

Handbuch für das VMware Cloud Director Service Provider Admin Portal

9. April 2020

VMware Cloud Director 10.1

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	Handbuch für das VMware Cloud Director™ Service Provider Admin Portal	9
2	Erste Schritte mit VMware Cloud Director Service Provider Admin Portal	10
	Überblick über die VMware Cloud Director-Verwaltung	10
	Anmelden bei VMware Cloud Director Service Provider Admin Portal	14
	Anzeigen von Aufgaben	15
	Beenden einer in Bearbeitung befindlichen Aufgabe	15
	Anzeigen von Ereignissen	16
	Festlegen der Benutzereinstellungen	16
	Längenbeschränkungen für Namen und Beschreibungen	17
3	Verwalten von vSphere-Ressourcen	19
	Hinzufügen von vCenter Server- und NSX-Ressourcen	20
	Anhängen einer vCenter Server-Instanz allein oder zusammen mit einer NSX Manager-Instanz	21
	Erkennen und Übernehmen von vApps	25
	Zuweisen des NSX-Lizenzschlüssels in vCenter Server	27
	Registrieren einer NSX-T Manager-Instanz	27
	Zugreifen auf vSphere-Komponenten über VMware Cloud Director-Proxys	28
	Hinzufügen eines Proxys für den Zugriff auf die zugrunde liegenden vCenter Server-Ressourcen	29
	Verwalten der Proxy-Zertifikate und CRLs	30
	Hinzufügen von Cloud-Ressourcen	31
	Provider-VDCs	31
	Erstellen eines virtuellen Provider-Datencenters	32
	Externe Netzwerke	35
	Netzwerkpools	38
	Anzeigen der vCenter Server-Instanzen	43
	Bearbeiten der vCenter Server-Einstellungen	44
	Aktivieren oder Deaktivieren einer vCenter Server-Instanz	45
	Erneutes Verbinden einer vCenter Server-Instanz	45
	Aktualisieren einer vCenter Server-Instanz	45
	Aktualisieren der Speicherrichtlinien einer vCenter Server-Instanz	46
	Aufheben der Registrierung einer vCenter Server-Instanz	46
	Bearbeiten der NSX Manager-Einstellungen	47
	Bearbeiten der NSX-T Manager-Einstellungen	48
	Löschen einer NSX-T Manager-Instanz	48
	Konfigurieren und Verwalten von Bereitstellungen mit mehreren Standorten	48

Ressourcenlisten für mehrere Standorte 51

4 Verwalten von virtuellen Provider-Datencentern 52

Aktivieren oder Deaktivieren eines virtuellen Provider-Datencenters 52

Löschen eines virtuellen Provider-Datencenters 53

Bearbeiten der allgemeinen Einstellungen eines virtuellen Provider-Datencenters 53

Zusammenführen von virtuellen Provider-Datencentern 54

Anzeigen der virtuellen Organisations-Datencenter eines virtuellen Provider-Datencenters 55

Anzeigen der Datenspeicher in einem virtuellen Provider-Datencenter 55

Anzeigen der externen Netzwerke in einem virtuellen Provider-Datencenter 56

Verwalten der VM-Speicherrichtlinien auf einem virtuellen Provider-Datencenter 57

Aktivieren der VM-Verschlüsselung für Speicherrichtlinien eines virtuellen Provider-Datencenters 57

Hinzufügen einer VM-Speicherrichtlinie zu einem virtuellen Provider-Datencenter 59

Aktivieren oder Deaktivieren einer VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter 59

Löschen einer VM-Speicherrichtlinie aus einem virtuellen Provider-Datencenter 60

Bearbeiten der Metadaten für eine VM-Speicherrichtlinie in einem virtuellen Provider-Datencenter 60

Aktivieren der Einstellung „E/A-Vorgänge pro Sekunde“ 61

Verwalten der Ressourcenpools in einem virtuellen Provider-Datencenter 62

Hinzufügen eines Ressourcenpools zu einem virtuellen Provider-Datencenter 62

Aktivieren oder Deaktivieren eines Ressourcenpools in einem virtuellen Provider-Datencenter 63

