziert.

Voraussetzungen

Eine Router-ID muss konfiguriert werden. [Angaben von Standard-Routing-Konfigurationen für das Edge-Gateway](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Edge-Gateways](#).


Stellen Sie sicher, dass Route Redistribution und Firewall-Konfiguration das Ankündigen der richtigen Routen zulassen. Weitere Informationen finden Sie unter [Konfigurieren der Route Redistribution](#).

Konfigurieren des BGP-Protokolls

Sie können das BGP-Protokoll (Border Gateway Protocol) für die dynamischen Routing-Funktionen eines Edge-Gateways konfigurieren.

Wie im *NSX-Administratorhandbuch* beschrieben, trifft BGP wichtige Routing-Entscheidungen mithilfe einer Tabelle mit IP-Netzwerken oder -Präfixen, die die Erreichbarkeit des Netzwerks unter verschiedenen autonomen Systemen festlegen. Auf dem Gebiet der Netzwerke bezieht sich der Begriff „BGP-Speaker“ auf ein Netzwerkgerät, das BGP ausführt. Zwei BGP-Speaker stellen eine Verbindung her, bevor Routing-Informationen ausgetauscht werden. Der Begriff „BGP-Nachbar“ bezieht sich auf einen BGP-Speaker, der eine solche Verbindung hergestellt hat. Nachdem die Verbindung hergestellt wurde, tauschen die Geräte Routen aus und synchronisieren ihre Tabellen. Jedes Gerät sendet Keep-Alive-Nachrichten, um diese Beziehung aufrecht zu erhalten.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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.

Option	Beschreibung
Hold Down-Zeit	<p>Das Intervall, für das die Software einen Peer als ausgefallen einstuft, nachdem keine Keepalive-Nachricht erhalten wurde. Dieses Intervall muss dreimal so lang wie das Keepalive-Intervall sein. Das Standardintervall beträgt 180 Sekunden. Nehmen Sie die Anpassungen entsprechend den Anforderungen Ihrer Organisation vor.</p> <p>Sobald Peering zwischen zwei BGP-Nachbarn erreicht ist, startet das Edge-Gateway einen Hold Down-Timer. Jede Keepalive-Nachricht, die es von einem Nachbarn empfängt, setzt den Hold Down-Timer auf 0 zurück. Wenn das Edge-Gateway drei aufeinander folgende Keepalive-Nachrichten nicht empfängt und somit der Hold Down-Timer das Dreifache des Keepalive-Intervalls erreicht, betrachtet das Edge-Gateway den Nachbarn als ausgefallen und löscht die Routen aus diesem Nachbarn.</p>
Kennwort	<p>Wenn dieser BGP-Nachbar Authentifizierung erfordert, geben Sie das Authentifizierungskennwort ein.</p> <p>Jedes Segment, das über die Verbindung zwischen Nachbarn gesendet wird, wird überprüft. MD5-Authentifizierung muss mit demselben Kennwort auf beiden BGP-Nachbarn konfiguriert sein, andernfalls kann die Verbindung zwischen ihnen nicht hergestellt werden.</p>
BGP-Filter	<p>Verwenden Sie diese Tabelle, um Routenfilterung anhand einer Präfixliste von diesem BGP-Nachbarn anzugeben.</p> <hr/> <p>Vorsicht Eine Regel des Typs Alle blockieren 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 ANY oder ein Netzwerk im CIDR-Format ein. ■ Geben Sie das IP-Präfix-GE und IP-Präfix-LE ein, um die Schlüsselwörter le und ge in der Liste der IP-Präfixe zu verwenden.

7 Klicken Sie auf **Änderungen speichern**, um die Konfigurationen im System zu speichern.

Nächste Schritte

Konfigurieren Sie BGP auf den anderen Edge-Gateways, mit denen Sie Routing-Informationen austauschen möchten.

Fügen Sie eine Firewallregel hinzu, die Datenverkehr zu und von den mit BGP konfigurierten Edge-Gateways zulässt. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).


Konfigurieren der Route Redistribution

Standardmäßig gibt der Router nur Routen für andere Router frei, auf denen dasselbe Protokoll ausgeführt wird. Wenn Sie eine Umgebung mit mehreren Protokollen erstellt haben, müssen Sie

die Route Redistribution mit protokollübergreifender Routenfreigabe konfigurieren. Sie können die Route Redistribution für ein Edge-Gateway konfigurieren.

Verfahren


1 Öffnen Sie „Edge-Gateway-Dienste“.

- Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- Klicken Sie im linken Bereich auf **Edge-Gateways**.
- Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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.

- Klicken Sie auf die Schaltfläche **Hinzufügen** ()
- Geben Sie einen Namen und die IP-Adresse des Netzwerks im CIDR-Format ein.
- 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 Netzwerkrouuten anzuwenden.
Learner-Protokoll	Wählen Sie das Protokoll, das Routen von anderen Protokollen unter diesen Neuverteilungskriterien erlernen soll.
Lernen zulassen von	Wählen Sie die Typen von Netzwerken aus, von denen Routen für das in der Liste Learner-Protokoll ausgewählte Protokoll gelernt werden können.
Aktion	Wählen Sie, ob Neuverteilung vom ausgewählten Netzwerktyp zugelassen werden soll oder nicht.

6 Klicken Sie auf **Änderungen speichern**.

Lastausgleich

Der Lastausgleichsdienst verteilt eingehende Dienstanforderungen an mehrere Server und sorgt dabei dafür, dass die Lastverteilung für den Benutzer erkennbar ist. Der Lastausgleich ermöglicht

eine optimale Ressourcennutzung, maximalen Durchsatz und minimale Antwortzeiten und verhindert gleichzeitig eine Überlastung.

Lastausgleich

Der NSX-Lastausgleichsdienst unterstützt zwei Lastausgleichsmodule. Der Ebene-4-Lastausgleich ist paketbasiert und bietet Fast-Path-Verarbeitung. Der Ebene-7-Lastausgleich ist Socket-basiert und unterstützt erweiterte Strategien zur Verwaltung des Datenverkehrs und die DDOS-Minimierung für Back-End-Dienste.

Der Lastausgleich für ein Edge-Gateway wird in der externen Schnittstelle konfiguriert, da das Edge-Gateway den Lastausgleich für den eingehenden Datenverkehr vom externen Netzwerk durchführt. Wenn Sie virtuelle Server für den Lastausgleich konfigurieren, geben Sie eine der verfügbaren IP-Adressen an, über die Sie in Ihrem Organisations-VDC verfügen. Weitere Informationen dazu finden Sie im *vCloud Director-Benutzerhandbuch*.

Strategien und Konzepte für den Lastausgleich

Eine paketbasierte Lastausgleichsstrategie wird auf der TCP- und der UDP-Ebene implementiert. Paketbasierter Lastausgleich hält die Verbindung weder an noch puffert er die gesamte Anforderung. Stattdessen sendet er das geänderte Paket direkt an den ausgewählten Server. TCP- und UDP-Sitzungen werden im Lastausgleichsdienst beibehalten, sodass Pakete für eine einzelne Sitzung an denselben Server geleitet werden. Sie können „Beschleunigung aktiviert“ sowohl in der globalen Konfiguration als auch in der entsprechenden Konfiguration des virtuellen Servers auswählen, um den paketbasierten Lastausgleich zu aktivieren.

Eine Socket-basierte Lastausgleichsstrategie wird zusätzlich zu der Socket-Schnittstelle implementiert. Es werden zwei Verbindungen für eine einzelne Anforderung eingerichtet, nämlich eine clientseitige und eine serverseitige Verbindung. Die serverseitige Verbindung wird nach der Serverauswahl eingerichtet. Bei der HTTP-Socket-basierten Implementierung wird die gesamte Anforderung vor dem Senden an den ausgewählten Server mit optionaler L7-Verarbeitung empfangen. Bei der HTTPS-Socket-Implementierung werden die Authentifizierungsinformationen entweder über die clientseitige Verbindung oder über die serverseitige Verbindung ausgetauscht. Der Socket-basierte Lastausgleich ist der Standardmodus für virtuelle TCP-, HTTP- und HTTPS-Server.

Die grundlegenden Konzepte des NSX-Lastausgleichs sind virtueller Server, Serverpool, Serverpoolmitglied und Dienstüberwachung.

Virtueller Server

Zusammenfassender Begriff für einen Anwendungsdienst, der durch eine eindeutige Kombination aus IP, Port, Protokoll und Anwendungsprofil wie TCP oder UDP dargestellt wird.

Serverpool

Gruppe von Back-End-Servern.

Serverpoolmitglied

Stellt den Back-End-Server als Mitglied in einem Pool dar.

Dienstüberwachung

Definiert, wie der Systemzustand eines Back-End-Servers untersucht wird.

Anwendungsprofil

Stellt die TCP-, UDP-, Persistenz- und Zertifikatkonfiguration für eine bestimmte Anwendung dar.

Übersicht über die Einrichtung

Zunächst legen Sie globale Optionen für den Lastausgleichsdienst fest. Sie erstellen nun einen Serverpool, der aus Back-End-Server-Mitgliedern besteht, und ordnen dem Pool eine Dienstüberwachung zu, damit die Back-End-Server effizient verwaltet und gemeinsam genutzt werden können.

Anschließend erstellen Sie ein Anwendungsprofil, um das allgemeine Anwendungsverhalten in einem Lastausgleichsdienst – Client-SSL, Server-SSL, X-Forwarded-For oder Persistenz – zu definieren. Bei Wahl von Persistenz werden nachfolgende Anforderungen mit ähnlichen Merkmalen gesendet – beispielsweise dass Quell-IP oder Cookie an dasselbe Poolmitglied gesendet werden müssen, ohne dass der Lastausgleichsalgorithmus ausgeführt wird. Das Anwendungsprofil kann auf allen virtuellen Servern wiederverwendet werden.

Anschließend erstellen Sie eine optionale Anwendungsregel, um anwendungsspezifische Einstellungen für die Manipulation von Datenverkehr zu konfigurieren: beispielsweise das Abgleichen eines bestimmten URL- oder Hostnamens, sodass verschiedene Anforderungen von verschiedenen Pools verarbeitet werden können. Anschließend erstellen Sie eine Dienstüberwachung speziell für Ihre Anwendung oder verwenden ggf. eine bereits vorhandene Dienstüberwachung, falls diese Ihre Anforderungen erfüllt.

Optional können Sie eine Anwendungsregel zur Unterstützung von erweiterten Funktionen virtueller L7-Server erstellen. Einige Anwendungsfälle für Anwendungsregeln beinhalten das Wechseln von Inhalten, die Kopfzeilenmanipulation, Sicherheitsregeln und DOS-Schutz.

Abschließend erstellen Sie einen virtuellen Server, der Ihren Serverpool, das Anwendungsprofil und potenzielle Anwendungsregeln miteinander verbindet.


Wenn der virtuelle Server eine Anforderung erhält, berücksichtigt der Lastausgleichsalgorithmus die Poolmitgliedskonfiguration und den Laufzeitstatus. Der Algorithmus berechnet dann den entsprechenden Pool für die Verteilung des Datenverkehrs für ein oder mehrere Mitglieder. Zur Poolmitgliedskonfiguration gehören Einstellungen wie Gewichtung, maximale Verbindung und Bedingungsstatus. Der Laufzeitstatus beinhaltet die aktuellen Verbindungen, die Antwortzeit und Informationen über den Systemstatus. Die Berechnungsmethoden können Round-Robin, gewichtetes Round-Robin, schwächste Verbindung, Quell-IP-Hash, gewichtete schwächste Verbindungen, URL, URI oder HTTP-Header sein.

Jeder Pool wird von der zugehörigen Dienstüberwachung überwacht. Wenn der Lastausgleichsdienst ein Problem bei einem Poolmitglied erkennt, wird das Mitglied als „Nicht erreichbar“ markiert. Beim Auswählen eines Poolmitglieds aus dem Serverpool wird nur ein Server ausgewählt, der als „Erreichbar“ gekennzeichnet ist. Wenn der Serverpool nicht mit einer Dienstüberwachung konfiguriert ist, werden alle Poolmitglieder als „Erreichbar“ betrachtet.

Konfigurieren des Lastausgleichsdiensts

Zu den globalen Konfigurationsparametern des Lastausgleichsdiensts zählen die allgemeine Aktivierung, die Auswahl der Engine für Layer 4 oder Layer 7 und die Angabe der zu protokollierenden Ereignistypen.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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> <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**.
Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

Konfigurieren Sie Anwendungsprofile für den Lastausgleichsdienst. Weitere Informationen finden Sie unter [Erstellen eines Anwendungsprofils](#).



Erstellen eines Anwendungsprofils

Ein Anwendungsprofil definiert das Verhalten des Lastausgleichsdiensts für einen bestimmten Typ des Netzwerkdatenverkehrs. Nach der Profilkonfiguration können Sie es einem virtuellen Server zuordnen. Der virtuelle Server verarbeitet dann den Datenverkehr gemäß den im Profil angegebenen Werten. Durch die Verwendung von Profilen wird Ihre Kontrolle über die Verwaltung des Netzwerkdatenverkehrs verbessert, und die Aufgaben für die Verwaltung des Datenverkehrs werden einfacher und effizienter.

Wenn Sie ein Profil für HTTPS-Datenverkehr erstellen, sind die folgenden HTTPS-Datenverkehrsmuster zulässig:

- Client -> HTTPS -> LB (SSL beenden) -> HTTP -> Server
- Client -> HTTPS -> LB (SSL beenden) -> HTTPS -> Server
- Client -> HTTPS -> LB (SSL-Passthrough) -> HTTPS -> Server
- Client -> HTTP -> LB -> HTTP -> Server

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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.

Option	Beschreibung
HTTP-Umleitungs-URL	(HTTP und HTTPS) Geben Sie die URL ein, an die der Datenverkehr, der an der Zieladresse ankommt, umgeleitet werden soll.
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>
Cookienamen	(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.

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: Bei dieser Option sendet der Server kein Cookie, sondern die Benutzersitzungsinformationen 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 Persistenztafel der App-Sitzung zur Fehlerbehebung anzuzeigen.
Läuft ab in (Sekunden)	<p>Geben Sie eine Zeitdauer in Sekunden ein, für die die Persistenz wirksam bleibt. Dies muss eine positive Ganzzahl im Bereich von 1–86400 sein.</p> <p>Hinweis Beim L7-Lastausgleich mit TCP-Quell-IP-Persistenz kommt es zu einer Zeitüberschreitung des Persistenzeintrags, wenn in einem bestimmten Zeitraum keine neuen TCP-Verbindungen hergestellt werden, selbst wenn die bestehenden Verbindungen noch aktiv sind.</p>
HTTP-Header 'X-Forwarded-For' einfügen	(HTTP und HTTPS) Wählen Sie HTTP-Header 'X-Forwarded-For' einfügen für das Identifizieren der Ursprungs-IP-Adresse eines Clients aus, der eine Verbindung zu einem Webserver über den Lastausgleichsdienst herstellt.
Pool-seitiges SSL aktivieren	(Nur HTTPS) Wählen Sie Pool-seitiges SSL aktivieren aus, um das Zertifikat, die Zertifizierungsstellen oder die CRLs zu definieren, die zur Authentifizierung des Lastausgleichsdiensts über die Serverseite auf der Registerkarte „Pool-Zertifikate“ verwendet werden.

- 6 (Nur HTTPS) Konfigurieren Sie die Zertifikate, die mit dem Anwendungsprofil verwendet werden. Wenn die benötigten Zertifikate nicht vorhanden sind, können Sie diese über die Registerkarte **Zertifikate** erstellen.

Option	Beschreibung
Zertifikate für den virtuellen Server	Wählen Sie das Zertifikat, die Zertifizierungsstellen oder CRLs aus, die zum Entschlüsseln des HTTPS-Datenverkehrs verwendet werden.
Pool-Zertifikate	Definieren Sie das Zertifikat, die Zertifizierungsstellen oder CRLs, die zur Authentifizierung des Lastausgleichsdiensts über die Serverseite verwendet werden. Hinweis Wählen Sie Pool-seitiges SSL aktivieren aus, um diese Registerkarte zu aktivieren.
Schlüssel	Wählen Sie die Schlüsselalgorithmen (oder Verschlüsselungs-Suite) aus, die während des SSL/TLS-Handshakes ausgehandelt wurden.
Clientauthentifizierung	Geben Sie an, ob die Clientauthentifizierung ignoriert werden soll oder erforderlich ist. Hinweis Wenn „Erforderlich“ festgelegt ist, muss der Client nach der Anforderung ein Zertifikat bereitstellen, oder der Handshake wird abgebrochen.

- 7 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.


Nächste Schritte

Fügen Sie eine Dienstüberwachung für den Lastausgleichsdienst hinzu, um Systemdiagnosen für verschiedene Arten von Netzwerkdatenverkehr zu definieren. Weitere Informationen finden Sie unter [Erstellen einer Dienstüberwachung](#).

Erstellen einer Dienstüberwachung

Sie können eine Dienstüberwachung erstellen, um Systemdiagnoseparameter für einen bestimmten Typ des Netzwerkdatenverkehrs zu definieren. Wenn Sie eine Dienstüberwachung einem Pool zuweisen, werden die Poolmitglieder gemäß den Dienstüberwachungsparametern überwacht.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend auf **Dienste**.
- 2 Navigieren Sie zu **Lastausgleichsdienst > Dienstüberwachung**.

3 Klicken Sie auf die Schaltfläche **Erstellen** ()

4 Geben Sie einen Namen für die Dienstüberwachung ein.

5 (Optional) Konfigurieren Sie die folgenden Optionen für die Dienstüberwachung:

Option	Beschreibung
Intervall	Geben Sie das Intervall ein, in dem ein Server unter Verwendung der angegebenen Methode zu überwachen ist.
Zeitüberschreitung	Geben Sie die maximale Zeit in Sekunden ein, in der eine Antwort vom Server empfangen werden muss.
Max. Wiederholungen	Geben Sie an, wie oft die angegebene Methode für die Überwachung hintereinander fehlschlagen muss, bevor der Server als ausgefallen erklärt wird.
Typ	Wählen Sie aus, wie die Systemdiagnoseanforderung an den Server gesendet werden soll: HTTP, HTTPS, TCP, ICMP oder UDP. Je nach ausgewähltem Typ werden die übrigen Optionen im Dialogfeld Neue Dienstüberwachung aktiviert oder deaktiviert.
Erwartet	(HTTP und HTTPS) Geben Sie die Zeichenfolge, deren Übereinstimmung die Überwachung erwartet, in die Statuszeile der HTTP- oder HTTPS-Antwort ein (z. B. HTTP/1.1).
Methode	(HTTP und HTTPS) Wählen Sie die Methode aus, die zum Erkennen des Serverstatus zu verwenden ist.
URL	(HTTP und HTTPS) Geben Sie die URL ein, die in der Serverstatusanforderung zu verwenden ist. Hinweis Wenn Sie die POST-Methode auswählen, müssen Sie einen Wert für Senden angeben.
Senden	(HTTP, HTTPS und UDP) Geben Sie die zu sendenden Daten ein.
Empfangen	(HTTP, HTTPS und UDP) Geben Sie die Zeichenfolge ein, die im Antwortinhalt abgeglichen werden soll. Hinweis Wenn Erwartet nicht übereinstimmt, versucht die Überwachung nicht, den Inhalt von Empfangen abzugleichen.
Erweiterung	(ALLE) Geben Sie erweiterte Überwachungsparameter als Schlüssel=Wert-Paare ein. Beispielsweise bedeutet „warning=10“, dass der Status eines Servers als Warnung festgelegt wird, wenn er nicht innerhalb von 10 Sekunden antwortet. Alle Erweiterungselemente müssen mit einem Wagenrücklaufzeichen getrennt werden. Beispiel: <pre><extension>delay=2 critical=3 escape</extension></pre>

6 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Beispiel: Erweiterungen unterstützt für jedes Protokoll

Tabelle 7-1. Erweiterungen für HTTP/HTTPS-Protokolle

Überwachungserweiterung	Beschreibung
no-body	Wartet nicht auf ein Dokumenthauptteil und beendet Lesevorgang nach dem HTTP/HTTPS-Header. Hinweis HTTP GET oder HTTP POST wird weiterhin gesendet, und keine HEAD-Methode.
max-age= <i>SECONDS</i>	Warnt, wenn ein Dokument älter als SEKUNDEN ist. Die Anzahl kann in der Form „10m“ für Minuten, „10h“ für Stunden oder „10d“ für Tage angegeben werden.
content-type= <i>STRING</i>	Gibt einen Header-Medientyp „Content-Type“ in POST-Aufrufen an.
linespan	Lässt zu, dass regex Zeilenvorschübe überbrückt (muss vor „-r“ oder „-R“ stehen).
regex= <i>STRING</i> oder ereg= <i>STRING</i>	Durchsucht die Seite nach regex-ZEICHENFOLGE.
eregi= <i>STRING</i>	Durchsucht die Seite nach regex-ZEICHENFOLGE, bei der nicht zwischen Groß- und Kleinschreibung unterschieden wird.
invert-regex	Gibt CRITICAL zurück, wenn gefunden, und OK, wenn nicht gefunden.
proxy-authorization= <i>AUTH_PAIR</i>	Gibt Benutzernamen:Kennwort auf Proxyservern mit Standardauthentifizierung an.
useragent= <i>STRING</i>	Sendet die Zeichenfolge im HTTP-Header als User Agent.
header= <i>STRING</i>	Sendet alle anderen Tags in den HTTP-Header. Mehrmalige Verwendung für zusätzliche Header.
onredirect=ok warning critical follow sticky stickyport	Gibt an, wie umgeleitete Seiten verarbeitet werden. sticky ist wie follow, aber ist an die angegebene IP-Adresse gebunden. stickyport stellt sicher, dass sich der Port nicht ändert.
pagesize= <i>INTEGER:INTEGER</i>	Gibt die erforderlichen minimalen und maximalen Seitengrößen in Bytes an.
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.

Tabelle 7-2. Erweiterungen nur für HTTPS-Protokoll

Überwachungserweiterung	Beschreibung
sni	Aktiviert die Unterstützung für die SSL/TLS-Hostnamenerweiterung (SNI).
certificate= INTEGER	Gibt an, wie viele Tage ein Zertifikat mindestens gültig sein muss. Der Port ist standardmäßig auf 443 gesetzt. Wenn diese Option verwendet wird, wird die URL nicht überprüft.
authorization=AUTH_PAIR	Gibt Benutzernamen:Kennwort auf Sites mit Standardauthentifizierung an.

Tabelle 7-3. Erweiterungen für TCP-Protokoll

Überwachungserweiterung	Beschreibung
escape	Ermöglicht die Verwendung von \n, \r, \t oder \ in einer send- oder quit-Zeichenfolge. Muss einer send- oder quit-Option vorangestellt werden. Standardmäßig wird nichts an „send“ angefügt, und \r\n wird ans Ende von „quit“ angefügt.
alle	Gibt an, dass alle erwarteten Zeichenfolgen in einer Serverantwort auftreten müssen. Standardmäßig wird any 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 ok, warn oder crit. Verwendet standardmäßig den Status crit.
mismatch=ok warn crit	Akzeptiert erwartete Zeichenfolgenkonflikte mit dem Status ok, warn oder crit. Verwendet standardmäßig den Status warn.
jail	Blendet die Ausgabe im TCP-Socket aus.
maxbytes= INTEGER	Schließt die Verbindung, wenn mehr als die angegebene Anzahl an Byte empfangen werden.
delay= INTEGER	Wartet die angegebene Anzahl von Sekunden zwischen dem Senden der Zeichenfolge und dem Abrufen einer Antwort.
certificate= INTEGER [, INTEGER]	Gibt an, wie viele Tage ein Zertifikat mindestens gültig sein muss. Der erste Wert ist #days für „warning“, und der zweite Wert ist „critical“ (wenn nicht angegeben, -0).
ssl	Verwendet SSL für die Verbindung.
warning= 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.



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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.



Nächste Schritte

Fügen Sie virtuelle Server für den Lastausgleichsdienst hinzu. Ein virtueller Server hat eine öffentliche IP-Adresse und bedient alle eingehenden Clientanforderungen. Weitere Informationen finden Sie unter [Hinzufügen eines virtuellen Servers](#).

Hinzufügen einer Anwendungsregel

Sie können eine Anwendungsregel schreiben, mit der der IP-Anwendungsdatenverkehr direkt gesteuert und verwaltet werden kann.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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/configuration-1.5.html>.
- 6 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Nächste Schritte



Ordnen Sie die neue Anwendungsregel einem virtuellen Server für den Lastausgleichsdienst hinzu. Weitere Informationen finden Sie unter [Hinzufügen eines virtuellen Servers](#).

Hinzufügen eines virtuellen Servers

Fügen Sie eine interne Edge-Gateway-Schnittstelle oder eine Edge-Gateway-Uplink-Schnittstelle als virtuellen Server hinzu. Ein virtueller Server hat eine öffentliche IP-Adresse und bedient alle eingehenden Clientanforderungen.

Der Lastausgleichsdienst schließt die TCP-Verbindung des Servers standardmäßig nach jeder Clientanforderung.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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.

Option	Beschreibung
Verbindungsgrenzwert	(Optional) Geben Sie die maximale Anzahl an gleichzeitigen Verbindungen ein, die der virtuelle Server verarbeiten kann.
Grenzwert für Verbindungsrate (CPS)	(Optional) Geben Sie die maximale Anzahl an eingehenden neuen Verbindungsanforderungen pro Sekunde ein.

- 5 (Optional) Wenn Sie dem virtuellen Server Anwendungsregeln zuordnen möchten, klicken Sie auf die Registerkarte **Erweitert** und führen Sie folgende Schritte aus:

- a Klicken Sie auf die Schaltfläche **Hinzufügen** ()

Die für den Lastausgleichsdienst erstellten Anwendungsregeln werden angezeigt. Fügen Sie ggf. Anwendungsregeln für den Lastausgleichsdienst hinzu. Weitere Informationen finden Sie unter [Hinzufügen einer Anwendungsregel](#).

- 6 Klicken Sie auf **Beibehalten**, um die Änderungen beizubehalten.

Der Vorgang kann eine Minute dauern.

Nächste Schritte

Erstellen Sie eine Edge-Gateway-Firewallregel, um Datenverkehr zum neuen virtuellen Server (Ziel-IP-Adresse) zuzulassen. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#)

Sicherer Zugriff mit virtuellen privaten Netzwerken

Sie können die VPN-Funktionen konfigurieren, die von der NSX-Software für Ihre Edge-Gateways bereitgestellt werden. Sie können VPN-Verbindungen zu Ihrem Organisations-VDC über einen SSL VPN-Plus-Tunnel, einen IPsec-VPN-Tunnel oder einen L2 VPN-Tunnel konfigurieren.