Trennen eines Ressourcenpools von einem virtuellen Provider-Datencenter 64

Bearbeiten der Metadaten für ein virtuelles Provider-Datencenter 64

5 Verwalten von Organisationen 66

Wissenswertes über Leases 66

Erstellen einer Organisation 67

Aktivieren oder Deaktivieren einer Organisation 67

Löschen einer Organisation 68

Konfigurieren von Katalogen für eine Organisation 68

Konfigurieren von Richtlinien für eine Organisation 69

Mandantenspeicher migrieren 71

6 Verwalten von virtuellen Organisations-Datencentern 73

Funktionsweise von Zuweisungsmodellen 73

Vorgeschlagene Verwendung der Zuweisungsmodelle 76

Flex-Zuweisungsmodell 77

Zuweisungspool-Zuweisungsmodell 79

Zuweisungsmodell Pay-As-You-Go 80

Reservierungspool-Zuweisungsmodell 81

Grundlegendes zu VM-Größen- und VM-Platzierungsrichtlinien	82
Attribute von VM-Größenrichtlinien	87
Erstellen einer VM-Platzierungsrichtlinie	89
Hinzufügen einer VM-Platzierungsrichtlinie zu einem Organisations-VDC	90
Löschen einer VM-Platzierungsrichtlinie	91
Erstellen einer VM-Größenrichtlinie	91
Hinzufügen einer VM-Größenrichtlinie zu einem Organisations-VDC	92
Bearbeiten einer VM-Größenrichtlinie	93
Löschen einer VM-Größenrichtlinie	93
Erstellen eines virtuellen Organisations-Datencenters	94
Aktivieren oder Deaktivieren eines virtuellen Organisations-Datencenters	97
Löschen eines virtuellen Organisations-Datencenters	98
Ändern des Namens und der Beschreibung eines virtuellen Organisations-Datencenters.	98
Ändern der Zuweisungsmodelleinstellungen eines virtuellen Organisations-Datencenters	99
Ändern der Speichereinstellungen eines virtuellen Organisations-Datencenters	99
Aktivieren der VM-Verschlüsselung für Speicherrichtlinien eines Organisations-VDC	99
Ändern der VM-Bereitstellungseinstellungen eines Organisations-VDC	100
Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC	101
Ändern der Standardspeicherrichtlinie für ein virtuelles Organisations-Datencenter	102
Bearbeiten des Grenzwerts einer Speicherrichtlinie für ein virtuelles Organisations-Datencenter	102
Ändern der Metadaten für eine VM-Speicherrichtlinie in einem virtuellen Organisations-Datencenter	103
Aktivieren oder Deaktivieren einer Speicherrichtlinie in einem virtuellen Organisations-Datencenter	103
Löschen einer Speicherrichtlinie aus einem virtuellen Organisations-Datencenter	104
Bearbeiten der Netzwerkeinstellungen eines Organisations-VDCs	105
Konfigurieren von VDC-übergreifenden Netzwerken	106
Ändern der Metadaten für ein virtuelles Organisations-Datencenter	107
Anzeigen der Ressourcenpools eines virtuellen Organisations-Datencenters	108
Verwalten der Distributed Firewall in einem virtuellen Organisations-Datencenter	108
Aktivieren der Distributed Firewall eines Organisations-VDCs	109
Hinzufügen einer Distributed Firewall-Regel	109
Bearbeiten einer Distributed Firewall-Regel	112
Benutzerdefiniertes Gruppieren von Objekten	113
Arbeiten mit Sicherheitsgruppen	117
Arbeiten mit Sicherheitstags	121

7 Verwalten von NSX Data Center for vSphere-Edge-Gateways 126

Arbeiten mit NSX Data Center for vSphere-Edge-Clustern	127
Hinzufügen eines NSX Data Center for vSphere-Edge-Gateways	129
Konfigurieren von NSX Data Center for vSphere-Edge-Gateway-Diensten	131