Wie im *NSX Administratorhandbuch* beschrieben, unterstützt das NSX Edge-Gateway die folgenden VPN-Dienste:

- SSL VPN-Plus, mit dem Remotebenutzer auf private Unternehmensanwendungen zugreifen können.
- IPsec-VPN, das Site-to-Site-Konnektivität zwischen einem NSX Edge-Gateway und Remote-Sites bietet, die auch über NSX oder Hardwarerouter von Drittanbietern oder VPN-Gateways verfügen.
- L2 VPN, das eine Erweiterung Ihres Organisations-VDC zulässt, indem die virtuellen Maschinen Netzwerkkonnektivität unter Verwendung derselben IP-Adresse über geografische Grenzen hinweg beibehalten können.

In einer vCloud Director-Umgebung können Sie die folgenden VPN-Tunnel erstellen:

- Zwischen VDC-Organisationsnetzwerken in derselben Organisation
- Zwischen VDC-Organisationsnetzwerken in verschiedenen Organisationen

- Zwischen einem VDC-Organisationsnetzwerk und einem externen Netzwerk

Hinweis vCloud Director unterstützt nicht mehrere VPN-Tunnel zwischen den gleichen zwei Edge-Gateways. Wenn ein Tunnel zwischen zwei Edge-Gateways besteht und Sie dem Tunnel ein weiteres Subnetz hinzufügen möchten, löschen Sie den VPN-Tunnel und erstellen Sie einen neuen Tunnel, in dem das neue Subnetz enthalten ist.

Nachdem Sie die VPN-Tunnel für ein Edge-Gateway konfiguriert haben, können Sie einen VPN-Client aus einem Remotespeicherort verwenden, um eine Verbindung zu dem Organisations-VDC herzustellen, das von diesem Edge-Gateway unterstützt wird.

Konfigurieren von SSL VPN-Plus

Die SSL VPN-Plus-Dienste für ein Edge-Gateway in einer vCloud Director-Umgebung ermöglichen Remotebenutzern die sichere Verbindung mit den privaten Netzwerken und Anwendungen in den Organisations-VDCs, die von diesem Edge-Gateway unterstützt werden. Sie können verschiedene SSL VPN-Plus-Dienste auf dem Edge-Gateway konfigurieren.

In Ihrer vCloud Director-Umgebung unterstützt die SSL VPN-Plus-Funktion des Edge-Gateways den Netzwerkzugriffsmodus. Remote-Benutzer müssen einen SSL-Client installieren, um sichere Verbindungen und Zugriff auf die Netzwerke und Anwendungen hinter dem Edge-Gateway herzustellen. Im Rahmen der SSL VPN-Plus-Konfiguration des Edge-Gateways fügen Sie die Installationspakete für das Betriebssystem hinzu und konfigurieren bestimmte Parameter. Weitere Informationen finden Sie unter [Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients](#).

Das Konfigurieren von SSL VPN-Plus auf einem Edge-Gateway ist ein mehrstufiger Prozess.

Voraussetzungen

Vergewissern Sie sich, dass alle für SSL VPN-Plus erforderlichen SSL-Zertifikate zum Bildschirm **Zertifikate** hinzugefügt wurden. Weitere Informationen finden Sie unter [SSL-Zertifikatsverwaltung](#).

Hinweis Auf einem Edge-Gateway ist Port 443 der Standardport für HTTPS. Für die SSL VPN-Funktionalität muss der HTTPS-Port des Edge-Gateways für externe Netzwerke zugänglich sein. Der SSL VPN-Client benötigt die IP-Adresse und den Port des Edge-Gateways, die im Bildschirm „Servereinstellungen“ auf der Registerkarte **SSL VPN-Plus** konfiguriert werden, um über das Clientsystem erreichbar zu sein. Weitere Informationen finden Sie unter [Konfigurieren der SSL-VPN-Servereinstellungen](#).

Verfahren

1 Navigieren zum Bildschirm „SSL-VPN Plus“

Sie können zum Bildschirm „SSL-VPN Plus“ navigieren, um mit der Konfiguration des SSL-VPN Plus-Diensts für ein Edge-Gateway zu beginnen.

2 Konfigurieren der SSL-VPN-Servereinstellungen

Mit diesen Servereinstellungen wird der SSL VPN-Server konfiguriert, wie z. B. die IP-Adresse und der Port, der vom Dienst überwacht wird, die Schlüsselliste des Diensts und das Dienstzertifikat. Beim Herstellen einer Verbindung mit dem Edge-Gateway geben die Remotebenutzer dieselbe IP-Adresse und den Port an, die/den Sie in diesen Servereinstellungen festlegen.

3 Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Den Remotebenutzern werden virtuelle IP-Adressen aus den statischen IP-Pools zugewiesen, die Sie über den Bildschirm **IP-Pools** auf der Registerkarte **SSL VPN-Plus** konfigurieren.

4 Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm „Private Netzwerke“ auf der Registerkarte **SSL VPN-Plus**, um die privaten Netzwerke zu konfigurieren. Die privaten Netzwerke sind diejenigen, auf die die VPN-Clients Zugriff haben sollen, wenn die Remotebenutzer eine Verbindung über ihre VPN-Clients und den SSL-VPN-Tunnel herstellen. Die aktivierten privaten Netzwerke werden in der Routing-Tabelle des VPN-Clients installiert.

5 Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm **Authentifizierung** auf der Registerkarte **SSL VPN-Plus**, um einen lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways einzurichten und optional die Authentifizierung von Clientzertifikaten zu aktivieren. Dieser Authentifizierungsserver wird zur Authentifizierung der Benutzer, die eine Verbindung herstellen, verwendet. Alle Benutzer, die im lokalen Authentifizierungsserver konfiguriert sind, werden authentifiziert.

6 Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver

Verwenden Sie den Bildschirm **Benutzer** auf der Registerkarte **SSL VPN-Plus**, um dem lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways Konten für Remotebenutzer hinzuzufügen.

7 Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients

Verwenden Sie den Bildschirm „Installationspakete“ auf der Registerkarte **SSL VPN-Plus**, um benannte Installationspakete des SSL VPN-Plus-Clients für die Remotebenutzer zu erstellen.

8 Bearbeiten der SSL VPN-Plus-Client-Konfiguration

Verwenden Sie den Bildschirm **Client-Konfiguration** auf der Registerkarte **SSL VPN-Plus**, um die Reaktion des SSL VPN-Client-Tunnels anzupassen, wenn sich der Remotebenutzer bei SSL VPN anmeldet.


9 Anpassen der allgemeinen SSL VPN-Plus-Einstellungen für ein Edge-Gateway

Das System legt standardmäßig einige SSL VPN-Plus-Einstellungen für ein Edge-Gateway in Ihrer vCloud Director-Umgebung fest. Auf dem Bildschirm **Allgemeine Einstellungen** auf der Registerkarte **SSL VPN-Plus** im vCloud Director-Mandantenportal können Sie diese Einstellungen anpassen.

Navigieren zum Bildschirm „SSL-VPN Plus“

Sie können zum Bildschirm „SSL-VPN Plus“ navigieren, um mit der Konfiguration des SSL-VPN Plus-Diensts für ein Edge-Gateway zu beginnen.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Edge-Gateway](#).

Konfigurieren der SSL-VPN-Servereinstellungen

Mit diesen Servereinstellungen wird der SSL VPN-Server konfiguriert, wie z. B. die IP-Adresse und der Port, der vom Dienst überwacht wird, die Schlüsselliste des Diensts und das Dienstzertifikat. Beim Herstellen einer Verbindung mit dem Edge-Gateway geben die Remotebenutzer dieselbe IP-Adresse und den Port an, die/den Sie in diesen Servereinstellungen festlegen.

Wenn Ihr Edge-Gateway mit mehreren Overlay-IP-Adressnetzwerken für die externe Schnittstelle konfiguriert ist, kann sich die IP-Adresse, die Sie für den SSL VPN-Server auswählen, von der für die standardmäßige externe Schnittstelle des Edge-Gateways unterscheiden.

Beim Konfigurieren der SSL-VPN-Servereinstellungen müssen Sie den Verschlüsselungsalgorithmus auswählen, der für den SSL-VPN-Tunnel verwendet werden soll. Sie können eine oder mehrere Verschlüsselungen auswählen. Gehen Sie bei der Auswahl der Verschlüsselungen sorgfältig vor und berücksichtigen Sie die Vor- und Nachteile der verschiedenen Verschlüsselungen.

Standardmäßig verwendet das System das selbstsignierte Standardzertifikat, das das System für jedes Edge-Gateway als Standard-Serveridentitätszertifikat für den SSL-VPN-Tunnel generiert. Statt dieses Standardzertifikats können Sie auch ein digitales Zertifikat verwenden, das Sie dem System im Bildschirm **Zertifikate** hinzugefügt haben.

Voraussetzungen

- Vergewissern Sie sich, dass die unter [Konfigurieren von SSL VPN-Plus](#) beschriebenen Voraussetzungen erfüllt sind.
- Wenn Sie ein anderes Dienstzertifikat als das Standardzertifikat verwenden möchten, importieren Sie das erforderliche Zertifikat in das System. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).
- [Navigieren zum Bildschirm „SSL-VPN Plus“](#).

Verfahren

- 1 Klicken Sie im Bildschirm **SSL VPN-Plus** auf **Servereinstellungen**.
- 2 Klicken Sie auf **Aktiviert**.
- 3 Wählen Sie im Dropdown-Menü eine IP-Adresse aus.
- 4 (Optional) Geben Sie eine TCP-Portnummer ein.

Die TCP-Portnummer wird vom SSL-Clientinstallationspaket verwendet. Standardmäßig verwendet das System Port 443. Dies ist der Standardport für HTTPS/SSL-Datenverkehr. Es ist zwar eine Portnummer erforderlich, Sie können aber einen beliebigen TCP-Port für die Kommunikation festlegen.

Hinweis Der SSL VPN-Client benötigt die an dieser Stelle konfigurierte IP-Adresse und den Port, um über die Clientsysteme der Remotebenutzer erreichbar zu sein. Stellen Sie bei einer Änderung der Standardeinstellung für die Portnummer sicher, dass die Kombination aus IP-Adresse und Port über die Systeme der vorgesehenen Benutzer erreichbar ist.

- 5 Wählen Sie in der Schlüsselliste eine Verschlüsselungsmethode aus.
- 6 Konfigurieren Sie die Syslog-Protokollierungsrichtlinie des Diensts.
Die Protokollierung ist standardmäßig aktiviert. Sie können den Grad der Nachrichten, die protokolliert werden sollen, ändern oder die Protokollierung deaktivieren.
- 7 (Optional) Wenn Sie anstelle des vom System generierten selbstsignierten Standardzertifikats ein Dienstzertifikat verwenden möchten, klicken Sie auf **Server-Zertifikat ändern**, wählen Sie ein Zertifikat aus und klicken Sie auf **OK**.
- 8 Klicken Sie auf **Änderungen speichern**.

Nächste Schritte

Hinweis Die von Ihnen festgelegte Edge-Gateway-IP-Adresse und die TCP-Portnummer müssen für die Remotebenutzer erreichbar sein. Fügen Sie eine Edge-Gateway-Firewallregel hinzu, die Zugriff auf die in diesem Verfahren konfigurierte SSL VPN-Plus-IP-Adresse und den Port gestattet. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Fügen Sie einen IP-Pool hinzu, sodass Remotebenutzern IP-Adressen zugewiesen werden, wenn sie eine Verbindung über SSL VPN-Plus herstellen. Weitere Informationen finden Sie unter [Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway](#).

Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Den Remotebenutzern werden virtuelle IP-Adressen aus den statischen IP-Pools zugewiesen, die Sie über den Bildschirm **IP-Pools** auf der Registerkarte **SSL VPN-Plus** konfigurieren.


Jeder in diesem Bildschirm hinzugefügte IP-Pool führt zu einem IP-Adress-Subnetz, das auf dem Edge-Gateway konfiguriert ist. Die in diesen IP-Pools verwendeten IP-Adressbereiche müssen sich von allen anderen auf dem Edge-Gateway konfigurierten Netzwerken unterscheiden.

Hinweis SSL VPN-Plus weist den Remotebenutzern basierend auf der Reihenfolge, in der die IP-Pools in der Tabelle auf dem Bildschirm angezeigt werden, IP-Adressen aus den IP-Pools zu. Nachdem Sie die IP-Pools zur Tabelle auf dem Bildschirm hinzugefügt haben, können Sie ihre Positionen in der Tabelle mit den Pfeiltasten nach oben und unten anpassen.

Voraussetzungen

- [Navigieren zum Bildschirm „SSL-VPN Plus“.](#)
- [Konfigurieren der SSL-VPN-Servereinstellungen.](#)

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **IP-Pools**.
- 2 Klicken Sie auf die Schaltfläche **Erstellen** ().
- 3 Konfigurieren Sie die Einstellungen des IP-Pools.

Option	Aktion
IP-Bereich	Geben Sie einen IP-Adressbereich für diesen IP-Pool ein, wie z. B. 127.0.0.1-127.0.0.9.. Diese IP-Adressen werden VPN-Clients zugewiesen, wenn sie sich authentifizieren und eine Verbindung mit dem SSL-VPN-Tunnel herstellen.
Netzmaske	Geben Sie die Netzmaske des IP-Pools ein, wie z. B. 255.255.255.0 .
Gateway	Geben Sie die IP-Adresse ein, die das Edge-Gateway erstellen soll, und weisen Sie sie als Gateway-Adresse für diesen IP-Pool zu. Beim Erstellen des IP-Pools wird ein virtueller Adapter auf der Edge-Gateway-VM erstellt und diese IP-Adresse auf dieser virtuellen Schnittstelle konfiguriert. Diese IP-Adresse kann eine beliebige IP-Adresse innerhalb des Subnetzes sein, die nicht auch im Bereich des Feldes IP-Bereich liegt.
Beschreibung	(Optional) Geben Sie eine Beschreibung für diesen IP-Pool ein.
Status	Wählen Sie aus, ob dieser IP-Pool aktiviert oder deaktiviert werden soll.
Primäres DNS	(Optional) Geben Sie den Namen des primären DNS-Servers ein, der für die Namensauflösung für diese virtuellen IP-Adressen verwendet wird.

Option	Aktion
Sekundäres DNS	(Optional) Geben Sie den Namen des zu verwendenden sekundären DNS-Servers ein.
DNS-Suffix	(Optional) Geben Sie das DNS-Suffix für die Domäne, in der die Clientsysteme gehostet werden, für eine domänenbasierte Hostnamensauflösung ein.
WINS-Server	(Optional) Geben Sie die Adresse des WINS-Servers entsprechend den Anforderungen Ihrer Organisation ein.

4 Klicken Sie auf **Behalten**.

Ergebnisse

Die IP-Pool-Konfiguration wird zur Tabelle auf dem Bildschirm hinzugefügt.

Nächste Schritte

Fügen Sie private Netzwerke hinzu, auf die die Remotebenutzer bei der Verbindungsherstellung mit SSL VPN-Plus zugreifen können. Weitere Informationen finden Sie unter [Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway](#).

Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm „Private Netzwerke“ auf der Registerkarte **SSL VPN-Plus**, um die privaten Netzwerke zu konfigurieren. Die privaten Netzwerke sind diejenigen, auf die die VPN-Clients Zugriff haben sollen, wenn die Remotebenutzer eine Verbindung über ihre VPN-Clients und den SSL-VPN-Tunnel herstellen. Die aktivierten privaten Netzwerke werden in der Routing-Tabelle des VPN-Clients installiert.


Die privaten Netzwerke sind eine Liste aller erreichbaren IP-Netzwerke hinter dem Edge-Gateway, das Datenverkehr für einen VPN-Client verschlüsseln soll, oder das von der Verschlüsselung ausgeschlossen werden soll. Jedes private Netzwerk, das Zugriff über einen SSL-VPN-Tunnel erfordert, muss als separater Eintrag hinzugefügt werden. Unter Verwendung von Techniken zur Routenzusammenfassung können Sie die Anzahl der Einträge einschränken.

- SSL VPN-Plus ermöglicht Remotebenutzern den Zugriff auf private Netzwerke, basierend auf der Reihenfolge von oben nach unten, in der die IP-Pools in der Tabelle auf dem Bildschirm angezeigt werden. Nachdem Sie die privaten Netzwerke zur Tabelle auf dem Bildschirm hinzugefügt haben, können Sie ihre Positionen in der Tabelle mit den Pfeiltasten nach oben und unten anpassen.
- Wenn Sie für ein privates Netzwerk „TCP-Optimierung aktivieren“ auswählen, funktionieren möglicherweise einige Anwendungen wie z. B. FTP im aktiven Modus nicht innerhalb dieses Subnetzes. Zum Hinzufügen eines FTP-Servers im aktiven Modus müssen Sie ein weiteres privates Netzwerk für diesen FTP-Server hinzufügen und die Option „TCP-Optimierung“ für dieses private Netzwerk deaktivieren. Außerdem muss das private Netzwerk für diesen FTP-Server aktiviert sein und in der Tabelle auf dem Bildschirm über dem TCP-optimierten privaten Netzwerk angezeigt werden.

Voraussetzungen

- Navigieren zum Bildschirm „SSL-VPN Plus“.
- Erstellen eines IP-Pools für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway.

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Private Netzwerke**.
- 2 Klicken Sie auf die Schaltfläche **Hinzufügen** ().
- 3 Konfigurieren Sie die Einstellungen des privaten Netzwerks.

Option	Aktion
Netzwerk	Geben Sie die IP-Adresse des privaten Netzwerks im CIDR-Format ein, wie z. B. 192169.1.0/24 .
Beschreibung	(Optional) Geben Sie eine Beschreibung für das Netzwerk ein.
Datenverkehr senden	<p>Geben Sie an, wie der VPN-Client den Datenverkehr des privaten Netzwerks und des Internets senden soll.</p> <ul style="list-style-type: none"> ■ Über Tunnel <p>Der VPN-Client sendet den Datenverkehr des privaten Netzwerks und des Internets über das Edge-Gateway, auf dem SSL VPN-Plus aktiviert ist.</p> ■ Bypass für Tunnel <p>Der VPN-Client umgeht das Edge-Gateway und sendet den Datenverkehr direkt an den privaten Server.</p>

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 Edge-Gateway](#).

Wichtig Fügen Sie die entsprechenden Firewallregeln hinzu, um den Netzwerkverkehr zu den privaten Netzwerken, die Sie in diesem Bildschirm hinzugefügt haben, zuzulassen. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für Edge-Gateways](#).

Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem Edge-Gateway

Verwenden Sie den Bildschirm **Authentifizierung** auf der Registerkarte **SSL VPN-Plus**, um einen lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways einzurichten und optional die Authentifizierung von Clientzertifikaten zu aktivieren. Dieser Authentifizierungsserver wird zur Authentifizierung der Benutzer, die eine Verbindung herstellen, verwendet. Alle Benutzer, die im lokalen Authentifizierungsserver konfiguriert sind, werden authentifiziert.

Es kann nur ein lokaler SSL-VPN-Plus-Authentifizierungsserver auf dem Edge-Gateway konfiguriert werden. Wenn Sie auf **+ Lokal** klicken und weitere Authentifizierungsserver angeben, wird beim Versuch, die Konfiguration zu speichern, eine Fehlermeldung angezeigt.

Die maximale Zeit für die Authentifizierung über SSL-VPN beträgt drei (3) Minuten. Dieser Maximalwert wird durch die Nichtauthentifizierungs-Zeitüberschreitung festgelegt, die standardmäßig 3 Minuten beträgt und nicht konfigurierbar ist. Wenn mehrere Authentifizierungsserver in der Autorisierungskette vorhanden sind und die Benutzerauthentifizierung länger als 3 Minuten dauert, wird der Benutzer infolgedessen nicht authentifiziert.

Voraussetzungen

- [Navigieren zum Bildschirm „SSL-VPN Plus“.](#)
- [Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem Edge-Gateway.](#)
- Wenn Sie die Clientzertifikatauthentifizierung aktivieren möchten, stellen Sie sicher, dass ein CA-Zertifikat zum Edge-Gateway hinzugefügt wurde. Weitere Informationen finden Sie unter [Hinzufügen eines CA-Zertifikats zum Edge-Gateway für die Überprüfung der Vertrauenswürdigkeit von SSL-Zertifikaten.](#)

Verfahren

- 1 Klicken Sie auf die Registerkarte **SSL VPN-Plus** und anschließend auf **Authentifizierung**.
- 2 Klicken Sie auf **Lokal**.

3 Konfigurieren Sie die Einstellungen des Authentifizierungsservers.

a (Optional) Aktivieren und konfigurieren Sie die Kennwortrichtlinie.

Option	Beschreibung
Kennwortrichtlinie aktivieren	Aktivieren Sie die Durchsetzung der Einstellungen für die Kennwortrichtlinie, die Sie hier konfigurieren.
Kennwortlänge	Geben Sie die zulässige minimale und maximale Zeichenanzahl für die Kennwortlänge ein.
Mindestanzahl Buchstaben	(Optional) Geben Sie die Mindestanzahl von Buchstabe ein, die für das Kennwort erforderlich sind.
Mindestanzahl Ziffern	(Optional) Geben Sie die Mindestanzahl von numerischen Zeichen ein, die für das Kennwort erforderlich sind.
Mindestanzahl Sonderzeichen	(Optional) Geben Sie die Mindestanzahl der Sonderzeichen ein, beispielsweise kaufmännisches Und-Zeichen (&), Hashtag (#), Prozentzeichen (%) usw., die für das Kennwort erforderlich sind.
Kennwort darf keine Benutzer-ID enthalten	(Optional) Aktivieren Sie diese Option, um durchzusetzen, dass das Kennwort nicht die Benutzer-ID enthalten darf.
Kennwort läuft ab in	(Optional) Geben Sie die maximale Gültigkeitsdauer in Tagen für ein Kennwort ein, bevor der Benutzer es ändern muss.
Ablaufbenachrichtigung in	(Optional) Geben Sie die Anzahl der Tage vor dem Wert Kennwort läuft ab in ein, bei dem der Benutzer benachrichtigt wird, dass das Kennwort in Kürze abläuft.

b (Optional) Aktivieren und konfigurieren Sie die Kontosperrungsrichtlinie.

Option	Beschreibung
Kontosperrungsrichtlinie aktivieren	Aktivieren Sie die Durchsetzung der Einstellungen für die Kontosperrungsrichtlinie, die Sie hier konfigurieren.
Wiederholungsanzahl	Geben Sie die Anzahl der Zugriffsversuche ein, die ein Benutzer auf sein Konto hat.
Wiederholungsdauer	Geben Sie das Zeitintervall in Minuten ein, nach dessen Ablauf das Konto des Benutzers bei fehlgeschlagenen Anmeldeversuchen gesperrt wird. Wenn Sie beispielsweise für Wiederholungsanzahl den Wert 5 und für Wiederholungsdauer 1 Minute festlegen, wird das Konto des Benutzers nach 5 fehlgeschlagenen Anmeldeversuchen innerhalb einer Minute gesperrt.
Sperrdauer	Geben Sie den Zeitraum ein, für den das Benutzerkonto gesperrt bleibt. Nach Ablauf dieses Zeitraums wird die Kontosperrung automatisch aufgehoben.

c Aktivieren Sie im Abschnitt „Status“ diesen Authentifizierungsserver.

- d (Optional) Konfigurieren Sie die sekundäre Authentifizierung.

Optionen	Beschreibung
Diesen Server für die sekundäre Authentifizierung verwenden	(Optional) Geben Sie an, ob der Server als zweite Authentifizierungsebene verwendet werden soll.
Sitzung bei Fehlschlag der Authentifizierung beenden	(Optional) Geben Sie an, ob die VPN-Sitzung beendet werden soll, wenn die Authentifizierung fehlschlägt.

- e Klicken Sie auf **Behalten**.

- 4 (Optional) Um die Clientzertifikatauthentifizierung zu aktivieren, klicken Sie auf **Zertifikat ändern**, aktivieren Sie die Umschaltoption für die Aktivierung und wählen Sie das zu verwendende CA-Zertifikat aus. Klicken Sie anschließend auf **OK**.

Nächste Schritte

Fügen Sie dem lokalen Authentifizierungsserver lokale Benutzer hinzu, damit diese eine Verbindung mit SSL VPN-Plus herstellen können. Weitere Informationen finden Sie unter [Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver](#).

Erstellen Sie ein Installationspaket, das den SSL-Client enthält, damit Remotebenutzer ihn auf ihren lokalen Systemen installieren können. Weitere Informationen finden Sie unter [Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients](#).

Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver

Verwenden Sie den Bildschirm **Benutzer** auf der Registerkarte **SSL VPN-Plus**, um dem lokalen Authentifizierungsserver für den SSL VPN-Dienst des Edge-Gateways Konten für Remotebenutzer hinzuzufügen.


Hinweis Wenn noch kein lokaler Authentifizierungsserver konfiguriert wurde, wird durch das Hinzufügen eines Benutzers im Bildschirm **Benutzer** automatisch ein lokaler Authentifizierungsserver mit Standardwerten hinzugefügt. Über die Schaltfläche „Bearbeiten“ im Bildschirm **Authentifizierung** können Sie die Standardwerte anzeigen und bearbeiten. Informationen zur Verwendung des Bildschirms **Authentifizierung** finden Sie unter [Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem Edge-Gateway](#).

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Benutzer**.

- 2 Klicken Sie auf die Schaltfläche **Erstellen** ()

3 Konfigurieren Sie die folgenden Optionen für den Benutzer:

Option	Beschreibung
Benutzer-ID	Geben Sie die Benutzer-ID ein.
Kennwort	Geben Sie ein Kennwort für den Benutzer ein.
Kennwort erneut eingeben	Geben Sie das Kennwort erneut ein.
Vorname	(Optional) Geben Sie den Vornamen des Benutzers ein.
Nachname	(Optional) Geben Sie den Nachnamen des Benutzers ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für den Benutzer ein.
Aktiviert	Geben Sie an, ob der Benutzer aktiviert oder deaktiviert ist.
Kennwort läuft nie ab	(Optional) Geben Sie an, ob für diesen Benutzer dasselbe Kennwort beibehalten werden soll.
Kennwortänderung erlauben	(Optional) Geben Sie an, ob der Benutzer das Kennwort ändern kann.
Kennwort bei der nächsten Anmeldung ändern	(Optional) Geben Sie an, ob dieser Benutzer das Kennwort bei der nächsten Anmeldung ändern muss.