Verwalten einer NSX Data Center for vSphere-Edge-Gateway-Firewall	131
Verwalten von DHCP für NSX Data Center for vSphere-Edge-Gateways	136
Hinzufügen einer SNAT- oder DNAT-Regel	141
Konfiguration für erweitertes Routing	144
Lastausgleich	154
Sicherer Zugriff mit virtuellen privaten Netzwerken	169
SSL-Zertifikatsverwaltung	199
Benutzerdefiniertes Gruppieren von Objekten	206
Anzeigen der Netzwerknutzung und der IP-Zuweisungen auf einem Edge-Gateway	210
Bearbeiten der Edge-Gateway-Eigenschaften	210
Aktivieren oder Deaktivieren von Distributed Routing auf einem Edge-Gateway	211
Ändern der externen Netzwerke und der Edge-Gateway-Einstellungen	211
Bearbeiten der allgemeinen Einstellungen für ein Edge-Gateway	212
Bearbeiten des Standard-Gateways für ein Edge-Gateway	212
Bearbeiten der IP-Einstellungen für ein Edge-Gateway	213
Bearbeiten der unterzugewiesenen IP-Pools eines Edge-Gateways	213
Bearbeiten von Ratengrenzwerten für ein Edge-Gateway	214
Edge-Gateway erneut bereitstellen	214
Löschen eines Edge-Gateways	215
Statistiken und Protokolle für ein Edge-Gateway	215
Anzeigen von Statistiken	215
Protokollierung aktivieren	216
Aktivieren des SSH-Befehlszeilenzugriffs auf ein Edge-Gateway	218

8 Verwalten von NSX-T Data Center-Edge-Gateways 219

Dedizierte externe Netzwerke	219
Hinzufügen eines NSX-T Data Center-Edge-Gateways	220
Hinzufügen einer Firewallgruppe zu einem NSX-T-Edge-Gateway	221
Hinzufügen einer Firewallregel für NSX-T-Edge-Gateways	222
Hinzufügen einer SNAT- oder DNAT-Regel zu einem NSX-T-Edge-Gateway	223
Konfigurieren eines DNS-Weiterleitungsdiensts auf einem NSX-T-Edge-Gateway	226
Bearbeiten der IP-Zuweisungen für ein NSX-T-Edge-Gateway	226
Schnelle IP-Zuweisung	227
Erstellen von benutzerdefinierten Anwendungsportprofilen	228
Richtlinienbasiertes IPSec-VPN für NSX-T Data Center-Edge-Gateways	229
Konfigurieren des richtlinienbasierten NSX-T-IPSec-VPN	229
Anpassen des Sicherheitsprofils eines IPSec-VPN-Tunnels	230
Konfigurieren dedizierter externer Netzwerkdienste	232
Verwalten der Routenankündigung	232
Konfigurieren von allgemeinen BGP-Einstellungen	233
Erstellen einer IP-Präfixliste	235

Hinzufügen eines BGP-Nachbarn 236

9 Verwalten dedizierter vCenter Server-Instanzen 238

Aktivieren des Mandantenzugriffs eines angehängten vCenter Server 241

Veröffentlichen eines dedizierten vCenter Server 241

10 Verwalten von Systemadministratoren und Rollen 243

Verwalten von Rechten und Rollen 243

Vordefinierte Rollen und ihre Rechte 245

Rechte von Systemadministratoren 248

Rechte in vordefinierten globalen Mandantenrollen 256

Verwalten von Rechtepaketen 262

Verwalten von globalen Mandantenrollen 265

Verwalten von Anbieterrollen 269

Verwalten von Anbieterbenutzern und -gruppen 272

Verwalten von Anbieterbenutzern 272

Verwalten von Anbietergruppen 275

11 Verwalten der Systemeinstellungen 277

Bearbeiten der allgemeinen Systemeinstellungen 277

Allgemeine Systemeinstellungen 278

Konfigurieren der System-E-Mail-Einstellungen 280

Ändern der VMware Cloud Director-Lizenz 281

Konfigurieren der Einstellungen für die Katalogsynchronisierung 281

Konfigurieren und Überwachen von blockierenden Aufgaben und Benachrichtigungen 282