4 Klicken Sie auf **Behalten**.

5 Wiederholen Sie die Schritte, um weitere Benutzer hinzuzufügen.

Nächste Schritte

Fügen Sie dem lokalen Authentifizierungsserver lokale Benutzer hinzu, damit diese eine Verbindung mit SSL VPN-Plus herstellen können. Weitere Informationen finden Sie unter [Hinzufügen von SSL VPN-Plus-Benutzern zum lokalen SSL VPN-Plus-Authentifizierungsserver](#).

Erstellen Sie ein Installationspaket mit dem SSL-Client, damit Remotebenutzer diesen auf ihren lokalen Systemen installieren können. Weitere Informationen finden Sie unter [Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients](#).

Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients

Verwenden Sie den Bildschirm „Installationspakete“ auf der Registerkarte **SSL VPN-Plus**, um benannte Installationspakete des SSL VPN-Plus-Clients für die Remotebenutzer zu erstellen.


Sie können dem Edge-Gateway ein Installationspaket des SSL VPN-Plus-Clients hinzufügen. Neue Benutzer werden zum Herunterladen und Installieren dieses Pakets aufgefordert, wenn sie sich anmelden, um die VPN-Verbindung zum ersten Mal zu nutzen. Diese Clientinstallationspakete können nach dem Hinzufügen vom FQDN der öffentlichen Schnittstelle des Edge-Gateways heruntergeladen werden.


Sie können Installationspakete erstellen, die unter Windows-, Linux- und Mac-Betriebssysteme ausgeführt werden. Wenn Sie unterschiedliche Installationsparameter pro SSL VPN-Client benötigen, erstellen Sie ein Installationspaket für jede Konfiguration.

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“](#)

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im Mandantenportal auf **Installationspakete**.
- 2 Klicken Sie auf die Schaltfläche **Hinzufügen** ()
- 3 Konfigurieren Sie die Einstellungen für das Installationspaket.

Option	Beschreibung
Profilname	Geben Sie einen Profilnamen für dieses Installationspaket ein. Dieser Name wird dem Remotebenutzer angezeigt, um diese SSL-VPN-Verbindung zum Edge-Gateway zu identifizieren.
Gateway	Geben Sie die IP-Adresse oder den FQDN der öffentlichen Schnittstelle des Edge-Gateways ein. Die IP-Adresse oder der FQDN, die bzw. den Sie eingeben, ist an den SSL-VPN-Client gebunden. Wenn der Client auf dem lokalen System des Remotebenutzers installiert ist, wird diese IP-Adresse bzw. dieser FQDN auf diesem SSL VPN-Client angezeigt. Um zusätzliche Edge-Gateway-Uplink-Schnittstellen an diesen SSL-VPN-Client zu binden, klicken Sie auf die Schaltfläche Hinzufügen ()
Port	(Optional) Um den Portwert des angezeigten Standardwerts zu ändern, doppelklicken Sie auf den Wert und geben Sie einen neuen Wert ein.
Windows Linux Mac	Wählen Sie die Betriebssysteme aus, für die Sie die Installationspakete erstellen möchten.
Beschreibung	(Optional) Geben Sie eine Beschreibung für den Benutzer ein.
Aktiviert	Geben Sie an, ob dieses Paket aktiviert oder deaktiviert ist.

- 4 Wählen Sie die Installationsparameter für Windows aus.

Option	Beschreibung
Client bei der Anmeldung starten	Startet den SSL-VPN-Client, wenn sich der Remotebenutzer beim lokalen System anmeldet.
Kennwortspeicherung erlauben	Lässt zu, dass der Client das Kennwort des Benutzers speichert.
Unbeaufsichtigten Installationsmodus aktivieren	Blendet die Installationsbefehle der Remotebenutzer aus.
SSL-Client-Netzwerkadapter ausblenden	Blendet den VMware SSL VPN-Plus-Adapter aus, der zusammen mit dem Installationspaket des SSL-VPN-Clients auf dem Computer des Remotebenutzers installiert wird.
Taskleistensymbol für Client ausblenden	Mit dieser Option können Sie das SSL VPN-Taskleistensymbol, das angibt, ob die VPN-Verbindung aktiv ist oder nicht, ausblenden.
Desktopsymbol erstellen	Erstellt auf dem Desktop des Benutzers ein Symbol zum Aufrufen des SSL-Clients.

Option	Beschreibung
Unbeaufsichtigten Betriebsmodus aktivieren	Blendet das Fenster mit der Information, dass die Installation abgeschlossen ist, aus.
Validierung des Serversicherheitszertifikats	Der SSL VPN-Client prüft das SSL VPN-Serverzertifikat, bevor die sichere Verbindung hergestellt wird.

5 Klicken Sie auf **Behalten**.

Nächste Schritte

Bearbeiten Sie die Clientkonfiguration. Weitere Informationen finden Sie unter [Bearbeiten der SSL VPN-Plus-Client-Konfiguration](#).

Bearbeiten der SSL VPN-Plus-Client-Konfiguration

Verwenden Sie den Bildschirm **Client-Konfiguration** auf der Registerkarte **SSL VPN-Plus**, um die Reaktion des SSL VPN-Client-Tunnels anzupassen, wenn sich der Remotebenutzer bei SSL VPN anmeldet.

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“](#)

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Client-Konfiguration**.
- 2 Wählen Sie den **Tunneling-Modus** aus.
 - Im Split-Tunnel-Modus fließt nur der VPN-Datenverkehr über das Edge-Gateway.
 - Im Full-Tunnel-Modus wird das Edge-Gateway zum Standard-Gateway des Remotebenutzers und der gesamte Datenverkehr (z. B. VPN, lokal und Internet) wird über dieses Gateway geleitet.
- 3 Geben Sie bei Verwendung des Full-Tunnel-Modus die IP-Adresse für das Standard-Gateway ein, das von den Clients der Remotebenutzer verwendet wird. Wählen Sie optional aus, ob der Datenverkehr im lokalen Subnetz von der Leitung über den VPN-Tunnel ausgeschlossen werden soll.
- 4 (Optional) Deaktivieren Sie die automatische erneute Verbindungsherstellung.

Automatische erneute Verbindungsherstellung aktivieren ist standardmäßig aktiviert. Wenn die automatische erneute Verbindungsherstellung aktiviert ist, verbindet der SSL VPN-Client Benutzer, deren Verbindung getrennt wurde, automatisch erneut.
- 5 (Optional) Aktivieren Sie optional auch die Möglichkeit für den Client, Remotebenutzer zu benachrichtigen, wenn ein Client-Upgrade verfügbar ist.

Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option aktivieren, können Remotebenutzer wahlweise das Upgrade installieren.
- 6 Klicken Sie auf **Änderungen speichern**.

Anpassen der allgemeinen SSL VPN-Plus-Einstellungen für ein Edge-Gateway

Das System legt standardmäßig einige SSL VPN-Plus-Einstellungen für ein Edge-Gateway in Ihrer vCloud Director-Umgebung fest. Auf dem Bildschirm **Allgemeine Einstellungen** auf der Registerkarte **SSL VPN-Plus** im vCloud Director-Mandantenportal können Sie diese Einstellungen anpassen.

Voraussetzungen

[Navigieren zum Bildschirm „SSL-VPN Plus“.](#)

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Allgemeine Einstellungen**.
- 2 Bearbeiten Sie die allgemeinen Einstellungen entsprechend den Anforderungen Ihrer Organisation.

Option	Beschreibung
Mehrere Anmeldungen mit demselben Benutzernamen verhindern	Aktivieren Sie diese Einstellung, um einen Remotebenutzer auf eine aktive Anmeldungssitzung unter demselben Benutzernamen zu beschränken.
Komprimierung	Aktivieren Sie diese Einstellung, um die TCP-basierte intelligente Datenkomprimierung zu aktivieren und die Datenübertragungsgeschwindigkeit zu erhöhen.
Protokollierung aktivieren	Aktivieren Sie diese Einstellung, um ein Protokoll des Datenverkehrs bereitzustellen, der über das SSL VPN-Gateway geleitet wird. Die Protokollierung ist standardmäßig aktiviert.
Virtuelle Tastatur erzwingen	Aktivieren Sie diese Einstellung, um festzulegen, dass Remotebenutzer nur für die Eingabe von Anmeldeinformationen eine virtuelle Tastatur (Bildschirmtastatur) verwenden müssen.
Tasten der virtuellen Tastatur zufällig anordnen	Aktivieren Sie diese Einstellung, damit für die virtuelle Tastatur ein zufallsgeneriertes Tastenlayout verwendet wird.
Sitzungszeitüberschreitung bei Leerlauf	Geben Sie die Zeitüberschreitung der Sitzung bei Leerlauf in Minuten ein. Wenn während des angegebenen Zeitraums in der Sitzung eines Benutzers keine Aktivität stattfindet, wird die Sitzung des Benutzers getrennt. Der Standardwert des Systems ist 10 Minuten.
Benutzerbenachrichtigung	Geben Sie die Nachricht ein, die Remotebenutzern nach der Anmeldung angezeigt werden soll.
Öffentlichen URL-Zugriff aktivieren	Aktivieren Sie diese Einstellung, damit Remotebenutzer auf Sites zugreifen können, die nicht explizit von Ihnen für den Zugriff durch Remotebenutzer konfiguriert wurden.
Erzwungene Zeitüberschreitung aktivieren	Aktivieren Sie diese Einstellung, damit das System die Verbindung zu Remotebenutzern trennt, nachdem der Zeitraum verstrichen ist, den Sie im Feld Erzwungene Zeitüberschreitung angegeben haben.
Erzwungene Zeitüberschreitung	Geben Sie das Zeitlimit in Minuten ein. Dieses Feld wird angezeigt, wenn die Umschaltoption Erzwungene Zeitüberschreitung aktivieren aktiviert ist.

3 Klicken Sie auf **Änderungen speichern**.

Konfigurieren von IPsec-VPN

Die Edge-Gateways in einer vCloud Director-Umgebung unterstützen Site-to-Site Internet Protocol Security (IPsec), um sichere VPN-Tunnel zwischen VDC-Organisationsnetzwerken oder zwischen einem VDC-Organisationsnetzwerk und einer externen IP-Adresse einzurichten. Sie können den IPsec-VPN-Dienst auf einem Edge-Gateway konfigurieren.

Die Einrichtung einer IPsec-VPN-Verbindung von einem Remotenetzwerk zum Organisations-VDC ist das häufigste Szenario. Die NSX-Software stellt die IPsec-VPN-Funktionen eines Edge-Gateways bereit, u. a. Unterstützung für Zertifikatsauthentifizierung, vorinstallierter Schlüssellmodus und IP-Unicast-Datenverkehr zwischen dem Edge-Gateway und VPN-Remote-Routern. Sie können auch mehrere Subnetze für die Verbindung über IPsec-Tunnel mit dem internen Netzwerk hinter einem Edge-Gateway konfigurieren. Wenn Sie mehrere Subnetze für die Verbindung über IPsec-Tunnel mit dem internen Netzwerk konfigurieren, dürfen diese Subnetze und das interne Netzwerk hinter dem Edge-Gateway keine überlappenden Adressbereiche aufweisen.

Hinweis Wenn der lokale und der Remote-Peer eines IPsec-Tunnels überlappende IP-Adressen haben, ist die Datenverkehrsweiterleitung über den Tunnel möglicherweise inkonsistent, abhängig davon, ob lokal verbundene Routen und autoPlumbed-Routen vorhanden sind.

Die folgenden IPsec-VPN-Algorithmen werden unterstützt:

- AES (AES128-CBC)
- AES256 (AES265-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie-Hellman-Gruppe 2)
- DH-5 (Diffie-Hellman-Gruppe 5)
- DH-14 (Diffie-Hellman-Gruppe 14)

Hinweis Dynamische Routing-Protokolle werden mit IPsec-VPN nicht unterstützt. Wenn Sie einen IPsec-VPN-Tunnel zwischen einem Edge-Gateway der VDC-Organisation und einem physisches Gateway-VPN an einer Remote-Site konfigurieren, können Sie für diese Verbindung kein dynamisches Routing konfigurieren. Die IP-Adresse dieser Remote-Site kann nicht durch dynamisches Routing auf dem Edge-Gateway-Uplink gelernt werden.

Wie im Thema *Überblick über IPsec-VPN* im *NSX-Administratorhandbuch* beschrieben, wird die maximale Anzahl unterstützter Tunnel auf einem Edge-Gateway von seiner konfigurierten Größe bestimmt: „Kompakt“, „Groß“, „Vollständig“, „Vollständig-4“. Sie können die Größe des Edge-Gateways anzeigen, indem Sie sich bei der vCloud Director-Webkonsole anmelden, zum Edge-Gateway navigieren und die Aktion **Eigenschaften** verwenden, um die Edge-Gateway-Konfiguration anzuzeigen. Unter *vCloud Director-Administratorhandbuch* finden Sie weitere Informationen zur Verwendung der vCloud Director-Webkonsole.

Das Konfigurieren von IPsec-VPN auf einem Edge-Gateway ist ein mehrstufiger Prozess.

Hinweis Wenn eine Firewall zwischen den Tunnel-Endpoints vorhanden ist, müssen Sie nach dem Konfigurieren des IPsec-VPN-Diensts die Firewallregeln aktualisieren, um die folgenden IP-Protokolle und UDP-Ports zuzulassen:

- IP Protocol ID 50 (ESP)
 - IP Protocol ID 51 (AH)
 - UDP-Port 500 (IKE)
 - UDP-Port 4500
-

Verfahren

1 Navigieren zum Bildschirm „IPsec-VPN“

Im Bildschirm **IPsec-VPN** können Sie den IPsec-VPN-Dienst für ein Edge-Gateway konfigurieren.

2 Konfigurieren von IPsec-VPN-Site-Verbindungen für das Edge-Gateway

Verwenden Sie den Bildschirm **IPsec-VPN-Sites** im vCloud Director-Mandantenportal, um die Einstellungen zu konfigurieren, die zum Erstellen einer IPsec-VPN-Verbindung zwischen dem Organisations-VDC und einer anderen Site mithilfe der IPsec-VPN-Funktionen des Edge-Gateways benötigt werden.

3 Aktivieren des IPsec-VPN-Diensts auf einem Edge-Gateway

Wenn mindestens eine IPsec-VPN-Verbindung konfiguriert ist, können Sie den IPsec-VPN-Dienst auf dem Edge-Gateway aktivieren.

4 Angeben der globalen IPsec-VPN-Einstellungen


Verwenden Sie den Bildschirm **Globale Konfiguration**, um Einstellungen für die IPsec-VPN-Authentifizierung auf einer Edge-Gateway-Ebene zu konfigurieren. Auf dieser Seite können Sie einen globalen vorinstallierten Schlüssel festlegen und die Zertifizierungsauthentifizierung aktivieren.

Navigieren zum Bildschirm „IPsec-VPN“

Im Bildschirm **IPsec-VPN** können Sie den IPsec-VPN-Dienst für ein Edge-Gateway konfigurieren.

Verfahren

1 Öffnen Sie „Edge-Gateway-Dienste“.

- a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- b Klicken Sie im linken Bereich auf **Edge-Gateways**.
- c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Edge-Gateway](#).

Konfigurieren von IPsec-VPN-Site-Verbindungen für das Edge-Gateway

Verwenden Sie den Bildschirm **IPsec-VPN-Sites** im vCloud Director-Mandantenportal, um die Einstellungen zu konfigurieren, die zum Erstellen einer IPsec-VPN-Verbindung zwischen dem Organisations-VDC und einer anderen Site mithilfe der IPsec-VPN-Funktionen des Edge-Gateways benötigt werden.

Wenn Sie eine IPsec-VPN-Verbindung zwischen Sites konfigurieren, konfigurieren Sie die Verbindung aus der Sicht Ihres derzeitigen Standorts. Zum Einrichten einer Verbindung müssen Sie die Konzepte im Zusammenhang mit der vCloud Director-Umgebung verstehen, sodass Sie die VPN-Verbindung ordnungsgemäß konfigurieren.


- Die lokalen und Peer-Subnetze geben die Netzwerke an, mit denen das VPN eine Verbindung herstellt. Wenn Sie diese Subnetze in den Konfigurationen für IPsec-VPN-Sites angeben, geben Sie einen Netzwerkbereich und keine bestimmte IP-Adresse ein. Verwenden Sie das CIDR-Format, z. B. **192.168.99.0/24**.
- Die Peer-ID ist ein Bezeichner, der das Remotegerät eindeutig identifiziert, das die VPN-Verbindung beendet. In der Regel ist dies die öffentliche IP-Adresse. Bei Peers mit Zertifikatsauthentifizierung muss diese ID als Distinguished Name im Peer-Zertifikat festgelegt sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. NSX empfiehlt die Verwendung des FQDN oder der öffentlichen IP-Adresse des Remotegeräts als Peer-ID. Wenn die IP-Adresse des Peers aus einem anderen VDC-Organisationsnetzwerk stammt, geben Sie die native IP-Adresse des Peers ein. Wenn NAT für den Peer konfiguriert wurde, geben Sie die private IP-Adresse des Peers ein.
- Der Peer-Endpoint gibt die öffentliche IP-Adresse des Remotegeräts an, zu dem Sie eine Verbindung herstellen. Der Peer-Endpoint kann eine andere Adresse als die Peer-ID haben, wenn das Gateway des Peers nicht direkt über das Internet erreicht werden kann, sondern über ein anderes Gerät verbunden wird. Wenn NAT für den Peer konfiguriert wurde, geben Sie die öffentliche IP-Adresse ein, die das Gerät für NAT verwendet.

- Mit der lokalen ID wird die öffentliche IP-Adresse des Edge-Gateways des Organisations-VDCs angegeben. Sie können eine IP-Adresse oder einen Hostnamen zusammen mit der Firewall des Edge-Gateways eingeben.
- Der lokale Endpoint gibt das Netzwerk im Organisation-VDC an, in dem das Edge-Gateway überträgt. In der Regel stellt das externe Netzwerk des Edge-Gateways den lokalen Endpunkt dar.

Voraussetzungen

- [Navigieren zum Bildschirm „IPsec-VPN“](#).
- [Konfigurieren von IPsec-VPN](#).
- Wenn Sie beabsichtigen, ein globales Zertifikat als Authentifizierungsmethode zu verwenden, stellen Sie sicher, dass die Zertifikatauthentifizierung im Bildschirm **Globale Konfiguration** aktiviert ist. Weitere Informationen finden Sie unter [Angaben der globalen IPsec-VPN-Einstellungen](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **IPsec-VPN** auf **IPsec-VPN-Sites**.
- 2 Klicken Sie auf die Schaltfläche **Hinzufügen** (.
- 3 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>

Option	Aktion
Lokaler Endpoint	<p>Geben Sie das Netzwerk ein, das der lokale Endpoint für diese Verbindung ist.</p> <p>Der lokale Endpoint gibt das Netzwerk im Organisation-VDC an, in dem das Edge-Gateway überträgt. In der Regel ist das externe Netzwerk der lokale Endpoint.</p> <p>Wenn Sie unter Verwendung eines vorinstallierten Schlüssels einen IP-zu-IP-Tunnel hinzufügen, können die lokale ID und die ID des lokalen Endpoints identisch sein.</p>
Lokale Subnetze	<p>Geben Sie die Netzwerke ein, die von den Sites gemeinsam genutzt werden sollen, und verwenden Sie zur Eingabe mehrerer Subnetze ein Komma als Trennzeichen.</p> <p>Geben Sie einen Netzwerkbereich (keine spezifische IP-Adresse) ein, indem Sie die IP-Adresse im CIDR-Format eingeben, z. B. 192.168.99.0/24.</p>
Peer-ID	<p>Geben Sie eine Peer-ID ein, um die Peer-Site eindeutig zu identifizieren.</p> <p>Die Peer-ID ist ein Bezeichner, der das Remotegerät eindeutig identifiziert, das die VPN-Verbindung beendet. In der Regel ist dies die öffentliche IP-Adresse.</p> <p>Bei Peers mit Zertifikatsauthentifizierung muss die ID der Distinguished Name im Peer-Zertifikat sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. Eine Best Practice für NSX besteht darin, die öffentliche IP-Adresse oder den FQDN des Remotegeräts als Peer-ID zu verwenden.</p> <p>Wenn die IP-Adresse des Peers aus einem anderen VDC-Organisationsnetzwerk stammt, geben Sie die native IP-Adresse des Peers ein. Wenn NAT für den Peer konfiguriert wurde, geben Sie die private IP-Adresse des Peers ein.</p>
Peer-Endpoint	<p>Geben Sie die IP-Adresse oder den FQDN der Peer-Site ein, also die öffentliche Adresse des Remotegeräts, mit dem Sie eine Verbindung herstellen.</p> <p>Hinweis Wenn NAT für den Peer konfiguriert wurde, geben Sie die öffentliche IP-Adresse ein, die das Gerät für NAT verwendet.</p>
Peer-Subnetze	<p>Geben Sie das Remotenetzwerk ein, mit dem das VPN eine Verbindung herstellt, und verwenden Sie zur Eingabe mehrerer Subnetze ein Komma als Trennzeichen.</p> <p>Geben Sie einen Netzwerkbereich (keine spezifische IP-Adresse) ein, indem Sie die IP-Adresse im CIDR-Format eingeben, z. B. 192.168.99.0/24.</p>
Verschlüsselungsalgorithmus	<p>Wählen Sie den Typ des Verschlüsselungsalgorithmus im Dropdown-Menü aus.</p> <p>Hinweis Der Verschlüsselungstyp, den Sie auswählen, muss mit dem Verschlüsselungstyp übereinstimmen, der auf dem VPN-Gerät der Remote-Site konfiguriert ist.</p>

Option	Aktion
Authentifizierung	<p>Wählen Sie eine Authentifizierung aus. Zu den Optionen gehören:</p> <ul style="list-style-type: none"> ■ PSK <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>
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	<p>(Optional) Aktivieren Sie diese Option, damit der gemeinsam verwendete Schlüssel auf dem Bildschirm angezeigt wird.</p>
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=P-Adresse</code> zum Umleiten des lokalen Datenverkehrs des Edge-Gateways über den IPsec-VPN-Tunnel. Dies ist der Standardwert. ■ <code>passthroughSubnets=PeerSubnetIPAddress</code>, um überlappende Subnetze zu unterstützen.

4 Klicken Sie auf **Behalten**.

5 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

Konfigurieren Sie die Verbindung für die Remote-Site. Sie müssen die IPsec-VPN-Verbindung auf beiden Seiten der Verbindung konfigurieren: dem Organisations-VDC und der Peer-Site.

Aktivieren Sie den IPsec-VPN-Dienst auf diesem Edge-Gateway. Wenn mindestens eine IPsec-VPN-Verbindung konfiguriert ist, können Sie den Dienst aktivieren. Weitere Informationen finden Sie unter [Aktivieren des IPsec-VPN-Diensts auf einem Edge-Gateway](#).

Aktivieren des IPsec-VPN-Diensts auf einem Edge-Gateway

Wenn mindestens eine IPsec-VPN-Verbindung konfiguriert ist, können Sie den IPsec-VPN-Dienst auf dem Edge-Gateway aktivieren.

Voraussetzungen

- [Navigieren zum Bildschirm „IPsec-VPN“](#).
- Stellen Sie sicher, dass mindestens eine IPsec-VPN-Verbindung für dieses Edge-Gateway konfiguriert ist. Weitere Informationen finden Sie in den unter [Konfigurieren von IPsec-VPN-Site-Verbindungen für das Edge-Gateway](#) beschriebenen Schritten.

Verfahren

- 1 Klicken Sie auf der Registerkarte „**IPsec-VPN**“ auf die Option **Aktivierungsstatus**.
- 2 Klicken Sie auf **IPSec-VPN-Dienststatus**, um den IPSec-VPN-Dienst zu aktivieren.
- 3 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

Der IPsec-VPN-Dienst des Edge-Gateways ist aktiv.

Angeben der globalen IPsec-VPN-Einstellungen

Verwenden Sie den Bildschirm **Globale Konfiguration**, um Einstellungen für die IPsec-VPN-Authentifizierung auf einer Edge-Gateway-Ebene zu konfigurieren. Auf dieser Seite können Sie einen globalen vorinstallierten Schlüssel festlegen und die Zertifizierungsauthentifizierung aktivieren.


Für Sites, deren Peer-Endpoint auf **Beliebig** festgelegt ist, wird ein globaler vorinstallierter Schlüssel verwendet.

Voraussetzungen

- Wenn Sie die Zertifikatsauthentifizierung aktivieren möchten, stellen Sie sicher, dass auf dem Bildschirm **Zertifikate** mindestens ein Dienstzertifikat sowie entsprechende von einer Zertifizierungsstelle signierte Zertifikate angezeigt werden. Selbstsignierte Zertifikate können nicht für IPSec-VPNs verwendet werden. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).
- [Navigieren zum Bildschirm „IPsec-VPN“](#).

Verfahren

1 Öffnen Sie „Edge-Gateway-Dienste“.

- a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- b Klicken Sie im linken Bereich auf **Edge-Gateways**.
- c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Edge-Gateway](#).

L2 VPN konfigurieren

Die Edge-Gateways in einer vCloud Director-Umgebung unterstützen L2 VPN. L2 VPN lässt eine Erweiterung Ihres Organisations-VDC zu, indem die virtuellen Maschinen Netzwerkkonnektivität unter Verwendung derselben IP-Adresse über geografische Grenzen hinweg beibehalten können. Sie können den L2 VPN-Dienst auf einem Edge-Gateway konfigurieren.

Die NSX-Software stellt die L2 VPN-Funktionen eines Edge-Gateways bereit. Mit L2 VPN kann ein Tunnel zwischen zwei Sites konfiguriert werden. Virtuelle Maschinen verbleiben im selben Subnetz, obwohl sie zwischen diesen Sites verschoben werden. Daher können Sie das Organisations-VDC erweitern, indem Sie sein Netzwerk mit L2 VPN ausdehnen. Ein Edge-Gateway auf einer Site kann alle Dienste für virtuelle Maschinen auf der anderen Site bereitstellen.

Um den L2 VPN-Tunnel zu erstellen, konfigurieren Sie einen L2 VPN-Server und einen L2 VPN-Client. Wie im *Administratorhandbuch für NSX* beschrieben, ist der L2 VPN-Server das Ziel-Edge-Gateway und der L2 VPN-Client das Quell-Edge-Gateway. Nach dem Konfigurieren der L2 VPN-Einstellungen auf jedem Edge-Gateway müssen Sie den L2 VPN-Dienst sowohl auf dem Server als auch auf dem Client aktivieren.

Hinweis Auf den Edge-Gateways muss ein geroutetes VDC-Organisationsnetzwerk vorhanden sein, das als Teilschnittstelle erstellt wurde. Unter *vCloud Director-Administratorhandbuch* finden Sie die Schritte für die Erstellung eines externen gerouteten VDC-Organisationsnetzwerks.

Verfahren

1 Navigieren zum Bildschirm „L2 VPN“

Zum Konfigurieren des L2 VPN-Diensts für ein Edge-Gateway müssen Sie zum Bildschirm **L2 VPN** navigieren.

2 Konfigurieren des Edge-Gateways als L2 VPN-Server

Der L2 VPN-Server ist der Ziel-NSX Edge, mit dem der L2 VPN-Client eine Verbindung herstellen wird.

3 Konfigurieren des Edge-Gateways als L2 VPN-Client

Der L2 VPN-Client ist das quellseitige NSX Edge-Gateway, das die Kommunikation mit dem zielseitigen NSX Edge-Gateway, dem L2 VPN-Server, initiiert.

4 Aktivieren des L2 VPN-Diensts auf einem Edge-Gateway


Wenn die erforderlichen L2 VPN-Einstellungen konfiguriert sind, können Sie den L2 VPN-Dienst auf dem Edge-Gateway aktivieren.

Navigieren zum Bildschirm „L2 VPN“

Zum Konfigurieren des L2 VPN-Diensts für ein Edge-Gateway müssen Sie zum Bildschirm **L2 VPN** navigieren.

Verfahren

1 Öffnen Sie „Edge-Gateway-Dienste“.

- a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- b Klicken Sie im linken Bereich auf **Edge-Gateways**.
- c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend auf **Dienste**.

2 Navigieren Sie zu **VPN > L2 VPN**.

Nächste Schritte

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

Konfigurieren des Edge-Gateways als L2 VPN-Server

Der L2 VPN-Server ist der Ziel-NSX Edge, mit dem der L2 VPN-Client eine Verbindung herstellen wird.

Wie im *Administratorhandbuch für NSX* beschrieben, können Sie mehrere Peer-Sites mit diesem L2 VPN-Server verbinden.

Hinweis Änderungen an den Site-Konfigurationseinstellungen führen dazu, dass das Edge-Gateway alle vorhandenen Verbindungen trennt und erneut herstellt.

Voraussetzungen

- Stellen Sie sicher, dass das Edge-Gateway über ein geroutetes VDC-Organisationsnetzwerk verfügt, das als Teilschnittstelle auf dem Edge-Gateway konfiguriert ist. Unter *vCloud Director-Administratorhandbuch* finden Sie die Schritte für die Erstellung eines externen gerouteten VDC-Organisationsnetzwerks.
- [Navigieren zum Bildschirm „L2 VPN“](#).
- Wenn Sie ein Dienstzertifikat an die L2 VPN-Verbindung binden möchten, vergewissern Sie sich, dass das Serverzertifikat bereits auf das Edge-Gateway hochgeladen wurde. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).
- Sie müssen die Listener-IP des Servers, den Listener-Port, den Verschlüsselungsalgorithmus und mindestens eine Peer-Site konfiguriert haben, bevor Sie den L2 VPN-Dienst aktivieren können.

Verfahren

- 1 Wählen Sie auf der Registerkarte **L2 VPN** die Option **Server** für den L2 VPN-Modus aus.
- 2 Konfigurieren Sie auf der Registerkarte **Server – Global** die globalen Konfigurationsdetails des L2 VPN-Servers.

Option	Aktion
Listener-IP	Wählen Sie die primäre oder sekundäre IP-Adresse einer externen Schnittstelle des Edge-Gateways aus.
Listener-Port	Bearbeiten Sie den angezeigten Wert entsprechend den Anforderungen Ihrer Organisation. Der Standardport für den L2 VPN-Dienst ist 443.

Option	Aktion
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 Kennwort Kennwort bestätigen	Geben Sie den Benutzernamen und das Kennwort ein, mit denen die Peer-Site authentifiziert werden soll. Die Benutzeranmeldedaten auf der Peer-Site müssen mit den Anmeldedaten auf der Clientseite identisch sein.
Ausgeweitete Schnittstellen	Wählen Sie mindestens eine Teilschnittstelle aus, die mit dem Client ausgeweitet werden soll. Die zur Auswahl stehenden Teilschnittstellen sind die VDC-Organisationsnetzwerke, die als Teilschnittstellen auf dem Edge-Gateway konfiguriert sind.
Adresse des Egress-Optimierungs-Gateways	(Optional) Wenn das Standard-Gateway für virtuelle Maschinen auf beiden Sites das gleiche ist, geben Sie die Gateway-IP-Adressen der Teilschnittstellen ein, für die der Datenverkehr lokal weitergeleitet oder über den L2 VPN-Tunnel blockiert werden soll.

6 Klicken Sie auf **Behalten**.

7 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

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

Konfigurieren des Edge-Gateways als L2 VPN-Client

Der L2 VPN-Client ist das quellseitige NSX Edge-Gateway, das die Kommunikation mit dem zielseitigen NSX Edge-Gateway, dem L2 VPN-Server, initiiert.

Voraussetzungen

- [Navigieren zum Bildschirm „L2 VPN“](#).
- Wenn dieser L2 VPN-Client eine Verbindung mit einem L2 VPN-Server herstellt, der ein Serverzertifikat verwendet, müssen Sie überprüfen, ob das entsprechende CA-Zertifikat auf das Edge-Gateway hochgeladen wurde, um die Validierung des Serverzertifikats für diesen L2 VPN-Client zu ermöglichen. Weitere Informationen finden Sie unter [Hinzufügen eines CA-Zertifikats zum Edge-Gateway für die Überprüfung der Vertrauenswürdigkeit von SSL-Zertifikaten](#).

Verfahren

- 1 Wählen Sie auf der Registerkarte **L2 VPN** die Option **Client** für den L2 VPN-Modus aus.
- 2 Konfigurieren Sie auf der Registerkarte **Client – Global** die globalen Konfigurationsdetails des L2 VPN-Clients.

Option	Beschreibung
Serveradresse	Geben Sie die IP-Adresse des L2 VPN-Servers ein, mit dem dieser Client verbunden werden soll.
Server-Port	Geben Sie den Port des L2 VPN-Servers ein, mit dem der Client eine Verbindung herstellen soll. Der Standardport ist 443.
Verschlüsselungsalgorithmus	Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation mit dem Server aus.
Ausgeweitete Schnittstellen	Wählen Sie die Teilschnittstellen aus, die auf den Server ausgeweitet werden sollen. Die zur Auswahl stehenden Teilschnittstellen sind die VDC-Organisationsnetzwerke, die als Teilschnittstellen auf dem Edge-Gateway konfiguriert sind.
Adresse des Egress-Optimierungs-Gateways	(Optional) Wenn das Standard-Gateway für virtuelle Maschinen bei den beiden Sites identisch ist, geben Sie die Gateway-IP-Adressen der Teilschnittstellen oder die IP-Adressen ein, an die der Datenverkehr nicht über den Tunnel fließen soll.
Benutzerdetails	Geben Sie die Benutzer-ID und das Kennwort für die Authentifizierung beim Server ein.

- 3 Klicken Sie auf **Änderungen speichern**.
Der Speichervorgang kann eine Minute dauern.
- 4 (Optional) Um erweiterte Optionen zu konfigurieren, klicken Sie auf die Registerkarte **Client – Erweitert**.

- 5 Wenn dieses L2 VPN-Client-Edge-Gateway keinen direkten Zugriff auf das Internet hat und das L2 VPN-Server-Edge-Gateway über einen Proxyserver erreichen muss, geben Sie die Proxyeinstellungen an.

Option	Beschreibung
Sicheren Proxy aktivieren	Wählen Sie diese Option aus, um den sicheren Proxy zu aktivieren.
Adresse	Geben Sie die IP-Adresse des Proxyservers ein.
Port	Geben Sie den Port des Proxyservers ein.
Benutzername Kennwort	Geben Sie Anmeldeinformationen für die Authentifizierung des Proxyservers ein.

- 6 Um die Validierung der Serverzertifizierung zu aktivieren, klicken Sie auf **Zertifikat der Zertifizierungsstelle ändern** und wählen Sie das entsprechende CA-Zertifikat aus.

- 7 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

Nächste Schritte

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

Aktivieren des L2 VPN-Diensts auf einem Edge-Gateway

Wenn die erforderlichen L2 VPN-Einstellungen konfiguriert sind, können Sie den L2 VPN-Dienst auf dem Edge-Gateway aktivieren.

Hinweis Wenn HA bereits auf diesem Edge-Gateway konfiguriert ist, müssen Sie sicherstellen, dass für das Edge-Gateway mehr als eine interne Schnittstelle konfiguriert ist. Wenn nur eine einzige Schnittstelle vorhanden ist und diese bereits durch die HA-Funktion verwendet wurde, schlägt die L2 VPN-Konfiguration für dieselbe interne Schnittstelle fehl.

Voraussetzungen

- Wenn dieses Edge-Gateway ein L2 VPN-Server ist, d. h. das Ziel-NSX-Edge, müssen Sie sicherstellen, dass die erforderlichen L2 VPN-Servereinstellungen und mindestens eine L2 VPN-Peer-Site konfiguriert sind. Weitere Informationen finden Sie in den unter [Konfigurieren des Edge-Gateways als L2 VPN-Server](#) beschriebenen Schritten.
- Wenn dieses Edge-Gateway ein L2 VPN-Client ist, d. h. das Quell-NSX-Edge, müssen Sie sicherstellen, dass die L2 VPN-Clienteneinstellungen konfiguriert sind. Weitere Informationen finden Sie in den unter [Konfigurieren des Edge-Gateways als L2 VPN-Client](#) beschriebenen Schritten.
- [Navigieren zum Bildschirm „L2 VPN“](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **L2 VPN** auf die Umschaltfläche **Aktivieren**.

2 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

Der L2 VPN-Dienst des Edge-Gateways wird aktiv.

Nächste Schritte

Erstellen Sie NAT- oder Firewallregeln auf der mit dem Internet verbundenen Seite der Firewall, um die Verbindung des L2 VPN-Servers mit dem L2 VPN-Client zu aktivieren.

Entfernen der L2 VPN-Dienstkonfiguration von einem Edge-Gateway

Sie können die vorhandene L2 VPN-Dienstkonfiguration des Edge-Gateways entfernen. Durch diese Aktion wird auch der L2 VPN-Dienst auf dem Edge-Gateway deaktiviert.

Voraussetzungen

[Navigieren zum Bildschirm „L2 VPN“](#)

Verfahren

- 1 Führen Sie einen Bildlauf zum unteren Rand des Bildschirms „L2 VPN“ aus und klicken Sie auf **Konfiguration löschen**.
- 2 Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Ergebnisse

Der L2 VPN-Dienst wird deaktiviert, und die Konfigurationsdetails werden vom Edge-Gateway entfernt.

SSL-Zertifikatsverwaltung

Die NSX-Software in der vCloud Director-Umgebung bietet die Möglichkeit, Secure Sockets Layer (SSL)-Zertifikate mit den für Ihre Edge-Gateways konfigurierten Tunneln SSL VPN-Plus und IPsec-VPN zu verwenden.

Die Edge-Gateways in Ihrer vCloud Director-Umgebung unterstützen selbstsignierte Zertifikate, von einer Zertifizierungsstelle (CA) signierte Zertifikate und Zertifikate, die von einer Zertifizierungsstelle generiert und signiert wurden. Sie können CSRs (Certificate Signing Requests, Zertifikatsignieranforderungen) generieren, die Zertifikate importieren, die importierten Zertifikate verwalten und CRLs (Certificate Revocation Lists, Zertifikatswiderrufslisten) erstellen.

Informationen zur Verwendung von Zertifikaten mit Ihrem Organisations-VDC

Sie können Zertifikate für die folgenden Netzwerkbereiche in Ihrem vCloud Director-Organisations-VDC verwalten.

- IPsec-VPN-Tunnel zwischen einem VDC-Organisationsnetzwerk und einem Remotenetzwerk.
- SSL VPN-Plus-Verbindungen zwischen Remotebenutzern, privaten Netzwerken und Webressourcen in Ihrem Organisations-VDC.

- Ein L2 VPN-Tunnel zwischen zwei NSX-Edge-Gateways.
- Die virtuellen Server und die Poolserver, die für den Lastausgleich in Ihrem Organisations-VDC konfiguriert sind

Verwendung von Clientzertifikaten

Sie können ein Clientzertifikat unter Verwendung eines CAI-Befehls oder eines REST-Aufrufs erstellen. Anschließend können Sie dieses Zertifikat an Ihre Remotebenutzer verteilen, die das Zertifikat dann im Webbrowser installieren können.

Der Hauptvorteil des Implementierens von Clientzertifikaten besteht darin, dass für jeden Remotebenutzer ein Client-Referenzzertifikat gespeichert und anhand des vom Remotebenutzer bereitgestellten Clientzertifikats überprüft werden kann. Um zu verhindern, dass ein bestimmter Benutzer zukünftig eine Verbindung herstellt, können Sie das Referenzzertifikat aus der Liste der Clientzertifikate des Sicherheitsservers löschen. Durch das Löschen des Zertifikats kann der Benutzer keine Verbindungen herstellen.


Generieren einer Zertifikatsignieranforderung für ein Edge-Gateway

Bevor Sie ein signiertes Zertifikat bei einer Zertifizierungsstelle anfordern oder ein selbstsigniertes Zertifikat erstellen können, müssen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) für Ihr Edge-Gateway generieren.

Eine CSR ist eine codierte Datei, die Sie benötigen, um auf einem NSX Edge Gateway, das ein SSL-Zertifikat benötigt, ein Zertifikat zu generieren. Durch eine CSR wird die Art und Weise, wie Unternehmen ihre öffentlichen Schlüssel zusammen mit den Informationen senden, die ihre Unternehmens- und Domännennamen identifizieren, standardisiert.

Sie generieren eine CSR mit einer übereinstimmenden Datei mit dem privaten Schlüssel, die auf dem Edge-Gateway verbleiben muss. Die CSR enthält den passenden öffentlichen Schlüssel sowie weitere Informationen, wie z. B. Namen, Standort und Domännennamen Ihrer Organisation.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 vCloud Director-Organisation zu unterscheiden, denen dieses Zertifikat zugeordnet ist. Zum Beispiel Konstruktion oder Vertrieb.
Name der Organisation	Geben Sie den Namen ein, unter dem Ihr Unternehmen gesetzlich eingetragen ist. Die aufgeführte Organisation muss der gesetzliche Registrant des Domännennamens in der Zertifikatsanforderung sein.
Ort	Geben Sie die Stadt oder den Ort an, in der bzw. dem Ihr Unternehmen gesetzlich eingetragen ist.
Bundesland oder Kanton	Geben Sie den vollständigen Namen (keine Abkürzungen) des Bundeslandes, des Kantons, der Region oder des Gebiets ein, in dem bzw. der Ihr Unternehmen gesetzlich eingetragen ist.
Ländercode	Geben Sie den Namen des Landes ein, in dem Ihr Unternehmen gesetzlich eingetragen ist.
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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- b Klicken Sie im linken Bereich auf **Edge-Gateways**.
- c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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.
 - Wenn sich die Daten in einer PEM-Datei auf einem System befinden, zu dem Sie navigieren können, klicken Sie auf die Schaltfläche **Hochladen**, um zu der Datei zu navigieren, und wählen Sie diese aus.
 - Falls Sie die PEM-Daten kopieren und einfügen können, fügen Sie sie in das Feld **Privater Schlüssel (PEM-Format)** ein.
Fügen Sie die Zeilen **-----BEGIN RSA PRIVATE KEY-----** und **-----END RSA PRIVATE KEY-----** hinzu.
- 6 Geben Sie die Passphrase des privaten Schlüssels ein und bestätigen Sie sie.
- 7 (Optional) Geben Sie eine Beschreibung ein.
- 8 Klicken Sie auf **Behalten**.

Ergebnisse

Das Zertifikat vom Typ „Dienstzertifikat“ wird in der Liste auf dem Bildschirm angezeigt. Dieses Dienstzertifikat kann nun von Ihnen ausgewählt werden, wenn Sie die VPN-bezogenen Einstellungen des Edge-Gateways konfigurieren.

Benutzerdefiniertes Gruppieren von Objekten

Die NSX-Software in der vCloud Director-Umgebung bietet die Möglichkeit, Sätze und Gruppen von bestimmten Entitäten zu definieren, die Sie dann beim Angeben weiterer netzwerkbezogener Konfigurationen verwenden können, z. B. in Firewallregeln.

Erstellen eines IP Sets zur Verwendung in Firewallregeln und bei der DHCP-Relay-Konfiguration

Bei einem IP Set handelt es sich um eine Gruppe von IP-Adressen, die Sie auf Organisations-VDC-Ebene erstellen können. Sie können ein IP Set als Quelle oder Ziel in einer Firewallregel oder in einer DHCP-Relay-Konfiguration verwenden.

Ein IP Set erstellen Sie auf der Seite **Gruppierungsobjekte**. Um diese Seite zu öffnen, müssen Sie entweder zu den Einstellungen der Distributed Firewall des Organisations-VDC oder zu den Diensteinstellungen eines zum Organisations-VDC gehörenden Edge-Gateways navigieren.


Verfahren

- 1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ol style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Organisations-VDCs. c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. d Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Diensteinstellungen eines Edge-Gateways im Organisations-VDC	<ol style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Edge-Gateways. c Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. d Klicken Sie auf die Registerkarte 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 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 erstellen ein MAC Set mithilfe der Seite **Gruppierungsobjekte**. Zum Öffnen dieser Seite müssen Sie entweder zu den Distributed Firewall-Einstellungen des Organisations-VDC oder den Dienstinstellungen eines Edge-Gateways navigieren, das zum Organisations-VDC gehört.

Verfahren

1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Organisations-VDCs. c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. d Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Dienstinstellungen eines Edge-Gateways im Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. b Klicken Sie im linken Bereich auf Edge-Gateways. c Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. d Klicken Sie auf die Registerkarte 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 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 mithilfe der Seite **Gruppierungsobjekte** anzeigen. Zum Öffnen dieser Seite müssen Sie entweder zu den Distributed Firewall-Einstellungen des Organisations-VDC oder den Diensteinstellungen eines Edge-Gateways navigieren, das zum Organisations-VDC gehört.

Verfahren

- 1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ol style="list-style-type: none"> Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. Klicken Sie im linken Bereich auf Organisations-VDCs. Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Diensteinstellungen eines Edge-Gateways im Organisations-VDC	<ol style="list-style-type: none"> Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. Klicken Sie im linken Bereich auf Edge-Gateways. Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. Klicken Sie auf die Registerkarte 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 mithilfe der Seite **Gruppierungsobjekte** anzeigen. Zum Öffnen dieser Seite müssen Sie entweder zu den Distributed Firewall-Einstellungen des Organisations-VDC oder den Diensteinstellungen eines Edge-Gateways navigieren, das zum Organisations-VDC gehört.

Verfahren

1 Öffnen Sie die Seite **Gruppierungsobjekte**.

Option	Aktion
In den Einstellungen der Distributed Firewall des Organisations-VDC	<ol style="list-style-type: none"> Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. Klicken Sie im linken Bereich auf Organisations-VDCs. Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten virtuellen Organisations-Datencenters und klicken Sie auf Firewall verwalten. Klicken Sie auf die Registerkarte Gruppierungsobjekte.
In den Diensteeinstellungen eines Edge-Gateways im Organisations-VDC	<ol style="list-style-type: none"> Wählen Sie im Hauptmenü () die Option Cloud-Ressourcen aus. Klicken Sie im linken Bereich auf Edge-Gateways. Klicken Sie auf das Optionsfeld neben dem Namen eines Edge-Gateways, das zum virtuellen Organisations-Zieldatencenter gehört, und klicken Sie auf Dienste. Klicken Sie auf die Registerkarte 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.

Anzeigen der Netzwerknutzung und der IP-Zuweisungen auf einem Edge-Gateway

Sie können die Netzwerke auf einem Edge-Gateway mit Informationen zur IP-Poolnutzung und zu den Subnetzen anzeigen. Sie können auch die IP-Adresse anzeigen, die jedem Netzwerk zugewiesen ist.

Verfahren

- Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie auf den Namen des Ziel-Edge-Gateways.
- Um die externen Netzwerke mit Informationen über ihre IP-Poolnutzung und Subnetze anzuzeigen, klicken Sie auf die Registerkarte **Externe Netzwerke > Netzwerke und Subnetze**.
- Um die externen Netzwerke mit Informationen zu ihren IP-Adressen und Kategorien anzuzeigen, klicken Sie auf die Registerkarte **Externe Netzwerke > IP-Zuweisungen**.

Bearbeiten der Edge-Gateway-Eigenschaften


Aktivieren oder Deaktivieren von Distributed Routing auf einem Edge-Gateway

Nachdem Sie vCloud Director Distributed Routing auf einem Edge-Gateway aktiviert haben, kann der Organisationsadministrator viele VDC-Organisationsnetzwerke mit Routing mit verteilten Schnittstellen erstellen, die mit diesem Edge-Gateway verbunden sind. Der Datenverkehr in diesen Netzwerken ist für die VM-zu-VM-Kommunikation optimiert.

Voraussetzungen

Die unterstützende NSX Manager-Instanz ist mit einem NSX Controller-Cluster konfiguriert. Weitere Informationen dazu finden Sie im *Administratorhandbuch für NSX*.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways**.
- 3 Wählen Sie das Optionsfeld neben dem Namen des gewünschten Edge-Gateways aus und klicken Sie auf **Distributed Routing aktivieren** oder **Distributed Routing deaktivieren**.
- 4 Klicken Sie zur Bestätigung auf **OK**.


Ändern der externen Netzwerke und der Edge-Gateway-Einstellungen

Um die externen Netzwerke und die Edge-Gateway-Einstellungen zu ändern, können Sie den Assistenten **Edge-Gateway bearbeiten** verwenden, der dieselben Seiten wie der Assistent enthält, den Sie zum Erstellen des Edge-Gateways verwendet haben.

Sie können die Einstellungen ändern, die Sie beim Hinzufügen des Edge-Gateways konfiguriert haben. Weitere Informationen finden Sie unter [Hinzufügen eines Edge-Gateways](#).

Informationen zum Ändern der Distributed Routing-Einstellung finden Sie unter [Aktivieren oder Deaktivieren von Distributed Routing auf einem Edge-Gateway](#).


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des zu ändernden Edge-Gateways und dann auf **Bearbeiten**.
- 4 Um die Edge-Gateway-Einstellungen zu ändern, navigieren Sie durch die Seiten des Assistenten **Edge-Gateway bearbeiten**, indem Sie auf **Weiter** klicken, und klicken Sie auf der Seite **Bereit zum Abschließen** auf **Beenden**.

Bearbeiten der allgemeinen Einstellungen für ein Edge-Gateway

Sie können den Namen und die Beschreibung eines Edge-Gateways ändern, den FIPS-Modus und den Hochverfügbarkeitsstatus aktivieren bzw. deaktivieren und die Edge-Gateway-Größenkonfiguration ändern.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie auf den Namen des Ziel-Edge-Gateways.
- 3 Klicken Sie auf der Registerkarte **Allgemein** in der oberen rechten Ecke auf **Bearbeiten**.
- 4 (Optional) Bearbeiten Sie den Namen und die Beschreibung des Edge-Gateways.
- 5 (Optional) Aktivieren oder deaktivieren Sie alle allgemeinen Edge-Gateway-Einstellungen.

Allgemeine Einstellung	Beschreibung
FIPS-Modus	Konfiguriert das Edge-Gateway für die Verwendung des NSX-FIPS-Modus.
Hochverfügbarkeit	Aktiviert automatisches Failover auf ein Sicherungs-Edge-Gateway.

- 6 (Optional) Ändern Sie die Edge-Gateway-Konfiguration für Ihre Systemressourcen.


Option	Beschreibung
Kompakt	Benötigt weniger Arbeitsspeicher- und Rechenressourcen.
Groß	Bietet eine größere Kapazität und eine höhere Leistung als mit der Option „Kompakt“. Große und sehr große Konfigurationen bieten exakt dieselben Sicherheitsfunktionen.
Sehr groß	Wird für Umgebungen verwendet, die über einen Lastausgleichsdienst mit einer großen Anzahl gleichzeitiger Sitzungen verfügen.
Vollständig-4	Wird für Umgebungen mit hohem Durchsatz verwendet. Erfordert eine hohe Verbindungsrate.

- 7 Klicken Sie zum Bestätigen der Änderungen auf **Speichern**.

Bearbeiten des Standard-Gateways für ein Edge-Gateway

Sie können das Netzwerk ändern, das ein Edge-Gateway als Standard-Gateway verwendet.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie auf den Namen des Ziel-Edge-Gateways.
- 3 Klicken Sie auf der Registerkarte **Externe Netzwerke > Standard-Gateway** in der oberen rechten Ecke auf **Bearbeiten**.

- 4 (Optional) Konfigurieren Sie ein Netzwerk als Standard-Gateway.
 - a Aktivieren Sie die Umschaltoption **Standard-Gateway konfigurieren**.
 - b Aktivieren Sie das Optionsfeld neben dem Namen des externen Zielnetzwerks und aktivieren Sie das Optionsfeld neben der Ziel-IP-Adresse.
 - c (Optional) Aktivieren Sie die Umschaltoption **Standard-Gateway für DNS-Relay verwenden**.
- 5 Klicken Sie zum Bestätigen der Änderungen auf **Speichern**.

Bearbeiten der IP-Einstellungen für ein Edge-Gateway

Sie können die IP-Einstellungen für externe Netzwerke auf einem Edge-Gateway ändern.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie auf den Namen des Ziel-Edge-Gateways.
- 3 Klicken Sie auf der Registerkarte **Externe Netzwerke > IP-Einstellungen** auf **Bearbeiten**.
- 4 Geben Sie für jedes Netzwerk auf dem Edge-Gateway in der Zelle **IP-Adressen** eine IP-Adresse ein oder lassen Sie die Zelle leer.


Wenn Sie für ein Netzwerk keine IP-Adresse eingeben, weist das System diesem Netzwerk eine beliebige IP-Adresse zu.
- 5 Klicken Sie zum Bestätigen der Änderungen auf **Speichern**.

Bearbeiten der unterzugewiesenen IP-Pools eines Edge-Gateways

Sie können mehrere statische IP-Pools aus den verfügbaren IP-Pools eines externen Netzwerks auf einem Edge-Gateway unterzuweisen.

Hinweis Die Zuweisung von IP-Adressen zu einem Edge-Gateway über die Unterzuweisung ist ein Prozess, bei dem der Anbieter dem Gateway den Besitz von IP-Adressen zuweist. vCloud Director konfiguriert die entsprechende Gateway-Schnittstelle während der Unterzuweisung automatisch mit den sekundären Adressen, was zu IP-Adressenkonflikten führen kann, wenn manche dieser IP-Adressen außerhalb von vCloud Director verwendet werden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie auf den Namen des Ziel-Edge-Gateways.