Konfigurieren eines AMQP Brokers 282

Konfigurieren der Einstellungen von blockierenden Aufgaben 283

Überwachen blockierter Aufgaben 284

Konfigurieren von öffentlichen Adressen 284

Verwalten von Identitätsanbietern 287

Verwalten von LDAP-Verbindungen 287

Konfigurieren Ihres Systems für die Verwendung eines SAML-Identitätsanbieters 291

Verwalten von Plug-Ins 293

Hochladen eines Plug-Ins 293

Aktivieren oder Deaktivieren eines Plug-Ins 294

Löschen eines Plug-Ins 294

Veröffentlichen oder Rückgängigmachen der Veröffentlichung eines Plug-Ins in einer Organisation 294

Anpassen der VMware Cloud Director-Portale 295

Konfigurieren der Kennwortrichtlinie 297

Konfigurieren von vSphere-Diensten 297

12 Überwachen von VMware Cloud Director 299

VMware Cloud Director und Kostenberichte 299

Anzeigen von Nutzungsinformationen für ein virtuelles Provider-Datencenter 300

13 Verwalten von Diensten 301

Integrieren von vRealize Orchestrator mit VMware Cloud Director 301

Registrieren einer vRealize Orchestrator-Instanz bei VMware Cloud Director 302

Erstellen einer Dienstkategorie 303

Bearbeiten einer Dienstkategorie 303

Importieren eines Diensts 304

Auffinden eines Diensts 305

Ausführen eines Diensts 305

Ändern einer Dienstkategorie 306

Aufheben der Registrierung eines Diensts 307

Veröffentlichen eines Diensts 307

14 Verwalten von benutzerdefinierten Entitäten 309

Auffinden einer benutzerdefinierten Entität 309

Bearbeiten einer benutzerdefinierten Entitätsdefinition 310

Hinzufügen einer benutzerdefinierten Entitätsdefinition 310

Benutzerdefinierte Entitätsinstanzen 311

Verknüpfen einer Aktion mit einer benutzerdefinierten Entität 312

Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten Entität 313

Veröffentlichen einer benutzerdefinierten Entität 313

Löschen einer benutzerdefinierten Entität 314

Handbuch für das VMware Cloud Director™ Service Provider Admin Portal

1

Das *VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal bereitgestellten Funktionen verwenden möchten.

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>.

Erste Schritte mit VMware Cloud Director Service Provider Admin Portal

2

Das VMware Cloud Director Service Provider Admin Portal ist eine dedizierte Schnittstelle für Dienstanbieteradministratoren.

Dieses Kapitel enthält die folgenden Themen:

- Überblick über die VMware Cloud Director-Verwaltung
- Anmelden bei VMware Cloud Director Service Provider Admin Portal
- Anzeigen von Aufgaben
- Beenden einer in Bearbeitung befindlichen Aufgabe
- Anzeigen von Ereignissen
- Festlegen der Benutzereinstellungen
- Längenbeschränkungen für Namen und Beschreibungen

Überblick über die VMware Cloud Director-Verwaltung

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

Das *VMware Cloud Director Service Provider Admin Portal-Handbuch* 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

VMware Cloud 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. VMware Cloud Director verwendet auch vSphere Distributed Switches, vSphere-Portgruppen und NSX Data Center for vSphere, um virtuelle Maschinennetzwerke zu unterstützen.

VMware Cloud 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 *VMware Cloud Director Service Provider Admin Portal-Handbuch* oder im *VMware Cloud Director API-Programmierhandbuch*.

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

Ab Version 9.7 kann VMware Cloud 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 VMware Cloud 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.