3 Klicken Sie auf die Registerkarte **Externe Netzwerke > Unterzugewiesene IP-Pools**.

Sie können die aktuellen unterzugewiesenen IP-Pools für jedes externe Netzwerk auf diesem Edge-Gateway anzeigen.

4 Klicken Sie auf das Optionsfeld neben dem Namen eines externen Netzwerks und anschließend auf **Bearbeiten**.

Sie können die verfügbaren IP-Pools für dieses externe Netzwerk und die aktuellen unterzugewiesenen IP-Pools anzeigen, sofern diese konfiguriert sind.

5 Bearbeiten Sie die unterzugewiesenen IP-Pools für dieses externe Netzwerk und klicken Sie auf **Speichern**.

Sie können IP-Adressen und Bereiche aus den Bereichen der verfügbaren IP-Pools hinzufügen, ändern und entfernen.

Ergebnisse

Das System kombiniert überlappende IP-Bereiche.

Bearbeiten von Ratengrenzwerten für ein Edge-Gateway

Sie können den Grenzwert für die eingehende und die ausgehende Rate für jedes aktivierte externe Netzwerk des Edge-Gateways konfigurieren.

Ratengrenzwerte gelten nur für externe Netzwerke, die von verteilten Portgruppen mit statischer Bindung gestützt werden.

Verfahren

1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.

2 Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie auf den Namen des Ziel-Edge-Gateways.

3 Klicken Sie auf der Registerkarte **Externe Netzwerke > Ratengrenzwerte** in der oberen rechten Ecke auf **Bearbeiten**.

Sie können die aktuellen Ratengrenzwerte für jedes externe Netzwerk dieses Edge-Gateways anzeigen.

4 Bearbeiten Sie die Ratengrenzwerte und klicken Sie auf **Speichern**.

Für jedes externe Netzwerk auf dem Edge-Gateway können Sie die Ratengrenzwerte aktivieren oder deaktivieren und die eingehende und ausgehende Rate ändern.

Edge-Gateway erneut bereitstellen


Sie können eine Edge-Gateway-Appliance löschen und mit den neuesten Konfigurationen erneut bereitstellen.

Wenn die Edge-Dienste nicht erwartungsgemäß funktionieren, können Sie die Edge-Gateway-Appliance erneut bereitstellen.

Sie können Legacy-Edge-Gateways erneut bereitstellen, um die Edge-Gateways auf neu erstellte Edge-Cluster zu migrieren.

Wenn Sie ein Edge-Gateway erneut bereitstellen, löscht vCloud Director es und erstellt es mit den neuesten Konfigurationen neu.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend auf **Erneut bereitstellen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Ergebnisse

Die Edge-Gateway-VM wird durch eine neue virtuelle Maschine ersetzt, und alle Dienste werden wiederhergestellt.


Löschen eines Edge-Gateways

Sie können ein Edge-Gateway aus dem virtuellen Organisations-Datencenter entfernen.

Voraussetzungen

Löschen Sie alle VDC-Organisationsnetzwerke, die das betreffende Edge-Gateway verwenden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **Löschen**.


Statistiken und Protokolle für ein Edge-Gateway

Sie können Statistiken und Protokolle für ein Edge-Gateway anzeigen.

Anzeigen von Statistiken

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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. Der Bildschirm enthält Diagramme für den Datenverkehr, der über die Schnittstellen der ausgewählten Edge-Gateway-Instanz fließt, sowie Verbindungsstatistiken für die Firewall- und Lastausgleichsdienste. Wählen Sie den Zeitraum aus, für den Sie die Statistiken anzeigen möchten.
IPSec-VPN	Der Bildschirm „IPsec-VPN“ zeigt den Status und Statistiken für IPsec-VPN sowie den Status und Statistiken für jeden Tunnel an.
L2 VPN	Der Bildschirm „L2 VPN“ zeigt den Status und Statistiken für L2 VPN an.


Protokollierung aktivieren

Sie können die Protokollierung für ein Edge-Gateway aktivieren. Zusätzlich zur Aktivierung der Protokollierung für die Funktionen, für die Sie Protokolldaten erfassen möchten, müssen Sie zur Vervollständigung der Konfiguration einen Syslog-Server definieren, der die erfassten Protokolldaten empfangen soll. Wenn Sie einen Syslog-Server auf dem Bildschirm „Edge-Einstellungen“ konfigurieren, können Sie von diesem Syslog-Server aus auf die protokollierten Daten zugreifen.

Voraussetzungen

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend 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 vCloud Director-Systemadministrator bereits einen Syslog-Server für die vCloud Director-Umgebung konfiguriert hat, verwendet das System standardmäßig diesen Syslog-Server. Die zugehörige IP-Adresse wird im Bildschirm **Edge-Einstellungen** angezeigt.

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 Nachrichtenstatusebene 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 Nachrichtenstatusebene 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 Nachrichtenstatusebene 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 Nachrichtenstatusebene festlegen.

Aktivieren des SSH-Befehlszeilenzugriffs auf ein Edge-Gateway

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Edge-Gateways**.
 - c Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Edge-Gateways und anschließend auf **Dienste**.
- 2 Klicken Sie auf die Registerkarte **Edge-Einstellungen**.
- 3 Konfigurieren Sie die SSH-Einstellungen.

Option	Beschreibung
Benutzername	Geben Sie die Anmeldeinformationen für 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 SSH-Zugriff auf dieses Edge-Gateway zu ermöglichen.

Verwalten von VDC-Organisationsnetzwerken

8

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten eines NSX-T-VDC-Organisationsnetzwerks](#)

Verwalten eines NSX-T-VDC-Organisationsnetzwerks

Nur Systemadministratoren können VDC-Organisationsnetzwerke, die auf logischen NSX-T-Switches basieren, erstellen, ändern und löschen.

Um VDC-Organisationsnetzwerke zu verwalten, müssen sich Systemadministratoren beim Service Provider Admin Portal anmelden und zum vCloud Director-Mandantenportal der gewünschten Organisation navigieren.

Informationen zur Verwaltung von VDC-Organisationsnetzwerken, die auf NSX Data Center for vSphere basieren, finden Sie im *Handbuch für das vCloud Director Mandantenportal*.

Hinzufügen eines NSX-T-VDC-Organisationsnetzwerks

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

Hinweis Mit einem logischen NSX-T-Switch können Sie nur ein isoliertes IPv4-Organisationsnetzwerk erstellen. Sie können basierend auf einem logischen NSX-T-Switch kein direktes oder geroutetes Organisationsnetzwerk erstellen.


Voraussetzungen

- Dem Provider-VDC, das dem virtuellen Datencenter der Zielorganisation zugrunde liegt, muss eine NSX-T Manager-Instanz zugeordnet sein.
- Sie haben mindestens einen logischen NSX-T-Switch erstellt, der nicht von anderen VDC-Organisationsnetzwerken verwendet wird.

Informationen zum Konfigurieren von logischen NSX-T-Switches finden Sie im *Administratorhandbuch für NSX-T*. Informationen zum Erstellen eines durch eine NSX-T Manager-Instanz gestützten Provider-VDCs finden Sie unter *vCloud API-Programmierhandbuch für Dienstanbieter*.

Verfahren

- 1 Navigieren Sie zum vCloud Director-Mandantenportal der gewünschten Organisation.

- a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- b Klicken Sie unter **Organisationen** auf den Namen der gewünschten Organisation.

Sie werden zur Ansicht **Datacenter** des vCloud Director-Mandantenportals für diese Organisation weitergeleitet.

- 2 Wenn in der Organisation mehrere VDCs vorhanden sind, klicken Sie auf die Karte des VDC der gewünschten Organisation.

- 3 Klicken Sie im linken Bereich unter **Netzwerke** auf **Netzwerk**.

- 4 Klicken Sie auf **Importieren**.

Der Assistent **Logischen Switch importieren** wird angezeigt.

- 5 Geben Sie einen Namen und optional eine Beschreibung für das neue VDC-Organisationsnetzwerk ein und klicken Sie auf **Weiter**.

- 6 Wählen Sie in der Liste der verfügbaren logischen NSX-T-Switches den Ziel-Switch aus. Klicken Sie dazu auf das Optionsfeld neben dem Switch-Namen und dann auf **Weiter**.

- 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 (Optional) Konfigurieren Sie die DNS-Einstellungen und den statischen IP-Pool.

Sie können mehrere IP-Adressen und IP-Bereiche hinzufügen.

- 9 Klicken Sie auf **Weiter**.


- 10 Überprüfen Sie die Angaben auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Fertig stellen**.

Bearbeiten eines NSX-T-VDC-Organisationsnetzwerks

Sie können den Namen, die Beschreibung, die DNS-Einstellungen und den statischen IP-Pool eines VDC-Organisationsnetzwerks ändern, das auf einem logischen NSX-T-Switch basiert. Die Classless Inter-Domain Routing(CIDR)-Netzwerkeinstellungen können Sie nicht bearbeiten.

Verfahren

- 1 Navigieren Sie zum vCloud Director-Mandantenportal der gewünschten Organisation.

- a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- b Klicken Sie unter **Organisationen** auf den Namen der gewünschten Organisation.

Sie werden zur Ansicht **Datacenter** des vCloud Director-Mandantenportals für diese Organisation weitergeleitet.

- 2 Wenn in der Organisation mehrere VDCs vorhanden sind, klicken Sie auf die Karte des VDC der gewünschten Organisation.
- 3 Klicken Sie im linken Bereich unter **Netzwerke** auf **Netzwerk**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Netzwerks und anschließend auf **Ändern**.

Der Assistent **VDC-Organisationsnetzwerk bearbeiten** wird angezeigt.

- 5 (Optional) Bearbeiten Sie auf der Registerkarte **Allgemein** den Namen und die Beschreibung des Netzwerks.
- 6 (Optional) Bearbeiten Sie auf der Registerkarte **Netzwerk konfigurieren** die DNS-Einstellungen und den statischen IP-Pool des Netzwerks.


Sie können IP-Adressen und IP-Bereiche hinzufügen, ändern und entfernen.

- 7 Klicken Sie auf **Speichern**.

Löschen eines NSX-T-VDC-Organisationsnetzwerks

Wenn Sie ein NSX-T-VDC-Organisationsnetzwerk nicht mehr verwenden, können Sie es löschen.

Verfahren

- 1 Navigieren Sie zum vCloud Director-Mandantenportal der gewünschten Organisation.
 - a Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
 - b Klicken Sie unter **Organisationen** auf den Namen der gewünschten Organisation.

Sie werden zur Ansicht **Datacenter** des vCloud Director-Mandantenportals für diese Organisation weitergeleitet.

- 2 Wenn in der Organisation mehrere VDCs vorhanden sind, klicken Sie auf die Karte des VDC der gewünschten Organisation.
- 3 Klicken Sie im linken Bereich unter **Netzwerke** auf **Netzwerk**.
- 4 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Netzwerks und dann auf **Löschen**.
- 5 Klicken Sie zur Bestätigung auf **OK**.

Verwalten von SDDCs und SDDC-Proxys

9

Ab Version 9.7 kann vCloud Director als HTTP-Proxy-Server zwischen Mandanten und der zugrunde liegenden vSphere-Umgebung fungieren. Ein Software-Defined Data Center (SDDC) kapselt die Infrastruktur einer angehängten vCenter Server-Instanz. Ein SDDC-Proxy ist ein Zugriffspunkt auf eine Komponente aus einem SDDC, z. B. eine vCenter Server-Instanz, ein ESXi-Host oder eine NSX Manager-Instanz.

Mit der SDDC-Funktion können Sie vCloud Director als zentralen Verwaltungspunkt für alle vSphere-Umgebungen verwenden.

- Sie können die Ressourcen einer vCenter Server-Instanz für einen einzelnen Mandanten reservieren, indem Sie das entsprechende SDDC nur für dessen Organisation veröffentlichen. Der Mandant nutzt diese Ressourcen nicht mit anderen Mandanten gemeinsam. Der Mandant kann auf dieses SDDC mithilfe einer Benutzeroberfläche oder eines API-Proxys zugreifen, ohne dass ein VPN erforderlich ist.
- Sie können vCloud Director als Lightweight-Verzeichnis verwenden, um alle vCenter Server-Instanzen zu registrieren.
- Sie können vCloud Director als API-Endpoint für alle vCenter Server-Instanzen verwenden.

Bevor Sie ein SDDC erstellen, müssen Sie die vCenter Server-Zielinstanz an vCloud Director anhängen. Weitere Informationen finden Sie unter [Anhängen einer vCenter Server-Instanz allein oder zusammen mit einer NSX Manager-Instanz](#).

Hinweis Standardmäßig können Sie mit einer angehängten vCenter Server-Instanz entweder ein Provider-VDC oder ein SDDC erstellen. Wenn Sie ein Provider-VDC erstellt haben, das von einer vCenter Server-Instanz gestützt wird, können Sie diese vCenter Server-Instanz nicht zum Erstellen eines SDDC verwenden, bzw. umgekehrt. Sie können die vCloud-API verwenden, um die Systemeinstellungen Ihrer vCloud Director-Installation zu ändern, sodass eine vCenter Server-Instanz sowohl ein Provider-VDC als auch ein SDDC stützen kann.

Sie können SDDCs und SDDC-Proxys für Organisationen in Ihrer Cloud erstellen und veröffentlichen. Benutzer können die SDDC-Proxys verwenden, um auf die zugrunde liegende vSphere-Umgebung zuzugreifen. Benutzer können sich mithilfe ihrer vCloud Director-Konten bei der Benutzeroberfläche oder der API der Proxy-Komponenten anmelden.

Mit SDDCs in vCloud Director entfällt die Anforderung, dass vCenter Server öffentlich zugänglich sein muss. Um den Zugriff zu steuern, können Sie ein SDDC in vCloud Director aktivieren und deaktivieren, und Sie können einen SDDC-Proxy aktivieren und deaktivieren.

Erstellen und Verwalten von SDDCs und SDDC-Proxys

Um SDDCs und Proxys zu erstellen und zu verwalten, müssen Sie die vCloud OpenAPI verwenden. Weitere Informationen finden Sie unter *Erste Schritte mit vCloud OpenAPI* auf <https://code.vmware.com>.

Wichtig vCloud Director erfordert eine direkte Netzwerkverbindung zu jeder vCenter Server-Instanz für die Verwendung als SDDC. Wenn die vCenter Server-Instanz eine externe Platform Services Controller-Instanz verwendet, benötigt vCloud Director auch eine direkte Netzwerkverbindung mit der Platform Services Controller-Instanz.

Um das VMware OVF Tool in einem Proxy-SDDC zu verwenden, benötigt vCloud Director eine direkte Verbindung zu jedem ESXi-Host.

- 1 Erstellen Sie ein SDDC, das von einer angehängten und aktivierten vCenter Server-Instanz unterstützt wird.

vCloud Director erstellt das SDDC mit einem Standard-Proxy für die vCenter Server-Instanz. Wenn die vCenter Server-Instanz eine externe Platform Services Controller-Instanz verwendet, erstellt vCloud Director auch einen Proxy für die Platform Services Controller-Instanz.
- 2 Rufen Sie das Zertifikat und den Fingerabdruck der erstellten Proxys ab und überprüfen Sie, ob das Zertifikat und der Fingerabdruck vorhanden und korrekt sind.
- 3 Aktivieren Sie das SDDC.
- 4 Veröffentlichen Sie das SDDC für eine oder mehrere Organisationen.
- 5 Um Benutzern den Zugriff auf die SDDCs und die SDDC-Proxys von vCloud Director Tenant Portal zu ermöglichen, müssen Sie das **CPOM-Erweiterungs**-Plug-In für ihre Organisationen veröffentlichen. Weitere Informationen finden Sie unter [Veröffentlichen oder Rückgängigmachen der Veröffentlichung eines Plug-Ins in einer Organisation](#).

Nachdem Sie ein SDDC erstellt und veröffentlicht haben, können Sie Ihre SDDC-Proxys hinzufügen, bearbeiten, aktivieren, deaktivieren und entfernen.

Hinweis Wenn Sie einen Proxy zu einem SDDC hinzufügen, müssen Sie das Zertifikat und den Fingerabdruck hochladen, damit Mandanten das Zertifikat und den Fingerabdruck abrufen können, wenn die Proxy-Komponente selbstsignierte Zertifikate verwendet.

Verwalten von Systemadministratoren und Rollen

10

Über die vCloud Director-Webkonsole können Sie Systemadministratoren einzeln zu vCloud Director hinzufügen oder als Teil einer LDAP-Gruppe. Sie können auch Rollen hinzufügen und bearbeiten, über die die Berechtigungen der Benutzer in ihrer Organisation festgelegt werden.

Hinweis Ab vCloud Director 9.5 können Dienstanbieter über das vCloud Director Service Provider Admin Portal oder über die vCloud OpenAPI Anbieterrollen erstellen und Anbieterbenutzer und -gruppen erstellen. Informationen zum Verwalten von Anbieterrollen, Benutzern und Gruppen finden Sie im *vCloud Director Service Provider Admin Portal-Handbuch*. Wenn Sie sich die Dokumentation zu vCloud OpenAPI ansehen möchten, wechseln Sie zu https://vCloud_Director_IP_address_or_host_name/docs.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von Rechten und Rollen](#)
- [Verwalten von Anbieterbenutzern und -gruppen](#)

Verwalten von Rechten und Rollen

In vCloud Director ist ein Recht die Grundeinheit für die Zugriffssteuerung. Eine Rolle ordnet einen Rollennamen einem Satz von Rechten zu. Jede Organisation kann verschiedene Rechte und Rolle aufweisen.

vCloud Director verwendet Rollen und ihre verknüpften Rechte, um zu ermitteln, ob ein Benutzer oder eine Gruppe zum Durchführen eines Vorgangs berechtigt ist. Viele der in den vCloud Director-Handbüchern beschriebenen Verfahren setzen eine bestimmte Rolle voraus. In diesen Voraussetzungen wird davon ausgegangen, dass es sich bei der benannten Rolle um die unveränderte vordefinierte Rolle oder um eine Rolle mit einem äquivalenten Satz von Rechten handelt.

Ab vCloud Director 9.5 werden Rechtepakete und globale Mandantenrollen eingeführt, mit denen Systemadministratoren die Rechte und Rollen verwalten können, die für die einzelnen Organisationen verfügbar sind.

Nachdem Sie vCloud Director installiert haben, enthält das System nur das Systemrechtapaket mit allen Rechten, die im System verfügbar sind. Das Systemrechtapaket wird nicht für Organisationen veröffentlicht. Das System enthält außerdem integrierte globale Mandantenrollen, die für alle Organisationen veröffentlicht werden. Informationen zu den vordefinierten Rollen erhalten Sie unter [Vordefinierte Rollen und ihre Rechte](#).

Nachdem Sie vCloud Director von Version 9.1 oder früher aktualisiert haben, enthält das System zusätzlich zum Systemrechtapaket für jede vorhandene Organisation ein Alt-Rechtapaket. Jedes Alt-Rechtapaket enthält die Rechte, die für die zugehörige Organisation zur Verfügung standen, als das Upgrade durchgeführt wurde, und wird nur für die jeweilige Organisation veröffentlicht.

Hinweis Um das Rechtapaketmodell für eine bestehende Organisation verwenden zu können, müssen Sie das entsprechende Alt-Rechtapaket löschen.

Wenn Sie vCloud Director von Version 9.1 oder niedriger aktualisiert haben, werden die vorhandenen Rollenvorlagen für alle Organisationen als globale Mandantenrollen veröffentlicht. Die vorhandenen Rollen, deren Verknüpfung mit Rollenvorlagen entfernt wird, stehen für ihre jeweiligen Organisationen als mandantenspezifische Rollen zur Verfügung.

Fachbegriffe zum Thema Rechte

Rechts

Jedes Recht ermöglicht die Ansicht oder Verwaltung des Zugriffs auf einen bestimmten Objekttyp in vCloud Director. Rechte gehören unterschiedlichen Kategorien an, je nachdem, auf welche Objekte sie sich beziehen, zum Beispiel: vApp, Katalog, Organisation usw. Die Anbieterorganisation enthält alle im System verfügbaren Rechte. Der Systemadministrator legt fest, welche Rechte jeweils für die einzelnen Organisationen verfügbar sind. Sie können die in vCloud Director enthaltenen Rechte weder erstellen noch ändern.

Rechtapaket

Systemadministratoren können mithilfe von Rechtepaketen die Rechte verwalten, die jeweils für die einzelnen Organisationen verfügbar sind. Ein Rechtapaket ist ein Satz von Rechten, die der Systemadministrator für eine oder mehrere Organisationen veröffentlichen kann. Der Systemadministrator kann Rechtepakete erstellen und veröffentlichen, die Dienstebenen, separat abgerechneten Funktionen oder anderen willkürlichen Rechtegruppierungen entsprechen. Nur Systemadministratoren können die Rechtepakete anzeigen und verwalten. Sie können mehrere Pakete für ein und dieselbe Organisation veröffentlichen.

Rechte der Organisation

Organisationsrechte sind der vollständige Satz von Rechten, die für eine Organisation verfügbar sind. Die Rechte einer Organisation können mehrere Rechtepakete umfassen, aber die Organisationsadministratoren und Benutzer sehen einfach eine Liste aller Rechte, die sie zum Erstellen und Ändern von mandantenspezifischen Rollen verwenden können.

Fachbegriffe zum Thema Rollen

Rolle

Eine Rolle ist ein Satz von Rechten, der einer oder mehreren Benutzern und Gruppen zugewiesen werden kann. Beim Erstellen oder Importieren eines Benutzers oder einer Gruppe müssen Sie diesem bzw. dieser eine Rolle zuweisen.

Anbieterrollen

Anbieterrollen sind der Satz von Rollen, die nur für die Anbieterorganisation verfügbar sind. Anbieterrollen können nur Anbieterbenutzern zugewiesen werden. Systemadministratoren können benutzerdefinierte Anbieterrollen erstellen.

Mandantenrollen

Mandantenrollen sind der Satz von Rollen, die für eine Organisation verfügbar sind.

Systemadministratoren können globale Mandantenrollen erstellen und bearbeiten und sie für eine oder mehrere Organisationen veröffentlichen. Globale Mandantenrollen können Mandantenbenutzern in den Organisationen zugewiesen werden, für die sie veröffentlicht werden. Organisationsadministratoren können globale Mandantenrollen nicht bearbeiten.

Hinweis Mandantenbenutzer können nur diejenigen Rechte aus ihren Rollen verwenden, die für ihre Organisationen veröffentlicht sind.

Mandantenspezifische Rollen

Organisationsadministratoren können mandantenspezifische Rollen erstellen und bearbeiten, die lokal für ihre Organisationen sind. Mandantenspezifische Rollen können nur Mandantenbenutzern in der Organisation zugewiesen werden, zu der sie gehören. Mandantenspezifische Rollen können eine Untermenge nur mit den Rechten der Organisation enthalten.

Informationen zur Verwaltung von mandantenspezifischen Rollen finden Sie im *Handbuch für das vCloud Director Mandantenportal*.

Vordefinierte Rollen und ihre Rechte

Jede vordefinierte vCloud Director-Rolle enthält einen Standardsatz an Rechten, die erforderlich sind, um in gemeinsamen Workflows enthaltene Vorgänge auszuführen. Standardmäßig werden alle globalen vordefinierten Mandantenrollen für 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. Die Anmeldeinformationen des **Systemadministrators** werden während der Installation und Konfiguration festgelegt. Ein **Systemadministrator** kann zusätzliche Systemadministrator- und Benutzerkonten in der Anbieterorganisation einrichten.

Multisite-System

Wird zur Ausführung des Heartbeat-Prozesses für Bereitstellungen mit mehreren Standorten verwendet. Diese Rolle verfügt lediglich über das Recht **Multisite: Systemvorgänge**, mit dem eine vCloud-API-Anforderung zum Abrufen des Status des Remotemitglieds einer Sitezuordnung gestellt werden kann.

Vordefinierte globale Mandantenrollen

Standardmäßig werden die vordefinierten globalen Mandantenrollen und die darin enthaltenen Rechte für alle Organisationen veröffentlicht. **Systemadministratoren** können die Veröffentlichung von Rechten und globalen Mandantenrollen einzelner Organisationen rückgängig machen. **Systemadministratoren** können vordefinierte globale Mandantenrollen bearbeiten oder löschen. **Systemadministratoren** können zusätzliche globale Mandantenrollen erstellen und veröffentlichen.

Organisationsadministrator

Nach dem Erstellen einer Organisation kann ein **Systemadministrator** einem beliebigen Benutzer in der Organisation die Rolle **Organisationsadministrator** zuweisen. Ein Benutzer mit der vordefinierten Rolle **Organisationsadministrator** kann die vCloud Director-Webkonsole, das Mandantenportal oder die vCloud OpenAPI verwenden, um Benutzer und Gruppen in seiner Organisation zu verwalten und ihnen Rollen zuzuweisen, einschließlich der vordefinierten Rolle **Organisationsadministrator**. Von einem **Organisationsadministrator** erstellte oder geänderte Rollen sind für andere Organisationen nicht sichtbar.

Katalogautor

Die mit der vordefinierten Rolle **Katalogautor** verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu erstellen und zu veröffentlichen.

vApp-Autor

Die mit der vordefinierten Rolle **vApp-Autor** verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu verwenden und vApps zu erstellen.

vApp-Benutzer

Die mit der vordefinierten Rolle **vApp-Benutzer** verknüpften Rechte ermöglichen es einem Benutzer, vorhandene vApps zu verwenden.

Nur Konsolenzugriff

Die mit den vordefinierten Rolle **Nur Konsolenzugriff** verknüpften Rechte ermöglichen es einem Benutzer, den Status und die Eigenschaften von virtuellen Maschinen anzuzeigen und das Gastbetriebssystem zu verwenden.

Auf Identitätsanbieter zurückstellen

Die mit der vordefinierten Rolle **Auf Identitätsanbieter zurückstellen** verknüpften Rechte werden basierend auf vom OAuth- oder SAML-Identitätsanbieter empfangenen Informationen festgelegt. Um sich für die Aufnahme zu qualifizieren, wenn einem Benutzer oder einer Gruppe die Rolle **Auf Identitätsanbieter zurückstellen** zugewiesen ist, muss ein vom Identitätsanbieter bereitgestellter Rollen- oder Gruppenname exakt (unter Berücksichtigung von Groß-/Kleinschreibung) mit einem innerhalb Ihrer Organisation definierten Rollen- oder Gruppennamen übereinstimmen.

- Wenn der Benutzer von einem OAuth-Identitätsanbieter definiert wird, werden dem Benutzer die im Array `roles` des benutzereigenen OAuth-Tokens benannten Rollen zugewiesen.
- Einem von einem SAML-Identitätsanbieter definierten Benutzer werden die Rollen zugewiesen, die in dem SAML-Attribut angegeben werden, dessen Name im Element `RoleAttributeName` angezeigt wird, das sich wiederum im Element `SamlAttributeMapping` in `OrgFederationSettings` der Organisation befindet.

Wenn einem Benutzer die Rolle **Auf Identitätsanbieter zurückstellen** zugewiesen wird, jedoch keine übereinstimmende Rolle bzw. kein übereinstimmender Gruppenname in Ihrer Organisation vorhanden ist, kann sich der Benutzer bei der Organisation anmelden, verfügt jedoch über keine Rechte. Wenn ein Identitätsanbieter einem Benutzer eine Rolle auf Systemebene zuweist, wie beispielsweise die eines **Systemadministrators**, kann sich der Benutzer bei der Organisation anmelden, verfügt jedoch über keine Rechte. Solchen Benutzern müssen Sie eine Rolle manuell zuweisen.

Mit Ausnahme der Rolle **Auf Identitätsanbieter zurückstellen** enthält jede vordefinierte Rolle einen Satz von Standardrechten. Nur ein **Systemadministrator** kann die Rechte in einer vordefinierten Rolle ändern. Wenn ein **Systemadministrator** eine vordefinierte Rolle ändert, werden die Änderungen an alle Instanzen der Rolle im System weitergegeben.

Rechte in vordefinierten globalen Mandantenrollen

Mehrere vordefinierte globale Rollen haben verschiedene Rechte gemein. Diese Rechte werden standardmäßig allen neuen Organisationen gewährt und können in anderen Rollen verwendet werden, die vom **Organisationsadministrator** erstellt werden.

Tabelle 10-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolenz ugriff
Katalog: vApp von „Meine Cloud“ hinzufügen	X	X	X		
Katalog: Externe Veröffentlichung/Externe Abonnements für die Kataloge zulassen	X	X			
Katalog: Besitzer ändern	X				
Katalog: Katalog erstellen/löschen	X	X			
Katalog: Katalogeigenschaften bearbeiten	X	X			
Katalog: Katalog für andere Organisationen freigeben	X	X			
Katalog: Katalog für andere Benutzer/ Gruppen innerhalb der aktuellen Organisation freigeben	X	X			
Katalog: Private und freigegebene Kataloge innerhalb der aktuellen Organisation anzeigen	X	X	X		
Katalog: Freigegebene Kataloge von anderen Organisationen anzeigen	X				
Katalogelement: Zu „Meine Cloud“ hinzufügen	X	X	X	X	
Katalogelement: vApp-Vorlage/Medien kopieren/verschieben	X	X	X		
Katalogelement: vApp-Vorlage/Medien erstellen/hochladen	X	X			
Katalogelement: vApp-Vorlage/Medien bearbeiten	X	X			
Katalogelement: Herunterladen von vApp- Vorlagen/-Medien aktivieren	X	X			
Katalogelement: vApp-Vorlagen/Medien anzeigen	X	X	X	X	
Benutzerdefinierte Entität: Alle benutzerdefinierten Entitätsinstanzen in der Organisation anzeigen	X				
Benutzerdefinierte Entität: Benutzerdefinierte Entitätsinstanz anzeigen	X				
Datenträger: Besitzer ändern	X	X			
Datenträger: Datenträger erstellen	X	X	X		
Datenträger: Datenträger löschen	X	X	X		
Datenträger: Datenträgereigenschaften bearbeiten	X	X	X		

Tabelle 10-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolenz ugriff
Datenträger: Datenträgereigenschaften anzeigen	X	X	X	X	
Verteilte Firewall: Regeln der verteilten Firewall konfigurieren	X				
Distributed Firewall: Distributed Firewall aktivieren/deaktivieren	X				
Verteilte Firewall: Regeln der verteilten Firewall anzeigen	X				
Edge-Cluster: Edge-Cluster anzeigen	X				
Edge-Cluster: Edge-Cluster verwalten	X				
Gateway: Syslog-Server konfigurieren	X				
Gateway: Systemprotokollierung konfigurieren	X				
Gateway: In erweitertes Gateway konvertieren	X				
Gateway: Gateway anzeigen	X				
Gateway: Distributed Routing aktivieren	X				
Gateway: Edge-Gateway importieren	X				
Gateway-Dienste: BGP-Routing konfigurieren					
Gateway-Dienste: DHCP konfigurieren	X				
Gateway-Dienste: Firewall konfigurieren	X				
Gateway-Dienste: IPSEC-VPN konfigurieren	X				
Gateway-Dienste: L2-VPN konfigurieren					
Gateway-Dienste: Lastausgleichsdienst konfigurieren	X				
Gateway-Dienste: NAT konfigurieren	X				
Gateway-Dienste: OSPF-Routing konfigurieren	X				
Gateway-Dienste: Remotezugriff konfigurieren	X				
Gateway-Dienste: SSL-VPN konfigurieren	X				
Gateway-Dienste: Statisches Routing konfigurieren	X				
Gateway-Dienste: Nur Ansicht „BGP-Routing“	X				

Tabelle 10-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadministrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
Gateway-Dienste: Nur Ansicht „DHCP“	X				
Gateway-Dienste: Nur Ansicht „Firewall“	X				
Gateway-Dienste: Nur Ansicht „IPSEC-VPN“	X				
Gateway-Dienste: Nur Ansicht „L2 VPN“	X				
Gateway-Dienste: Nur Ansicht „Lastausgleichsdienst“	X				
Gateway-Dienste: Nur Ansicht „NAT“	X				
Gateway-Dienste: Nur Ansicht „OSPF-Routing“	X				
Gateway-Dienste: Nur Ansicht „Remotenzugriff“	X				
Gateway-Dienste: Nur Ansicht „SSL-VPN“	X				
Gateway-Dienste: Nur Ansicht „Statisches Routing“	X				
Allgemein: Administratorsteuerung	X				
Allgemein: Administratoransicht	X				
Allgemein: Benachrichtigung senden	X				
Hybrid-Tunnel: Ticket zur Steuerung abrufen	X				
Hybrid-Tunnel: Ticket für Aus-der-Cloud-Tunnel abrufen	X				
Hybrid-Tunnel: Cloud-Tunnel-Ticket abrufen	X				
Hybrid-Tunnel: Aus-der-Cloud-Tunnel erstellen	X				
Hybrid-Tunnel: Cloud-Tunnel erstellen	X				
Hybrid-Tunnel: Aus-der-Cloud-Tunnel löschen	X				
Hybrid-Tunnel: Cloud-Tunnel löschen	X				
Hybrid-Tunnel: Endpunkt-Tag des Aus-der-Cloud-Tunnels aktualisieren	X				
Hybrid-Tunnel: Cloud-Tunnel-Server-Einstellungen anzeigen	X				
Hybrid-Tunnel: Aus-der-Cloud-Tunnel anzeigen	X				
Hybrid-Tunnel: Cloud-Tunnel anzeigen	X				

Tabelle 10-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolenz ugriff
Organisation: Zugriff auf alle Organisations-VDCs zulassen	X				
Organisation: Zugriffskontrollliste von Organisations-VDCs bearbeiten	X				
Organisation: Verbundeinstellungen bearbeiten	X				
Organisation: Lease-Richtlinie bearbeiten	X				
Organisation: Organisationsverknüpfungen bearbeiten	X				
Organisation: Netzwerkeinstellungen einer Organisation bearbeiten	X				
Organisation: OAuth-Einstellungen der Organisation bearbeiten	X				
Organisation: Organisationseigenschaften bearbeiten	X				
Organisation: Kennwortrichtlinie bearbeiten	X				
Organisation: Kontingent-Richtlinie bearbeiten	X				
Organisation: SMTP-Einstellungen bearbeiten	X				
Organisation: Benutzer/Gruppe beim Bearbeiten der VDC-ACL implizit aus Identitätsanbieter importieren	X				
Organisation: Zugriffskontrollliste von Organisations-VDCs anzeigen	X				
Organisation: Katalog-ACL anzeigen	X	X			
Organisation: Organisationsnetzwerke anzeigen	X				
Organisation: Organisationen anzeigen	X	X	X		
Organisation: vApp-ACL anzeigen	X	X	X	X	
Organisations-VDC: VDC-Namen und -Beschreibung der Organisation bearbeiten	X				
Organisations-VDC: VM-VM-Affinitätsregel bearbeiten	X	X	X		
Organisations-VDC: Erweiterte Eigenschaften des Organisations-VDC bearbeiten	X				

Tabelle 10-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte
(Fortsetzung)

Name des Rechts	Organisationsadmi nistrator	Katalogautor	vApp- Autor	vApp- Benutzer	Nur Konsolenz ugriff
Organisations-VDC: Firewall verwalten	X				
Organisations-VDC: Standardmäßige Speicherrichtlinie festlegen	X				
Organisations-VDC: Computing-Richtlinien für ein Organisations-VDC anzeigen	X	X	X	X	
Organisations-VDC: Erweiterte Eigenschaften des Organisations-VDC anzeigen	X				
VDC-Organisationsnetzwerk: Eigenschaften anzeigen	X				
VDC-Organisationsnetzwerk: Eigenschaften bearbeiten	X				
VDC-Organisationsnetzwerk: Netzwerk importieren	X				
Organisations-VDC: Organisations-VDCs anzeigen	X				
Organisations-VDC-Vorlage: Organisations-VDC-Vorlagen instanziiieren	X				
Organisations-VDC-Vorlage: VDC-Vorlagen anzeigen	X				
Provider-Netzwerk: Provider-Netzwerk anzeigen	X				
Provider-Netzwerk: Provider-Netzwerk erstellen/löschen	X				
Rolle: Rolle erstellen/aktualisieren/löschen	X				
Dienstbibliothek: Dienste anzeigen, die in der Dienstbibliothek enthalten sind	X				
Benutzer: Gruppe/Benutzer anzeigen	X				
VCD-Erweiterung: Informationen zum Mandantenportal-Plug-In anzeigen	X	X	X	X	
VDC-Gruppe: VDC-Gruppe anzeigen	X				
VDC-Gruppe: VDC-Gruppe konfigurieren	X				
VM-Überwachung: Historische Metriken für die Organisation anzeigen	X				
VM-Überwachung: Historische Metriken für das Organisations-VDC anzeigen	X				
vApp: Auf die VM-Konsole zugreifen	X	X	X	X	X

Tabelle 10-1. In den globalen Mandantenrollen in vCloud Director enthaltene Rechte (Fortsetzung)

Name des Rechts	Organisationsadministrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
vApp: Zulassen, dass Metadaten Domäne zu vCenter Server zuordnen	X	X	X		
vApp: Besitzer ändern	X				
vApp: vApp-Vorlagenbesitzer ändern	X	X			
vApp: vApp kopieren	X	X	X	X	
vApp: vApp erstellen/neu konfigurieren	X	X	X		
vApp: Snapshot erstellen/wiederherstellen/entfernen	X	X	X	X	
vApp: vApp löschen	X	X	X	X	
vApp: vApp herunterladen	X	X	X		
vApp: VM-Startoptionen bearbeiten/anzeigen	X	X	X		
vApp: CPU der VM bearbeiten	X	X	X		
vApp: Festplatte der VM bearbeiten	X	X	X		
vApp: Arbeitsspeicher der VM bearbeiten	X	X	X		
vApp: VM-Netzwerk bearbeiten	X	X	X	X	
vApp: VM-Eigenschaften bearbeiten	X	X	X	X	
vApp: vApp-Eigenschaften bearbeiten	X	X	X	X	
vApp: VM-Computing-Richtlinie bearbeiten	X	X	X		
vApp: VM-Kennworteinstellungen verwalten	X	X	X	X	X
vApp: vApp freigeben	X	X	X	X	
vApp: vApp starten/beenden/anhalten/zurücksetzen	X	X	X	X	
vApp: vApp hochladen	X	X	X		
vApp: VM-Metriken anzeigen	X		X	X	

Informationen zu den neuen Rechten, die von vCloud Director 9.7 eingeführt werden, finden Sie unter [Neue Rechte in dieser Version](#).

Neue Rechte in dieser Version

vCloud Director 9.7 führt neue Rechte ein, die Sie möglicherweise zu allen vorhandenen globalen Rollen hinzufügen möchten, die Sie für Ihre Mandanten veröffentlicht haben.

Recht	Beschreibung	Standardrolle
SDDC: SDDC anzeigen	Ermöglicht Ihnen, alle SDDCs anzuzeigen, die in Ihrer Organisation veröffentlicht wurden. Der Systemadministrator kann alle SDDCs anzeigen.	Systemadministrator und Organisationsadministrator
SDDC: SDDC verwalten	Ermöglicht Ihnen, SDDCs hinzuzufügen, zu entfernen und zu bearbeiten.	Systemadministrator
SDDC: SDDC-Proxy verwalten	Ermöglicht Ihnen, SDDC-Proxys hinzuzufügen, zu entfernen, zu aktivieren und zu deaktivieren.	Systemadministrator
Dienstanwendungen: Dienstanwendungen anzeigen	Ermöglicht Ihnen, die Liste der registrierten Dienstanwendungen anzuzeigen. Wird für VMC-Konten verwendet.	Systemadministrator
Dienstanwendungen: VMC-SDDC registrieren	Ermöglicht Ihnen, Dienstanwendungen zu erstellen, anzuzeigen, zu bearbeiten und zu entfernen. Wird für VMC-Konten verwendet.	Systemadministrator
Dienstanwendungen: Dienstanwendungen verwalten	Ermöglicht Ihnen, Dienstanwendungen zu registrieren. Wird für VMC-Konten verwendet.	Systemadministrator
Edge-Cluster: Edge-Cluster anzeigen	Ermöglicht Ihnen, eine Liste von Edge-Clustern anzuzeigen und einen einzelnen Edge-Cluster abzurufen.	Systemadministrator und Organisationsadministrator
Edge-Cluster: Edge-Cluster verwalten	Ermöglicht Ihnen, Edge-Cluster zu erstellen, zu bearbeiten und zu entfernen.	Systemadministrator und Organisationsadministrator
vApp: VM-Computing-Richtlinie bearbeiten	Ermöglicht Benutzern die Änderung der Computing-Richtlinie einer virtuellen Maschine.	Systemadministrator , Organisationsadministrator , Katalogautor und vApp-Autor
Gateway: Edge-Gateway importieren	Ermöglicht Ihnen, einen Tier-1-Router als Edge-Gateway zu importieren.	Systemadministrator und Organisationsadministrator

Informationen zum Verwalten von Mandantenrechten und -rollen finden Sie im *vCloud Director Service Provider Admin Portal-Handbuch*.


Verwalten von Rechtepaketen

Als Systemadministrator können Sie Rechtepakete erstellen und sie in einer oder mehreren Organisationen in Ihrer Cloud veröffentlichen. Vorhandene Rechtepakete können Sie bearbeiten und löschen. Sie können die Veröffentlichung von Rechtepaketen aus den Organisationen in Ihrer Cloud rückgängig machen.

Erstellen eines Rechtepakets

Sie können einen Satz mit Rechten als Rechtepaket gruppieren, das Sie für eine oder mehrere Organisationen in Ihrem System veröffentlichen können.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Rechtepakete**.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für das neue Rechtepaket ein.
- 5 Wählen Sie die Rechte aus, die Sie diesem Paket zuordnen möchten.

Die Rechte sind in Kategorien und Unterkategorien für Anzeige- oder Verwaltungszugriff auf das Objekt, auf das sie sich beziehen, gruppiert.

Sie können die Rechte einzeln, nach Unterkategorie für Anzeige- oder Verwaltungszugriff oder global nach Anzeige- oder Verwaltungszugriff auswählen.

Kategorie	Beschreibung
Zugriffssteuerung	Enthält Rechte für die Ansicht und Verwaltung von Organisationen, Rechten, Rollen und Benutzern.
Administration	Enthält Rechte für die Ansicht und Verwaltung allgemeiner Einstellungen und der Einstellungen für mehrere Standorte.
Computing	Enthält die Rechte für die Ansicht und Verwaltung von Organisationen und Provider-VDCs, vApps, Vorlagen für Organisations-VDCs und VM-Überwachung.
Erweiterungen	Enthält Rechte für die Ansicht und Verwaltung von vCloud Director-Plug-Ins und -Erweiterungen.
Infrastruktur	Enthält Rechte für die Ansicht und Verwaltung von vSphere-Ressourcen.
Bibliotheken	Enthält Rechte für die Ansicht und Verwaltung von Katalogen und Katalogelementen.
Netzwerk	Enthält Rechte für die Ansicht und Verwaltung von Netzwerkressourcen.

- 6 Klicken Sie auf **Speichern**.

Nächste Schritte


Sie können das neu erstellte Rechtepakete für eine oder mehrere Organisationen in Ihrem System veröffentlichen. Weitere Informationen finden Sie unter [Veröffentlichen oder Aufheben der Veröffentlichung eines Rechtepakets](#).

Veröffentlichen oder Aufheben der Veröffentlichung eines Rechtepakets

Sie können ein Rechtepakete für eine oder mehrere Organisationen in Ihrem System veröffentlichen. Nach der Veröffentlichung eines Rechtepakets für eine Organisation werden die Rechte in diesem Paket Teil des Satzes von Rechten der Organisation.

Die Rechte einer Organisation können mehrere Rechtepakete umfassen, aber die Organisationsadministratoren und Benutzer sehen einfach eine Liste aller Rechte, die sie zum Erstellen und Ändern von Rollen verwenden können.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Rechtepakete**.
- 3 Wählen Sie das Optionsfeld neben dem gewünschten Paket und klicken Sie auf **Veröffentlichen**.
- 4 So veröffentlichen Sie das Paket:
 - a Wählen Sie **An Mandanten veröffentlichen**.
 - b Wählen Sie die Organisationen aus, für welche die Rolle veröffentlicht werden soll.
 - Wenn Sie das Paket für alle vorhandenen und neu erstellten Organisationen in Ihrem System veröffentlichen möchten, aktivieren Sie **An alle Mandanten veröffentlichen**.
 - Wenn Sie das Paket für bestimmte Organisationen in Ihrem System veröffentlichen möchten, wählen Sie die Organisationen einzeln aus.
- 5 So machen Sie die Veröffentlichung des Pakets rückgängig:
 - Wenn Sie die Veröffentlichung des Pakets von allen Organisationen in Ihrem System rückgängig machen möchten, deaktivieren Sie **An Mandanten veröffentlichen**.
 - Wenn Sie die Veröffentlichung des Pakets von bestimmten Organisationen in Ihrem System rückgängig machen möchten, deaktivieren Sie **An alle Mandanten veröffentlichen** und deaktivieren Sie die Organisationen einzeln.
- 6 Klicken Sie auf **Speichern**.

Ergebnisse


Die Rechte im veröffentlichten Paket sind in den ausgewählten Organisationen verfügbar und können in den Rollen dieser Organisationen verwendet werden.

Die Rechte in der Rolle, deren Veröffentlichung rückgängig gemacht wurde, werden aus den ausgewählten Organisationen entfernt und können in den Rollen dieser Organisationen nicht mehr verwendet werden.

Anzeigen und Bearbeiten von Rechtepaketen

Sie können die Rechte anzeigen, die in einem Rechtepaket enthalten sind. Sie können den Namen, die Beschreibung und die Rechte eines Pakets bearbeiten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Rechtepakete**.
- 3 Klicken Sie auf den Namen des gewünschten Pakets.

Sie können die dem Paket zugeordneten Rechte ansehen, indem Sie die Rechtekategorien erweitern.
- 4 Bearbeiten Sie das Paket und klicken Sie auf **Behalten**.


Ergebnisse

Wenn Sie die Rechte des Pakets geändert haben, wird der neue Satz von Rechten für alle Organisationen angewendet, für die dieses Rechtepaket veröffentlicht wird.

Löschen eines Rechtepakets

Sie können ein Rechtepaket entfernen, wenn Sie es in Ihren Organisationen nicht mehr verwenden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Rechtepakete**.
- 3 Wählen Sie das Optionsfeld neben dem gewünschten Paket aus und klicken Sie auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Verwalten von globalen Mandantenrollen

Als Systemadministrator können Sie globale Mandantenrollen erstellen und sie in einer oder mehreren Organisationen in Ihrer Cloud veröffentlichen. Sie können vorhandene globale Mandantenrollen bearbeiten und löschen. Sie haben die Möglichkeit, die Veröffentlichung globaler Mandantenrollen aus einzelnen Organisationen in Ihrer Cloud rückgängig zu machen.

Nach der ersten Installation und Einrichtung von vCloud Director enthält das System eine Reihe vordefinierter globaler Mandanten, die für alle Organisationen veröffentlicht werden. Weitere Informationen finden Sie unter [Vordefinierte Rollen und ihre Rechte](#).


Erstellen einer globalen Mandantenrolle

Sie können eine globale Mandantenrolle erstellen, die Sie für eine oder mehrere Organisationen in Ihrem System veröffentlichen können.

Nach der ersten Installation und Einrichtung von vCloud Director enthält das System vordefinierte globale Mandantenrollen, die für alle Organisationen veröffentlicht werden. Informationen zu den vordefinierten Rollen erhalten Sie unter [Vordefinierte Rollen und ihre Rechte](#).

Sie können benutzerdefinierte globale Rollen zu Ihrem System hinzufügen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Globale Rollen**.
- 3 Klicken Sie auf **Hinzufügen**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die neue Rolle ein.
- 5 Wählen Sie die Rechte aus, die Sie dieser Rolle zuordnen möchten.

Die Rechte sind in Kategorien und Unterkategorien für Anzeige- oder Verwaltungszugriff auf das Objekt, auf das sie sich beziehen, gruppiert.

Sie können die Rechte einzeln, nach Unterkategorie für Anzeige- oder Verwaltungszugriff oder global nach Anzeige- oder Verwaltungszugriff auswählen.

Kategorie	Beschreibung
Zugriffssteuerung	Enthält Rechte für die Ansicht und Verwaltung von Organisationen, Rechten, Rollen und Benutzern.
Administration	Enthält Rechte für die Ansicht und Verwaltung allgemeiner Einstellungen und der Einstellungen für mehrere Standorte.
Computing	Enthält die Rechte für die Ansicht und Verwaltung von Organisationen und Provider-VDCs, vApps, Vorlagen für Organisations-VDCs und VM-Überwachung.
Erweiterungen	Enthält Rechte für die Ansicht und Verwaltung von vCloud Director-Plug-Ins und -Erweiterungen.
Infrastruktur	Enthält Rechte für die Ansicht und Verwaltung von vSphere-Ressourcen.
Bibliotheken	Enthält Rechte für die Ansicht und Verwaltung von Katalogen und Katalogelementen.
Netzwerk	Enthält Rechte für die Ansicht und Verwaltung von Netzwerkressourcen.

- 6 Klicken Sie auf **Behalten**.

Ergebnisse

Bei der Erstellung ist das neue globale Mandantenrecht nur für die Organisation des vCloud Director-Anbieters verfügbar.

Nächste Schritte

Sie können die neu erstellte Rolle für eine oder mehrere Organisationen in Ihrem System veröffentlichen. Weitere Informationen finden Sie unter [Veröffentlichen oder Rückgängigmachen der Veröffentlichung einer globalen Mandantenrolle](#).


Veröffentlichen oder Rückgängigmachen der Veröffentlichung einer globalen Mandantenrolle

Sie können eine globale Mandantenrolle für eine oder mehrere Organisationen in Ihrem System veröffentlichen. Nachdem Sie eine Rolle für eine Organisation veröffentlicht haben, wird diese Rolle Teil des Satzes von Mandantenrollen dieser Organisation.

Voraussetzungen

Wenn Sie die Veröffentlichung einer globalen Mandantenrolle von einer Organisation aufheben möchten, müssen Sie sich vorher vergewissern, dass dieser Rolle kein Benutzer in der Organisation zugewiesen ist.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Globale Rollen**.
- 3 Wählen Sie das Optionsfeld neben der gewünschten Rolle und klicken Sie auf **Veröffentlichen**.
- 4 So veröffentlichen Sie die Rolle:
 - a Wählen Sie **An Mandanten veröffentlichen**.
 - b Wählen Sie die Organisationen aus, für welche die Rolle veröffentlicht werden soll.
 - Wenn Sie die Rolle für alle vorhandenen und neu erstellten Organisationen in Ihrem System veröffentlichen möchten, wählen Sie **An alle Mandanten veröffentlichen**.
 - Wenn Sie die Rolle für bestimmte Organisationen in Ihrem System veröffentlichen möchten, wählen Sie die Organisationen einzeln aus.
- 5 So machen Sie die Veröffentlichung der Rolle rückgängig:
 - Wenn Sie die Veröffentlichung der Rolle von allen Organisationen in Ihrem System rückgängig machen möchten, deaktivieren Sie **An Mandanten veröffentlichen**.
 - Wenn Sie die Veröffentlichung der Rolle von bestimmten Organisationen in Ihrem System rückgängig machen möchten, deaktivieren Sie **An alle Mandanten veröffentlichen** und deaktivieren Sie die Organisationen einzeln.

6 Klicken Sie auf **Speichern**.

Ergebnisse


Die veröffentlichte Rolle ist in den ausgewählten Organisationen verfügbar und kann Benutzern in diesen Organisationen zugewiesen werden. Organisationsadministratoren können globale Mandantenrollen, die in ihren Organisationen veröffentlicht werden, nicht bearbeiten.

Die Rolle, deren Veröffentlichung rückgängig gemacht wurde, wird aus den ausgewählten Organisationen entfernt und kann Benutzern in diesen Organisationen nicht mehr zugewiesen werden.

Anzeigen und Bearbeiten einer globalen Mandantenrolle

Sie können die Rechte anzeigen, die in einer globalen Mandantenrolle enthalten sind. Sie können den Namen, die Beschreibung und die Rechte einer globalen Mandantenrolle bearbeiten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Globale Rollen**.
- 3 Klicken Sie auf den Namen der gewünschten Rolle.

Sie können die der Rolle zugeordneten Rechte ansehen, indem Sie die Rechtekategorien erweitern.

- 4 Klicken Sie auf **Bearbeiten**, um den Namen, die Beschreibung oder die Rechte der Rolle zu bearbeiten.
- 5 Bearbeiten Sie die Rolle und klicken Sie auf **Behalten**.

Ergebnisse

Wenn Sie die Rechte der Rolle geändert haben, wird der neue Satz von Rechten auf die Benutzer in allen Organisationen angewendet, denen diese Rolle zugewiesen wurde.