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

Dedizierte vCenter Server-Instanzen und -Proxys

Eine dedizierte vCenter Server-Instanz ist eine Cloud-Ressource, die eine vollständige vCenter Server-Installation kapselt. Eine dedizierte vCenter Server-Instanz enthält einen oder mehrere Proxys, die Zugriffspunkte auf verschiedene Komponenten der zugrunde liegenden vSphere-Umgebung sind. Der Anbieter kann dedizierte vCenter Server-Instanzen und -Proxys erstellen und aktivieren. Der Anbieter kann eine dedizierte vCenter Server-Instanz für Mandanten veröffentlichen.

Um dedizierte vCenter Server-Instanzen und -Proxys zu erstellen und zu verwalten, können Sie das Service Provider Admin Portal oder die vCloud-OpenAPI verwenden. Weitere Informationen finden Sie in [Kapitel 9 Verwalten dedizierter vCenter Server-Instanzen](#) und *Erste Schritte mit VMware Cloud Director OpenAPI* unter <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.

VMware Cloud Director-Netzwerk

VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.

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

Beginnend mit VMware Cloud Director 9.5 können **Systemadministratoren** isolierte virtuelle Datacenter-Netzwerke erstellen, die von einem logischen NSX-T-Switch unterstützt werden.

Organisationsadministratoren können isolierte virtuelle Datacenter-Netzwerke erstellen, die von Netzwerkpools unterstützt werden.

VMware Cloud Director 9.5 führt auch VDC-übergreifende Netzwerke ein, indem erweiterte Netzwerke in virtuellen Datacenter-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-Datacenter-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 VMware Cloud Director Mandantenportal*.

Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die in einem virtuellen Organisations-Datacenter zur Verfügung gestellt werden. Ein Netzwerkpool wird von vSphere-Netzwerkressourcen wie VLAN-IDs oder Portgruppen unterstützt. In VMware Cloud 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 VMware Cloud 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

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal

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

Voraussetzungen

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

Verfahren

- 1 Geben Sie die Service Provider Admin Portal-URL der VMware Cloud 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 Klicken Sie in der oberen Navigationsleiste auf **Überwachung** und **Ereignisse**.

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

- 2 Klicken Sie auf das Editor-Symbol (), um die Details zu ändern, die Sie zu den Ereignissen anzeigen möchten.
- 3 (Optional) Klicken Sie auf ein Ereignis, um die Ereignisdetails anzuzeigen.

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

Festlegen der Benutzereinstellungen

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

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

Verfahren

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

Längenbeschränkungen für Namen und Beschreibungen

Befolgen Sie diese Richtlinien, wenn Sie Werte in VMware Cloud Director eingeben.

Zeichenfolgenwerte für das Attribut `name` und die Elemente `Description` und `ComputerName` unterliegen Längenbeschränkungen, die von dem Objekt abhängig sind, mit dem sie verbunden sind.

Tabelle 2-1. Längenbeschränkungen für Objekteigenschaften

Objekt	Eigenschaft	Maximale Länge in Zeichen
Catalog	name	128
Catalog	Description	256
EdgeGateway	name	35
Media	name	128
Media	Description	256
VApp	name	128
VApp	Description	256
VAppTemplate	name	128
VAppTemplate	Description	256
Vdc	name	128

Tabelle 2-1. Längenbeschränkungen für Objekteigenschaften (Fortsetzung)

Objekt	Eigenschaft	Maximale Länge in Zeichen
Vdc	Description	256
Vm	name	128
Vm	ComputerName	15 unter Windows 63, auf allen anderen Plattformen
Vm	Description	256

Verwalten von vSphere-Ressourcen

3

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

VMware Cloud Director verwendet eine oder mehrere vCenter Server-Umgebungen, um die virtuellen Datencenter zu unterstützen. Ab Version 9.7 kann VMware Cloud 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 VMware Cloud Director mit ihren VMware Cloud Director-Konten zu verwenden.