Löschen einer globalen Mandantenrolle

Sie können eine globale Mandantenrolle entfernen, die Sie in Ihren Organisationen nicht mehr verwenden.

Voraussetzungen

Die globale Mandantenrolle, die Sie löschen möchten, darf in keiner Organisation einem Benutzer zugewiesen sein.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Mandant** auf **Globale Rollen**.

- 3 Wählen Sie das Optionsfeld neben der gewünschten Rolle und klicken Sie auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Verwalten von Anbieterrollen

Sie können Rollen in der Organisation Ihres vCloud Director-Anbieters erstellen.

Informationen zum Verwalten von Mandantenrollen finden Sie im *Handbuch für das vCloud Director Mandantenportal*.

Erstellen einer Anbieterrolle


Sie können eine Rolle in der Organisation Ihres vCloud Director-Anbieters erstellen.

Nach der ersten Installation und Einrichtung von vCloud Director enthält das System vordefinierte Rollen, die für die Anbieterorganisation lokal und für alle Organisationen global sind.

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

Sie können benutzerdefinierte Anbieterrollen zu Ihrer Anbieterorganisation hinzufügen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Rollen**.
- 3 Klicken Sie auf **Neu**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die neue Rolle ein.
- 5 Wählen Sie die Rechte aus, die Sie dieser Rolle zuordnen möchten.

Die Rechte sind in Kategorien und Unterkategorien für Anzeige- oder Verwaltungszugriff auf das Objekt, auf das sie sich beziehen, gruppiert.

Sie können die Rechte einzeln, nach Unterkategorie für Anzeige- oder Verwaltungszugriff oder global nach Anzeige- oder Verwaltungszugriff auswählen.

Kategorie	Beschreibung
Zugriffssteuerung	Enthält Rechte für die Ansicht und Verwaltung von Organisationen, Rechten, Rollen und Benutzern.
Administration	Enthält Rechte für die Ansicht und Verwaltung allgemeiner Einstellungen und der Einstellungen für mehrere Standorte.
Computing	Enthält die Rechte für die Ansicht und Verwaltung von Organisationen und Provider-VDCs, vApps, Vorlagen für Organisations-VDCs und VM-Überwachung.
Erweiterungen	Enthält Rechte für die Ansicht und Verwaltung von vCloud Director-Plug-Ins und -Erweiterungen.
Infrastruktur	Enthält Rechte für die Ansicht und Verwaltung von vSphere-Ressourcen.

Kategorie	Beschreibung
Bibliotheken	Enthält Rechte für die Ansicht und Verwaltung von Katalogen und Katalogelementen.
Netzwerk	Enthält Rechte für die Ansicht und Verwaltung von Netzwerkressourcen.

6 Klicken Sie auf **Speichern**.


Ergebnisse

Die neu erstellte Rolle ist für die Zuweisung zu Benutzern in Ihrer Anbieterorganisation verfügbar.

Anzeigen oder Bearbeiten einer Anbieterrolle

Sie können die Rechte anzeigen, die in einer Rolle enthalten sind, die für Ihre vCloud Director-Anbieterorganisation lokal ist. Sie können den Namen, die Beschreibung und die Rechte einer Rolle bearbeiten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Rollen**.
- 3 Klicken Sie auf den Namen der gewünschten Rolle.
Sie können die der Rolle zugeordneten Rechte ansehen, indem Sie die Rechtekategorien erweitern.
- 4 Klicken Sie auf **Bearbeiten**, um den Namen, die Beschreibung oder die Rechte der Rolle zu bearbeiten.
- 5 Bearbeiten Sie die Rolle und klicken Sie auf **Speichern**.

Ergebnisse

Wenn Sie die Rechte der Rolle geändert haben, wird der neue Satz von Rechten auf die Benutzer angewendet, denen diese Rolle zugewiesen wurde.


Löschen einer Anbieterrolle

Sie können eine Rolle entfernen, die Sie in Ihrer vCloud Director-Anbieterorganisation nicht mehr verwenden.

Voraussetzungen

Die Rolle, die Sie löschen möchten, darf keinem Benutzer zugewiesen sein.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Rollen**.

- 3 Wählen Sie das Optionsfeld neben der gewünschten Rolle und klicken Sie auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Verwalten von Anbieterbenutzern und -gruppen

Sie können Benutzer und Gruppen zu Ihrer vCloud Director-Anbieterorganisation hinzufügen und in diese importieren.

Informationen zum Verwalten von Organisationsbenutzern und -gruppen finden Sie im *Handbuch für das vCloud Director Mandantenportal*.

Verwalten von Anbieterbenutzern

Sie können die Benutzer in Ihrer Anbieterorganisation über das Service Provider Admin Portal verwalten.


Informationen zum Verwalten von Mandantenbenutzern in Organisationen finden Sie im *Handbuch für das vCloud Director Mandantenportal*.

Erstellen eines Anbieterbenutzers

Sie können in der Organisation Ihres vCloud Director-Anbieters einen Benutzer erstellen.

Während der Installation und Einrichtung von vCloud Director können Sie ein **Systemadministrator**-Konto erstellen. Nach der ersten Einrichtung können Sie zusätzliche Administratoren und Benutzer für die Anbieterorganisation erstellen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Benutzer**.
- 3 Klicken Sie auf **Neu**.
- 4 Geben Sie einen Benutzernamen und ein Kennwort für den neuen Benutzer ein.
Das Kennwort muss mindestens sechs Zeichen enthalten.
- 5 Wählen Sie aus, ob der Benutzer bei der Erstellung aktiviert werden soll.
- 6 Wählen Sie im Dropdown-Menü **Verfügbare Rollen** eine Rolle für den Benutzer aus.
Die Liste verfügbarer Rollen umfasst die globalen Rollen und die lokalen Rollen für Ihre Systemorganisation.
- 7 (Optional) Geben Sie Kontaktinformationen für den Benutzer ein.
Sie können den vollständigen Namen, die E-Mail-Adresse, Telefonnummer und Instant Messaging-ID eingeben.

8 (Optional) Legen Sie die Kontingente für den Benutzer fest.

- a Sie können einen Grenzwert für die dem Benutzer gehörenden virtuellen Maschinen eingeben oder **Unbegrenzt** auswählen.
- b Sie können einen Grenzwert für die dem Benutzer gehörenden ausgeführten virtuellen Maschinen eingeben oder **Unbegrenzt** auswählen.


Anbieterbenutzer importieren

Sie können Benutzer aus einem zuvor konfigurierten LDAP- oder SAML-Identitätsanbieter in Ihre vCloud Director-Anbieterorganisation importieren.

Voraussetzungen

[Konfigurieren einer System-LDAP-Verbindung](#) oder [Konfigurieren Ihres Systems für die Verwendung eines SAML-Identitätsanbieters](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Benutzer**.
- 3 Klicken Sie auf **Benutzer importieren**.
- 4 Wählen Sie im Dropdown-Menü **Quelle** den Identitätsanbietertyp aus.
Hierbei kann es sich um **LDAP** oder **SAML** handeln.
Wenn Sie nur einen Identitätsanbieter konfiguriert haben, ist diese Option hartcodiert.
- 5 Geben Sie die Benutzer an.

Option	Beschreibung
LDAP	<ul style="list-style-type: none"> a Geben Sie einen vollständigen Namen oder den Teil eines Namens eines Benutzers ein und klicken Sie auf Suchen. b Wählen Sie aus den Suchergebnissen die Benutzer aus, die Sie importieren möchten. c Wählen Sie im Dropdown-Menü Rolle zuweisen eine Rolle für die Benutzer aus.
SAML	<ul style="list-style-type: none"> a Geben Sie die Benutzernamen der Benutzer ein, die Sie importieren möchten. Verwenden Sie dabei das vom SAML-Identitätsanbieter unterstützte Namensbezeichnerformat. Verwenden Sie für jeden Benutzernamen eine neue Zeile. b Wählen Sie im Dropdown-Menü Rolle zuweisen eine Rolle für die Benutzer aus.

- 6 Klicken Sie auf **Speichern**.


Ergebnisse

Sie können die importierten Benutzer in der Liste der Benutzer sehen.

Bearbeiten eines Anbieterbenutzers

Sie können das Kennwort, die Rolle, die Kontaktinformationen und die Kontingente eines Benutzers in Ihrer Anbieterorganisation ändern. Den Benutzernamen können Sie nicht ändern.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Benutzer**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Benutzers und anschließend auf **Bearbeiten**.
- 4 Bearbeiten Sie die Benutzerdetails und klicken Sie auf **Speichern**.

Aktivieren oder Deaktivieren eines Anbieterbenutzers

Nachdem Sie einen Benutzer deaktivieren, kann sich dieser nicht bei vCloud Director anmelden.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Benutzer**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Benutzers und anschließend auf **Deaktivieren** oder **Aktivieren**.
- 4 Wenn Sie einen Benutzer deaktivieren, bestätigen Sie die Einstellung mit einem Klick auf **OK**.


Löschen eines Anbieterbenutzers

Sie können einen Benutzer aus der vCloud Director-Anbieterorganisation entfernen, indem Sie das Benutzerkonto löschen.

Voraussetzungen

Deaktivieren Sie den Benutzer, den Sie löschen möchten. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren eines Anbieterbenutzers](#).

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Benutzer**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Benutzers und dann auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Entsperren eines Anbieterbenutzers

Wenn Sie die Kontosperrung in den Systemeinstellungen für Ihre Kennwortrichtlinie aktiviert haben, werden Benutzerkonten möglicherweise nach einer bestimmten Zahl von ungültigen Anmeldeversuchen gesperrt. Selbst wenn die Sperre mit einem Kontosperrungsintervall eingestellt wurde, können Sie ein Benutzerkonto bereits vor Ablauf der Sperre entsperren.

Informationen zur Konfiguration der Kontosperrungsrichtlinie finden Sie im *vCloud Director-Administratorhandbuch*.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Benutzer**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen des gewünschten Benutzers und anschließend auf **Entsperren**.

Verwalten von Anbietergruppen

Sie haben die Möglichkeit, Gruppen aus Ihrer Anbieterorganisation über das Service Provider Admin Portal zu importieren, zu bearbeiten und zu löschen.

Informationen zum Verwalten von Gruppen in Organisationen finden Sie im *Handbuch für das vCloud Director Mandantenportal*.


Importieren einer Anbietergruppe

Sie können Gruppen aus einem zuvor konfigurierten LDAP- oder SAML-Identitätsanbieter in Ihre vCloud Director-Anbieterorganisation importieren.

Voraussetzungen

[Konfigurieren einer System-LDAP-Verbindung](#) oder [Konfigurieren Ihres Systems für die Verwendung eines SAML-Identitätsanbieters](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Gruppen**.
- 3 Klicken Sie auf **Gruppen importieren**.
- 4 Wählen Sie im Dropdown-Menü **Quelle** den Identitätsanbietertyp aus.

Hierbei kann es sich um **LDAP** oder **SAML** handeln.

Wenn Sie nur einen Identitätsanbieter konfiguriert haben, ist diese Option hartcodiert.

5 Geben Sie die Benutzer an.


Option	Beschreibung
LDAP	<ol style="list-style-type: none"> Geben Sie einen vollständigen Namen oder den Teil eines Namens einer Gruppe ein und klicken Sie auf Suchen. Wählen Sie aus den Suchergebnissen die Gruppen aus, die Sie importieren möchten. Wählen Sie im Dropdown-Menü Rolle zuweisen eine Rolle für die Benutzer in den importierten Gruppen aus.
SAML	<ol style="list-style-type: none"> Geben Sie die Namen der Gruppen ein, die Sie importieren möchten. Verwenden Sie dabei das vom SAML-Identitätsanbieter unterstützte Namensbezeichnerformat. Verwenden Sie für jeden Gruppennamen eine neue Zeile. Wählen Sie im Dropdown-Menü Rolle zuweisen eine Rolle für die Benutzer in den importierten Gruppen aus.

6 Klicken Sie auf **Speichern**.

Bearbeiten einer Anbietergruppe

Sie können die Beschreibung der Rolle der Mitglieder einer Gruppe bearbeiten, die Sie vorher in Ihre vCloud Director-Anbieterorganisation importiert haben, und Sie können die Rolle der Mitglieder einer Gruppe ändern.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Gruppen**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der gewünschten Gruppe und anschließend auf **Bearbeiten**.
- 4 Bearbeiten Sie die Gruppendetails und klicken Sie auf **Speichern**.

Löschen einer Anbietergruppe

Sie können eine Gruppe aus der vCloud Director-Anbieterorganisation entfernen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Zugriffssteuerung Anbieter** auf **Gruppen**.
- 3 Klicken Sie auf das Optionsfeld neben dem Namen der gewünschten Gruppe und anschließend auf **Löschen**.
- 4 Klicken Sie zur Bestätigung auf **OK**.

Verwalten der Systemeinstellungen

11

vCloud Director-Systemadministratoren können die systemweit geltenden Einstellungen in Zusammenhang mit LDAP, E-Mail-Benachrichtigung und Lizenzierung sowie allgemeine Systemeinstellungen steuern.

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten von Identitätsanbietern](#)
- [Verwalten von Plug-Ins](#)
- [Anpassen der vCloud Director-Portale](#)

Verwalten von Identitätsanbietern

Sie können Ihre Cloud mit einem externen Identitätsanbieter integrieren und Benutzer und Gruppen in Ihre Organisationen importieren. Sie können eine LDAP-Serververbindung auf der System- oder Organisationsebene konfigurieren. Sie können eine SAML-Integration auf einer Organisationsebene konfigurieren.


Verwalten von LDAP-Verbindungen

Als Systemadministrator können Sie Ihre vCloud Director-Systemorganisation und beliebige andere Organisationen im System für die Verwendung eines LDAP-Servers als Quelle für Benutzer und Gruppen konfigurieren. Die Organisationen können entweder die System-LDAP-Verbindung oder eine private LDAP-Verbindung verwenden.

Konfigurieren einer System-LDAP-Verbindung

Um vCloud Director und den zugehörigen Organisationen gemeinsamen Zugriff auf Benutzer und Gruppen zu ermöglichen, können Sie eine LDAP-Verbindung auf Systemebene konfigurieren.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Identitätsanbieter**, auf **LDAP**.

Die aktuellen LDAP-Einstellungen werden angezeigt.



Nächste Schritte

[Konfigurieren, Testen und Synchronisieren einer LDAP-Verbindung.](#)

Konfigurieren einer Organisations-LDAP-Verbindung

Sie können eine Organisation so konfigurieren, dass die System-LDAP-Verbindung als gemeinsam genutzte Quelle für Benutzer und Gruppen verwendet wird. Zudem können Sie eine Organisation so konfigurieren, dass eine separate LDAP-Verbindung als private Quelle für Benutzer und Gruppen verwendet wird.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisationen**.
- 3 Klicken Sie auf den Namen der gewünschten Organisation.
Sie werden zum vCloud Director-Mandantenportal der Organisation umgeleitet.
- 4 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 5 Klicken Sie im linken Bereich unter **Identitätsanbieter**, auf **LDAP**.
Die aktuellen LDAP-Einstellungen werden angezeigt.
- 6 Klicken Sie auf der Registerkarte **LDAP-Optionen** auf **Bearbeiten**.
- 7 Konfigurieren die LDAP-Quelle für Benutzer und Gruppen für diese Organisation und klicken Sie auf **Speichern**.

Option	Beschreibung
LDAP nicht verwenden	Die Organisation verwendet keinen LDAP-Server als Quelle für Organisationsbenutzer und -gruppen.
LDAP-Dienst des VCD-Systems	Die Organisation verwendet die LDAP-Verbindung des vCloud Director-Systems, die Sie zuvor konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren einer System-LDAP-Verbindung .
Benutzerdefinierter LDAP-Dienst	Die Organisation verwendet einen privaten LDAP-Server als Quelle für Organisationsbenutzer und -gruppen. Klicken Sie auf die Registerkarte Benutzerdefiniertes LDAP und dann auf Konfigurieren, Testen und Synchronisieren einer LDAP-Verbindung .

Konfigurieren, Testen und Synchronisieren einer LDAP-Verbindung

Wenn Sie eine LDAP-Verbindung für ein System oder eine Organisation konfigurieren möchten, legen Sie die Details Ihres 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 vCloud Director jederzeit mit dem LDAP-Server synchronisieren.

Voraussetzungen

Wenn Sie eine Verbindung mit einem LDAPS-Server herstellen möchten, stellen Sie sicher, dass Sie über ein ordnungsgemäß erstelltes Zertifikat für die verbesserte LDAP-Unterstützung in Java 8 Update 181 verfügen. Weitere Informationen finden Sie in den *Java 8-Versionsänderungen* unter <https://www.java.com>.

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 vCloud Director verbunden werden soll. Um die Verbindung im Root-Verzeichnis herzustellen, geben Sie nur die Domänenkomponenten ein, beispielsweise DC=beispiel,DC=com . Wenn Sie eine Verbindung mit einem Knoten in der Baumstruktur herstellen möchten, geben Sie den DN 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 vCloud 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 das Symbol zum Hochladen () und importieren Sie ein LDAP-SSL-Zertifikat oder wählen Sie Alle Zertifikate akzeptieren aus.
Authentifizierungsmethode	Bei der einfachen Authentifizierung wird der DN des Benutzers und das Kennwort an den LDAP-Server übermittelt. Wenn Sie LDAP verwenden, wird das LDAP-Kennwort unverschlüsselt über das Netzwerk gesendet. Wenn Sie Kerberos verwenden möchten, müssen Sie die LDAP-Verbindung mithilfe des vCloud Director-Web-Clients konfigurieren. Weitere Informationen finden Sie unter <i>vCloud Director-Administratorhandbuch</i> .

Erforderliche Informationen	Beschreibung
Benutzername	Der vollständige LDAP-DN-Benutzername zum Herstellen der Verbindung mit dem LDAP-Server. 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 zum Herstellen der Verbindung mit dem LDAP-Server. 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 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**.

- 6 Um vCloud Director mit dem konfigurierten LDAP-Server zu synchronisieren, klicken Sie auf **Synchronisieren**.

vCloud 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.

Konfigurieren Ihres Systems für die Verwendung eines SAML-Identitätsanbieters

Wenn Sie Benutzer und Gruppen aus einem SAML-Identitätsanbieter in Ihre Systemorganisation importieren möchten, müssen Sie Ihre Systemorganisation mit diesem SAML-Identitätsanbieter konfigurieren. Importierte Benutzer können sich mit den im SAML-Identitätsanbieter festgelegten Anmeldedaten bei der Systemorganisation anmelden.

Um vCloud Director mit einem SAML-Identitätsprovider zu konfigurieren, richten Sie durch einen Austausch von Metadaten des SAML-Dienstanbieters und des Identitätsanbieters eine gegenseitige Vertrauensstellung ein.

Wenn ein importierter Benutzer versucht, sich anzumelden, extrahiert das System die folgenden Attribute (sofern sie verfügbar sind) aus dem SAML-Token und interpretiert mit ihrer Hilfe die entsprechenden Informationen über den Benutzer.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"` (dieses Attribut ist konfigurierbar)

Gruppeninformationen werden verwendet, wenn der Benutzer nicht direkt importiert wird, sondern wenn von ihm erwartet wird, dass er sich aufgrund seiner Mitgliedschaft in den importierten Gruppen selbst anmeldet. Ein Benutzer kann mehreren Gruppen angehören und daher während einer Sitzung mehrere Rollen haben.


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 über die API konfiguriert werden und nur das Attribut „Rollen“ ist konfigurierbar. Wenn die Rolle „Auf Identitätsanbieter zurückstellen“ verwendet wird, jedoch keine Rolleninformationen extrahiert werden können, kann sich der Benutzer zwar anmelden, verfügt jedoch über keine Rechte zum Durchführen von Aktivitäten.

Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf einen SAML 2.0-konformen Identitätsanbieter haben.
- Rufen Sie eine XML-Datei mit den folgenden Metadaten vom SAML-Identitätsanbieter ab:
 - 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 für einen SAML-Provider finden Sie in der Dokumentation zu Ihrem SAML-Provider.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Administration** aus.
- 2 Klicken Sie im linken Fensterbereich unter „Identitätsanbieter“ auf **SAML** und dann auf **Bearbeiten**.

Die aktuellen SAML-Einstellungen werden angezeigt.

- 3 Laden Sie über die Registerkarte **Dienstanbieter** die Metadaten des vCloud Director-SAML-Dienstanbieters herunter.

- a Geben Sie eine Element-ID für die Systemorganisation ein.

Die Element-ID identifiziert Ihre Systemorganisation eindeutig gegenüber Ihrem Identitätsanbieter.

- b Überprüfen Sie das Ablaufdatum des Zertifikats. Falls es bald abläuft, generieren Sie das Zertifikat neu, indem Sie auf **Neu generieren** klicken.

Das Zertifikat ist in den SAML-Metadaten enthalten und wird für die Verschlüsselung und Signierung verwendet. Eine oder beide Optionen sind möglicherweise erforderlich, je nachdem, wie die Vertrauensstellung zwischen Ihrem SAML-Identitätsanbieter und Ihrer Organisation eingerichtet ist.


- c Klicken Sie auf den Link **Metadaten**.

Der Link ähnelt der URL `https://VCD_host_name/cloud/org/System/saml/metadata/alias/vcd`.

Ihr Browser lädt die Metadaten des SAML-Dienstanbieters herunter. Dies ist eine XML-Datei, die Sie Ihrem Identitätsanbieter bereitstellen müssen.

- 4 Laden Sie auf der Registerkarte **Identitätsanbieter** die SAML-Metadaten hoch, die Sie zuvor von Ihrem Identitätsanbieter erhalten haben.

- a Wählen Sie **SAML-Identitätsprovider verwenden** aus.

- b Klicken Sie entweder auf das Symbol **Durchsuchen** () und laden Sie die Datei hoch oder kopieren Sie sie und fügen Sie ihren Inhalt in das Textfeld **Metadaten-XML** ein.

- 5 Klicken Sie auf **Speichern**.

Ergebnisse

Verwalten von Plug-Ins

vCloud Director-Plug-Ins erweitern die Funktionen von Service Provider Admin Portal und von vCloud Director Tenant Portal. Sie können Plug-Ins aus dem Service Provider Admin Portal hochladen, deaktivieren und löschen. Sie können ein Plug-In für den Dienstanbieter und einzelne Organisationen veröffentlichen.

Einige Plug-Ins werden als Teil von vCloud Director installiert.

CPOM-Erweiterung

Bietet die Möglichkeit zum Anzeigen und Verwalten von SDDCs und SDDC-Proxys mithilfe von vCloud Director Tenant Portal.

Portal anpassen

Bietet die Möglichkeit zum Anpassen von vCloud Director Service Provider Admin Portal und vCloud Director Tenant Portal.

vCloud-Verfügbarkeit

Das VMware vCloud® Availability™-Plug-In bietet die Möglichkeit, auf das vCloud Availability Portal direkt von der vCloud Director-Benutzeroberfläche. Weitere Informationen finden Sie in der [vCloud Availability-Dokumentation](#).


Hochladen eines Plug-Ins

Sie können zusätzliche Plug-Ins in das vCloud Director Service Provider Admin Portal hochladen, die vom Dienstanbieter und von Organisationen in der Cloud verwendet werden können.

Voraussetzungen

Laden Sie die Installationsdatei für das Plug-In herunter.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Portal anpassen** aus.
- 2 Klicken Sie auf **Upload**.
- 3 Klicken Sie auf **Plug-In-Datei auswählen**, navigieren Sie zur Zielinstallationsdatei und klicken Sie auf **Öffnen**.
- 4 Klicken Sie auf **Weiter**.
- 5 Wählen Sie den Geltungsbereich für dieses Plug-In aus.


Option	Beschreibung
Dienstanbieter	Die Plug-In-Funktion steht nun im vCloud Director Service Provider Admin Portal zur Verfügung.
Mandanten	Die Plug-In-Funktion steht nun im vCloud Director Service Provider Admin Portal der von Ihnen ausgewählten Organisationen zur Verfügung.

- 6 Wenn Sie den Geltungsbereich des Plug-Ins auf Mandanten erweitert haben, wählen Sie die Organisationen aus, für die dieses Plug-In veröffentlicht werden soll.
- 7 Überprüfen Sie die Seite **Überprüfen und beenden** und klicken Sie auf **Beenden**.

Aktivieren oder Deaktivieren eines Plug-Ins

Um alle Organisationen an der Verwendung eines Plug-Ins zu hindern, können Sie dieses Plug-In deaktivieren.


Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Portal anpassen** aus.
- 2 Aktivieren Sie das Kontrollkästchen neben den Namen der Ziel-Plug-Ins und klicken Sie auf **Aktivieren** oder **Deaktivieren**.

Löschen eines Plug-Ins

Sie können ein oder mehrere Plug-Ins aus dem vCloud Director Service Provider Admin Portal entfernen.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Portal anpassen** aus.
- 2 Aktivieren Sie die Kontrollkästchen neben den Namen der Plug-Ins, die Sie entfernen möchten, und klicken Sie auf **Löschen**.
- 3 Klicken Sie zur Bestätigung auf **Speichern**.

Veröffentlichen oder Rückgängigmachen der Veröffentlichung eines Plug-Ins in einer Organisation

Sie können die Gruppe von Organisationen ändern, die die von einem-Plug-In bereitgestellte Funktion verwenden können.

Sie können die Gruppe von Organisationen für mehrere Plug-Ins ändern.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Portal anpassen** aus.
- 2 Aktivieren Sie die Kontrollkästchen neben den Namen der gewünschten Plug-Ins und klicken Sie auf **Veröffentlichen**.
- 3 Wählen Sie den Geltungsbereich für dieses Plug-In aus.

Option	Beschreibung
Dienstanbieter	Die Plug-In-Funktion wird im vCloud Director Service Provider Admin Portal verfügbar.
Mandanten	Die Plug-In-Funktion wird im vCloud Director Service Provider Admin Portal der von Ihnen ausgewählten Organisationen verfügbar.

- 4 Wenn Sie das Plug-In als mandantenzentriert festgelegt haben, wählen Sie die Organisationen aus, für die Sie dieses Plug-In veröffentlichen möchten.

5 Klicken Sie auf **Speichern**.

Anpassen der vCloud Director-Portale

Um Ihre Corporate-Branding-Standards zu erfüllen und eine vollständig benutzerdefinierte Cloud-Erfahrung zu schaffen, können Sie das Logo und das Design für Ihr vCloud Director Service Provider Admin Portal und für das vCloud Director Tenant Portal jeder Organisation festlegen. Darüber hinaus können Sie benutzerdefinierte Links zu den beiden oberen rechten Menüs in den vCloud Director-Portalen ändern und hinzufügen.

Hinweis Um Ihre Branding-Attribute und -Links anzupassen, müssen Sie die branding-vCloud OpenAPI-Methoden verwenden. Weitere Informationen finden Sie unter *Erste Schritte mit vCloud OpenAPI* auf <https://code.vmware.com>.

Portal-Branding

Im Rahmen der Installation enthält vCloud Director zwei Designs: „Standard“ und „Dunkel“. Sie können benutzerdefinierte Designs erstellen, verwalten und anwenden. Darüber hinaus können Sie den Portalnamen, das Logo und das Browsersymbol ändern. Zudem übernimmt der Browser den von Ihnen festgelegten Portalnamen als Titel.

Sie legen die Branding-Attribute auf Systemebene fest, sodass Sie das vCloud Director Service Provider Admin Portal anpassen können. Das vCloud Director Tenant Portal für jede Organisation übernimmt die System-Branding-Attribute, es sei denn, Sie haben Branding-Attribute für den jeweiligen Mandanten konfiguriert.

Für einen bestimmten Mandanten können Sie eine beliebige Kombination aus Portalnamen, Hintergrundfarbe, Logo, Symbol, Design und benutzerdefinierten Links selektiv außer Kraft setzen. Für jeden Wert, den Sie nicht festlegen, wird der entsprechende Systemstandardwert verwendet.

Hinweis Standardmäßig wird das individuelle Mandanten-Branding außerhalb einer angemeldeten Sitzung nicht angezeigt. Das individuelle Mandanten-Branding wird auf der Anmelde- und Abmeldeseite nicht angezeigt, sodass Mandanten die Existenz anderer Mandanten nicht erkennen können. Sie können das Branding außerhalb der angemeldeten Sitzungen mithilfe des Zellenverwaltungstools aktivieren:

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

Informationen zur Verwendung des Zellenverwaltungstools finden Sie im *vCloud Director-Administratorhandbuch*.

Benutzerdefinierte Links

Benutzerdefinierte Links sind eine Komponente des Portal-Branding. Es gibt zwei Arten benutzerdefinierter Links:

- **override**-Menüelemente ersetzen die vorhandenen Links für die Menüelemente **Hilfe**, **Info** und **VMRC herunterladen**. Standardmäßig leitet **VMRC herunterladen** die Benutzer zu <https://my.vmware.com> zum Herunterladen von VMRC weiter, was bedeutet, dass Benutzer über registrierte Konten zum Herunterladen verfügen müssen. Indem Sie diesen Link außer Kraft setzen, können Sie das VMRC-Installationsprogramm auf Ihren eigenen Server verschieben.
- **link**-Menüelemente sind neue Links, die Sie dem Menüelement **Abmelden** in der oberen rechten Ecke des Portals hinzufügen. Die neuen benutzerdefinierten Links werden in der Reihenfolge angezeigt, die im API-Aufruf angegeben ist.

Sie können diese benutzerdefinierten Links mit den Menüelementen **section** und **separator** organisieren. Mit einem **section**-Menüelement wird dem Menü eine Kopfzeile hinzugefügt. Mit einem **separator**-Menüelement wird dem Menü eine Zeile hinzugefügt.

Benutzerdefinierte Links unterstützen benutzerdefinierte Variablen, die Sie verwenden können, um identifizierende Informationen an andere Anwendungen in Form von Abfrageparametern zu übergeben.

vCloud Director unterstützt die folgenden benutzerdefinierten Variablen im `url`-Wert für einen benutzerdefinierten Link:

Tabelle 11-1. Benutzerdefinierte Variablen für benutzerdefinierte Links

Variable	Beschreibung
<code>\${TENANT_NAME}</code>	Name der Organisation
<code>\${TENANT_ID}</code>	Organisations-ID
<code>\${SESSION_TOKEN}</code>	x-vcloud-authorization-Token

Beispiel:

```
url: https://host:port/tenant/${TENANT_NAME}/vdcs
```

im vCloud Director Tenant Portal für die Organisation „myorg“ wird konvertiert in:

```
url: https://host:port/tenant/myorg/vdcs
```

Überwachen von vCloud Director

12

Systemadministratoren können abgeschlossene Vorgänge und aktuell bearbeitete Vorgänge überwachen und Informationen zur Nutzung bzw. Auslastung auf der Ebene des virtuellen Provider-Datencenters, des virtuellen Organisations-Datencenters und des Datenspeichers anzeigen.

Dieses Kapitel enthält die folgenden Themen:

- [vCloud Director und Kostenberichte](#)
- [Anzeigen von Nutzungsinformationen für ein virtuelles Provider-Datencenter](#)

vCloud Director und Kostenberichte

Sie können VMware vRealize Operations Tenant App für vCloud Director verwenden, um ein System zur Erstellung von Kostenberichten für vCloud Director zu konfigurieren.

Die VMware vRealize Operations Tenant App bietet Messfunktionen, mit denen Dienstanbieter ihrer Kundenbasis Rückbelastungsdienste bereitstellen können.

Die VMware vRealize Operations Tenant App ist auch eine mandantenorientierte Anwendung, die Mandantenadministratoren ermöglicht, ihre Umgebung und ihre Abrechnungsdaten zu visualisieren.

Informationen zur Kompatibilität zwischen vCloud Director und VMware vRealize Operations Tenant App finden Sie in den *Tabellen zur Interoperabilität von VMware-Produkten* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.


Sie können die VMware vRealize Operations Tenant App unter <https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director> herunterladen.

Informationen zur Verwendung der VMware vRealize Operations Tenant App finden Sie unter *Verwenden der vRealize Operations Tenant App for vCloud Director als Dienstanbieter* und *Verwenden der vRealize Operations Tenant App for vCloud Director als Mandant*.

Anzeigen von Nutzungsinformationen für ein virtuelles Provider-Datencenter

Virtuelle Provider-Datencenter stellen Rechen-, Arbeitsspeicher- und Speicherressourcen für die virtuellen Datencenter der Organisation bereit. Sie können die Verwendung der Ressourcen des virtuellen Provider-Datencenters überwachen und somit entscheiden, ob Sie weitere Ressourcen hinzufügen möchten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Provider-VDCs** und dann auf den Namen des gewünschten virtuellen Provider-Datencenters.
- 3 Klicken Sie auf die Registerkarte **Metriken > konfigurieren**.
- 4 Nähere Informationen zu den einzelnen Parametern erhalten Sie, indem Sie auf jedes Informationssymbol klicken.

Die Ansicht „Inhaltsbibliotheken“ im vCloud Director Service Provider Admin Portal bietet eine Schnittstelle für die Integration mit vRealize Orchestrator. Die vRealize Orchestrator-Workflows stehen als Dienstkatalog zur Verfügung, den Dienstanbieteradministratoren für Mandanten oder andere Dienstanbieter veröffentlichen und somit die von ihnen bereitgestellten Funktionalitäten und Verwaltungsfunktionen erweitern können.

Dieses Kapitel enthält die folgenden Themen:

- [Integrieren von vRealize Orchestrator mit vCloud Director](#)
- [Erstellen einer Dienstkategorie](#)
- [Bearbeiten einer Dienstkategorie](#)
- [Importieren eines Diensts](#)
- [Auffinden eines Diensts](#)
- [Ausführen eines Diensts](#)
- [Ändern einer Dienstkategorie](#)
- [Aufheben der Registrierung eines Diensts](#)
- [Veröffentlichen eines Diensts](#)

Integrieren von vRealize Orchestrator mit vCloud Director

Sie integrieren vRealize Orchestrator mit vCloud Director über das vCloud Director Service Provider Admin Portal.

Durch die Integration von vRealize Orchestrator mit vCloud Director werden die Basisfunktionen von vCloud Director erweitert, wodurch Dienstanbieteradministratoren komplexe Automatisierungsaufgaben mittels Workflow-Orchestrierung und Nutzung von Drittanbieter-Plugins entwickeln können.

Über das vCloud Director Service Provider Admin Portal können Dienstanbieteradministratoren Workflows aus registrierten vRealize Orchestrator-Serverinstanzen anzeigen, importieren und ausführen.

Im vCloud Director Service Provider Admin Portal können vRealize Orchestrator-Workflows für Dienstanbieter oder Mandanten veröffentlicht werden, wodurch eine schnelle Zugriffssteuerung und die Ausführung von benutzerdefinierten und integrierten Diensten möglich wird.

vRealize Orchestrator verfügt über eine umfangreiche Workflow-Bibliothek mit vordefinierten Aufgaben, die zur Lösung bestimmter Probleme und Durchführung allgemeiner Verwaltungsaufgaben entworfen wurden. Drittanbieter-Plug-Ins sind auch bei der [VMware Solution Exchange](#) erhältlich.



Registrieren einer vRealize Orchestrator-Instanz bei vCloud Director

Zur Nutzung der Orchestrierung von Workflows und Automatisierung von Aufgaben über vRealize Orchestrator in vCloud Director registrieren Sie eine vRealize Orchestrator-Instanz im vCloud Director Service Provider Admin Portal.


Voraussetzungen

- Stellen Sie eine vRealize Orchestrator-Serverinstanz bereit und konfigurieren Sie sie. Weitere Informationen finden Sie unter *Installieren und Konfigurieren von VMware vRealize Orchestrator* in der Dokumentation zu vRealize Orchestrator.
- Konfigurieren Sie vRealize Orchestrator, um vSphere als Authentifizierungsanbieter zu verwenden.
- Stellen Sie sicher, dass vCloud Director mit dem Lookup Service desselben Platform Services Controller wie vCenter Single Sign-On registriert ist, den vRealize Orchestrator für die Authentifizierung verwendet.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Dienstverwaltung** aus.
Eine Liste der registrierten vRealize Orchestrator-Server wird angezeigt.
- 2 Klicken Sie zum Registrieren eines neuen vRealize Orchestrator-Servers auf die Schaltfläche .
Das Dialogfeld **vRealize Orchestrator registrieren** wird angezeigt.
- 3 Geben Sie die folgenden Werte ein.

Option	Beschreibung
Name	Name für die registrierte vRealize Orchestrator-Instanz.
Beschreibung	Eine Beschreibung für die registrierte vRealize Orchestrator-Serverinstanz.

Option	Beschreibung
Hostname	Der vollqualifizierte Domänenname und Serverport des vRealize Orchestrator-Servers. Der Standardwert für den HTTPS-Port lautet 8281. Hinweis vCloud Director stellt eine Verbindung mit der API-Schnittstelle von vRealize Orchestrator her.
Benutzername	Ein Benutzerkonto, das Mitglied der vRealize Orchestrator-Administratorengruppe ist.
Kennwort	Das Kennwort für das vRealize Orchestrator-Administratorkonto.
Vertrauensanker	Das SSL-Zertifikat des vRealize Orchestrator-Servers im PEM-Format. Klicken Sie auf das Symbol zum Hochladen (), um nach der Datei .pem zu suchen und sie auszuwählen.



- 4 Klicken Sie auf **OK**, um die Registrierung abzuschließen.

Der vRealize Orchestrator-Server wird mit vCloud Director registriert.

Erstellen einer Dienstkategorie

Sie können Dienste in Dienstkategorien einteilen.

Verfahren



- Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - Wählen Sie im linken Fensterbereich die Option **Dienstverwaltung** aus.
 - Navigieren Sie zur Registerkarte **Dienstkategorien**.
Eine Liste der vorhandenen Serverkategorien wird angezeigt.
- Zum Erstellen einer neuen Dienstkategorie klicken Sie auf die Schaltfläche .
Das Dialogfeld **Neue Dienstkategorie** wird angezeigt.
- Geben Sie die folgenden Werte ein.

Option	Beschreibung
Name	Name der Dienstkategorie.
Symbol	Importieren Sie das angezeigte Symbol für die Dienstkategorie.
Beschreibung	Kurzbeschreibung der Dienstkategorie.

Bearbeiten einer Dienstkategorie

Sie können vorhandene Dienstkategorien bearbeiten.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Dienstverwaltung** aus.
 - b Navigieren Sie zur Registerkarte **Dienstkategorien**.
Eine Liste der vorhandenen Serverkategorien wird angezeigt.
- 2 Verwenden Sie die Listenleiste () auf der linken Seite einer ausgewählten Dienstkategorie und klicken Sie auf **Bearbeiten**.
- 3 Bearbeiten Sie die folgenden Werte.

Option	Beschreibung
Name	Name der Dienstkategorie.
Symbol	Importieren Sie das angezeigte Symbol für die Dienstkategorie.
Beschreibung	Kurzbeschreibung der Dienstkategorie.


Importieren eines Diensts

Sie können Dienste aus der Workflow-Bibliothek einer vRealize Orchestrator-Instanz importieren, die bei vCloud Director registriert ist.

Voraussetzungen

- Registrieren Sie eine vRealize Orchestrator-Instanz. Weitere Informationen finden Sie unter [Registrieren einer vRealize Orchestrator-Instanz bei vCloud Director](#).
- Erstellen Sie eine Dienstkategorie. Weitere Informationen finden Sie unter [Erstellen einer Dienstkategorie](#).

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Dienstbibliothek** aus.
Verfügbare Dienste werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte gibt an, dass es sich bei dem Element um einen vRealize Orchestrator-Workflow handelt, und zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die der Workflow importiert wird.
- 2 Klicken Sie zum Importieren eines neuen Diensts auf die Schaltfläche **Importieren**.

3 Führen Sie die im Assistenten **Importieren** angezeigten Schritte durch.


Option	Beschreibung
In Zielbibliothek importieren	Wählen Sie die Dienstkategorie aus, in die der Dienst importiert werden soll.
Quelle auswählen	Wählen Sie die vRealize Orchestrator-Instanz aus, aus der Workflows importiert werden sollen.
Workflows auswählen	Erweitern Sie die hierarchische Strukturansicht, um mindestens einen zu importierenden Workflow auszuwählen.
Überprüfen	Überprüfen Sie die Details und klicken Sie auf Fertig , um den Importvorgang abzuschließen.

Die importierten Workflows werden in der Kartenansicht **Dienstbibliothek** angezeigt.

Auffinden eines Diensts

Sie können nach einem Dienst anhand seines Namens oder der Dienstkategorie suchen, zu der der Dienst gehört.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.

- a Wählen Sie im linken Fensterbereich die Option **Dienstbibliothek** aus.

Verfügbare Dienste werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte gibt an, dass es sich bei dem Element um einen vRealize Orchestrator-Workflow handelt, und zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die der Workflow importiert wird.

- 2 Geben Sie im Textfeld **Suchen** oben auf der Seite ein Wort oder ein Zeichen des Dienstnamens oder der Dienstkategorie ein, nach der Sie suchen.


- 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 vRealize Orchestrator-Workflows als importierte Dienste ausführen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.

- a Wählen Sie im linken Fensterbereich die Option **Dienstbibliothek** aus.

Verfügbare Dienste werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte gibt an, dass es sich bei dem Element um einen vRealize Orchestrator-Workflow handelt, und zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die der Workflow importiert wird.

- 2 Klicken Sie zum Ausführen eines Diensts auf der Karte des ausgewählten Diensts auf **Ausführen**.

Der Assistent **Dienst ausführen** wird angezeigt.

- 3 Geben Sie die erforderlichen Eingabeparameter des Diensts ein und klicken Sie auf **Beenden**.

Ergebnisse

Sie können in der Ansicht **Kürzlich bearbeitete Aufgaben** den Status der Ausführung überwachen. Weitere Informationen finden Sie unter [Anzeigen von Aufgaben](#).


Hinweis Wenn Sie einen vRealize Orchestrator-Workflow als vCloud Director-Dienst starten, fügt vCloud Director dem Ausführungskontext des Workflows einige benutzerdefinierte Parameter hinzu.

Benutzerdefinierte Eigenschaft	Beschreibung
_vcd_orgName	Name der Organisation, zu der der Benutzer gehört, der den Dienst ausführt.
_vcd_orgId	ID der Organisation, zu der der Benutzer gehört, der den Dienst ausführt.
_vcd_userName	Name des Benutzers, der den Dienst ausführt.
_vcd_isAdmin	Hat den Wert True, wenn der Benutzer, der den Dienst ausführt, ein Administrator ist.
_vdc_isAdmin	Veraltet. Hat den Wert True, wenn der Benutzer, der den Dienst ausführt, ein Administrator ist.
_vdc_userName	Veraltet. Name des Benutzers, der den Dienst ausführt.
_vcd_sessionToken	Authentifizierungstoken, das Sie nach erfolgreicher Authentifizierung bei vCloud Director erhalten haben
_vcd_apiEndpoint	vCloud Director-REST API-Endpoint

Ändern einer Dienstkategorie

Sie können die Kategorie ändern, der ein Dienst angehört.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Dienstbibliothek** aus.


Verfügbare Dienste werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte gibt an, dass es sich bei dem Element um einen vRealize Orchestrator-Workflow handelt, und zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die der Workflow importiert wird.

- 2 Wählen Sie in der Karte des ausgewählten Diensts **Verwalten > Kategorie ändern** aus.
Das Dialogfeld **Kategorie ändern** wird geöffnet.
- 3 Wählen Sie die Kategorie für den Dienst aus und klicken Sie auf **Speichern**.

Aufheben der Registrierung eines Diensts

Sie können den Zugriff auf einen Dienst für Dienstanbieter und Mandanten entfernen, indem Sie die Registrierung des Diensts aufheben.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Dienstbibliothek** aus.

Verfügbare Dienste werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte gibt an, dass es sich bei dem Element um einen vRealize Orchestrator-Workflow handelt, und zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die der Workflow importiert wird.
- 2 Wählen Sie in der Karte des ausgewählten Diensts **Verwalten > Registrierung des Workflows aufheben** aus.
Das Dialogfeld **Registrierung des Workflows aufheben** wird geöffnet.
- 3 Klicken Sie zum Entfernen des Diensts aus der Dienstbibliothek auf **Löschen**.

Veröffentlichen eines Diensts

Sie können den Zugriff von Dienstanbietern und Mandanten auf Dienste steuern, indem Sie einen Dienst veröffentlichen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Dienstbibliothek** aus.

Verfügbare Dienste werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte gibt an, dass es sich bei dem Element um einen vRealize Orchestrator-Workflow handelt, und zeigt den Namen des Diensts und ein Tag an, das der Dienstkategorie entspricht, in die der Workflow importiert wird.

- 2 Wählen Sie in der Karte des ausgewählten Diensts **Verwalten > Workflow veröffentlichen** aus.

Das Dialogfeld **Workflow veröffentlichen** wird angezeigt.

- 3 Zur Veröffentlichung für einen Dienstanbieter wählen Sie **Für Dienstanbieter veröffentlichen** aus und klicken Sie auf **Speichern**.

- 4 Zur Veröffentlichung für eine bestimmte Mandantenorganisation klicken Sie auf die Schaltfläche **Für Mandanten veröffentlichen**.

- a Eine Liste mit verfügbaren Mandantenorganisationen wird angezeigt. Wählen Sie die Mandantenorganisation aus, für die der Workflow veröffentlicht werden soll, und klicken Sie auf **Speichern**.

- 5 Zur Veröffentlichung für alle Mandantenorganisationen wählen Sie **Für alle Mandanten veröffentlichen** aus und klicken Sie auf **Speichern**.

Verwalten von benutzerdefinierten Entitäten

14

Bei den benutzerdefinierten Entitätsdefinitionen in vCloud Director handelt es sich um Objekttypen, die an vRealize Orchestrator-Objekttypen gebunden sind. Wenn ein Dienstanbieter eine benutzerdefinierte Entitätsdefinition für einen anderen Dienstanbieter oder einen oder mehrere Mandanten veröffentlicht, können vCloud Director-Benutzer diese Typen besitzen und entsprechend ihren Bedürfnissen verwalten und ändern. Durch Ausführen von Diensten können Dienstanbieterbenutzer und Organisationsbenutzer die benutzerdefinierten Entitäten instanziiieren und Aktionen auf die Instanzen der Objekte anwenden.


Dieses Kapitel enthält die folgenden Themen:

- [Auffinden einer benutzerdefinierten Entität](#)
- [Bearbeiten einer benutzerdefinierten Entitätsdefinition](#)
- [Hinzufügen einer benutzerdefinierten Entitätsdefinition](#)
- [Benutzerdefinierte Entitätsinstanzen](#)
- [Verknüpfen einer Aktion mit einer benutzerdefinierten Entität](#)
- [Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entität](#)
- [Veröffentlichen einer benutzerdefinierten Entität](#)
- [Löschen einer benutzerdefinierten Entität](#)

Auffinden einer benutzerdefinierten Entität

Sie können nach einer benutzerdefinierten Entität anhand ihres Namens suchen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.
- Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.


- 2 Geben Sie im Textfeld **Suchen** oben auf der Seite ein Wort oder ein Zeichen des Namens der Entität ein, nach der Sie suchen.

Die Suchergebnisse werden in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind.

Bearbeiten einer benutzerdefinierten Entitätsdefinition

Sie können den Namen und die Beschreibung einer benutzerdefinierten Entität ändern. Sie können den Typ der Entität oder den vRealize Orchestrator-Objektyp, an den die Entität gebunden ist, nicht ändern. Dies sind die Standardeigenschaften der benutzerdefinierten Entität. Wenn Sie beliebige Standardeigenschaften ändern möchten, müssen Sie die benutzerdefinierte Entitätsdefinition löschen und neu erstellen.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.
 - 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Bearbeiten** aus.
- Ein neues Dialogfeld wird geöffnet.
- 3 Ändern Sie den Namen oder die Beschreibung der benutzerdefinierten Entitätsdefinition.
 - 4 Klicken Sie auf **OK**, um die Änderung zu bestätigen.


Hinzufügen einer benutzerdefinierten Entitätsdefinition


Sie können eine benutzerdefinierte Entität erstellen und einem vorhandenen vRealize Orchestrator-Objektyp zuordnen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Klicken Sie auf das Symbol , um eine neue benutzerdefinierte Entität hinzuzufügen.
Ein neues Dialogfeld wird geöffnet.
- 3 Führen Sie die im Assistenten **Benutzerdefinierte Entitätsdefinition** angezeigten Schritte durch.

Schritt	
Name und Beschreibung	Geben Sie einen Namen und optional eine Beschreibung für die neue Entität ein. Geben Sie einen Namen für den Entitätstyp ein, z. B. sshHost.
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: SSH:Host.
Überprüfen	Überprüfen Sie die von Ihnen angegebenen Details und klicken Sie auf Fertig , um den Erstellvorgang abzuschließen.


Ergebnisse


Die neue benutzerdefinierte Entitätsdefinition wird in der Kartenansicht angezeigt.

Benutzerdefinierte Entitätsinstanzen

Wenn Sie einen vRealize Orchestrator-Workflow mit einem Eingabeparameter ausführen, der einen Objekttyp darstellt, der bereits als benutzerdefinierte Entitätsdefinition in vCloud Director definiert ist, wird der Ausgabeparameter als Instanz einer benutzerdefinierten Entität angezeigt.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.
Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.
- 2 Klicken Sie auf der Karte der ausgewählten benutzerdefinierten Entität auf **Instanzen**.
Die verfügbaren Instanzen werden in einer Rasteransicht angezeigt.


- 3 Klicken Sie auf die Listenleiste () auf der linken Seite jeder Entität, um die verknüpften Workflows anzuzeigen.

Durch Klicken auf einen Workflow wird eine Workflowausführung gestartet, die die Entitätsinstanz als Eingabeparameter verwendet.

Verknüpfen einer Aktion mit einer benutzerdefinierten Entität

Durch Verknüpfen einer Aktion mit einer benutzerdefinierten Entitätsdefinition können Sie mehrere vRealize Orchestrator-Workflows in den Instanzen einer bestimmten benutzerdefinierten Entität ausführen.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Aktion verknüpfen** aus.

Ein neues Dialogfeld wird geöffnet.

- 3 Führen Sie die im Assistenten **Benutzerdefinierte Entität mit VRO-Workflow verknüpfen** angezeigten Schritte durch.

Schritt	Details
VRO-Workflow auswählen	Wählen Sie einen der aufgelisteten Workflows aus. Hierbei handelt es sich um die Workflows, die auf der Seite Dienstbibliothek verfügbar sind.
Workflow-Eingabeparameter auswählen	Wählen Sie einen verfügbaren Eingabeparameter in der Liste aus. Sie verknüpfen den Typ des vRealize Orchestrator-Workflows mit dem Typ der benutzerdefinierten Entitätsdefinition.
Zuordnung überprüfen	Überprüfen Sie die von Ihnen angegebenen Details und klicken Sie auf Fertig , um die Zuordnung abzuschließen.


Beispiel

Wenn Sie beispielsweise über eine benutzerdefinierte Entität vom Typ SSH:Host verfügen, können Sie sie mit dem Workflow `Add a Root Folder to SSH Host` verknüpfen, indem Sie den `sshHost-`Eingabeparameter auswählen, der dem Typ der benutzerdefinierten Entität entspricht.

Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entität

Sie können einen vRealize Orchestrator-Workflow aus der Liste der verknüpften Aktionen entfernen.

Verfahren


- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.
 - 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Verknüpfung der Aktion aufheben** aus.
- Ein neues Dialogfeld wird geöffnet.
- 3 Wählen Sie den zu entfernenden Workflow aus und klicken Sie auf **Verknüpfung der Aktion aufheben**.
- Der vRealize Orchestrator-Workflow ist nicht mehr mit der benutzerdefinierten Entität verknüpft.

Veröffentlichen einer benutzerdefinierten Entität

Sie müssen eine benutzerdefinierte Entität veröffentlichen, damit Benutzer aus anderen Mandanten oder Diensteanbietern Workflows mithilfe der benutzerdefinierten Entitätsinstanzen als Eingabeparameter ausführen können.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.
 - 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Veröffentlichen** aus.
- Ein neues Dialogfeld wird geöffnet.


- 3 Geben Sie an, ob die benutzerdefinierte Entitätsdefinition für 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.

Verfahren

- 1 Wählen Sie im Hauptmenü () die Option **Inhaltsbibliotheken** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Benutzerdefinierte Entitätsdefinition** aus.

Die Liste der benutzerdefinierten Entitäten wird in einer Kartenansicht mit zwölf Elementen pro Seite angezeigt, die nach Namen in alphabetischer Reihenfolge sortiert sind. Jede Karte zeigt den Namen der benutzerdefinierten Entität, den vRealize Orchestrator-Typ, dem die Entität zugeordnet ist, den Typ der Entität und gegebenenfalls eine Beschreibung an.

- 2 Wählen Sie in der Karte der ausgewählten benutzerdefinierten Entität **Aktionen > Löschen** aus.
- 3 Bestätigen Sie den Löschvorgang.

Die benutzerdefinierte Entität wird aus der Kartenansicht entfernt.