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

Wenn Sie ein virtuelles Provider-Datencenter erstellen, das von einer angehängten vCenter Server-Instanz gestützt 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 [Erstellen eines virtuellen Provider-Datencenters](#).

Wenn Sie ein SDDC erstellen, das eine angehängte vCenter Server-Instanz kapselt, haben Sie den vCenter Server einem Mandanten zugewiesen. Diese vCenter Server-Instanz wird als für einen Mandanten veröffentlicht angezeigt, was auch als „mandantenzentriert“ bezeichnet wird. Informationen zum Erstellen eines SDDC finden Sie unter [Kapitel 9 Verwalten dedizierter vCenter Server-Instanzen](#).

Hinweis Standardmäßig können Sie mit einer angehängten vCenter Server-Instanz entweder ein Provider-VDC oder eine dedizierte vCenter Server-Instanz 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 einer dedizierten vCenter Server-Instanz verwenden, bzw. umgekehrt.

Zentralisierte SSL-Verwaltung

Ab Version 10.1 wird VMware Cloud Director zu einem zentralisierten, mandantenfähigen Speicherbereich für die Zertifikatsverwaltung. Auf diese Weise zentralisiert VMware Cloud Director alle Zertifikate an einem Ort, sodass **Systemadministratoren** und **Organisationsadministratoren** alle Zertifikate, die von verschiedenen Komponenten im System verwendet werden, anzeigen, überprüfen und verwalten können. Sie können die VMware Cloud Director-API zum Hinzufügen, Aktualisieren oder Entfernen von Zertifikaten aus dem neuen mandantenfähigen Speicherbereich verwenden. Weitere Informationen finden Sie im *VMware Cloud Director API-Schema-Referenz*.

Beim Hinzufügen oder Bearbeiten einer neuen vCenter Server-, NSX Manager- oder NSX-T Manager-Instanz prüft die VMware Cloud Director-Benutzeroberfläche diesen Endpoint auf bereitgestellte Zertifikate. VMware Cloud Director fügt alle Zertifikate, denen Sie vertrauen, einem zentralisierten Zertifikatspeicherbereich hinzu.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen von vCenter Server- und NSX-Ressourcen](#)
- [Zugreifen auf vSphere-Komponenten über VMware Cloud Director-Proxys](#)
- [Hinzufügen von Cloud-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](#)
- [Konfigurieren und Verwalten von Bereitstellungen mit mehreren Standorten](#)
- [Ressourcenlisten für mehrere Standorte](#)

Hinzufügen von vCenter Server- und NSX-Ressourcen

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

Informationen zu den Systemanforderungen von VMware Cloud 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 können eine vCenter Server-Instanz anhängen, sodass deren Ressourcen für die Verwendung in VMware Cloud Director verfügbar werden. Sie können eine vCenter Server-Instanz nur zusammen mit der zugehörigen NSX Manager-Instanz anhängen. Bei dedizierten vCenter Server-Instanzen oder Instanzen, die einer NSX-T Manager-Instanz zugeordnet sind, können Sie eine vCenter Server-Instanz allein anhängen.

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

Wenn VMware Cloud 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 VMware Cloud 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 VMware Cloud Director-Umgebung anhängen.

Sie können eine direkt zugängliche vCenter Server-Instanz oder eine vCenter Server-Instanz anhängen, die sich hinter einem Proxy befindet. Mithilfe von vCloud OpenAPI können Sie Proxy-Konfigurationen innerhalb von VMware Cloud Director verwenden, um eine Proxy-Verbindung zwischen einer VMware Cloud Director-Instanz und der ihr hinzugefügten vCenter Server-Instanz zu erstellen. Auf diese Weise können sich die VMware Cloud Director- und die vCenter Server-Instanz an unterschiedlichen Standorten oder Sites befinden.

Um eine vCenter Server-Instanz, die sich hinter einem Proxy befindet, anzuhängen, müssen Sie zunächst eine Proxy-Konfiguration deklarieren. Anschließend müssen Sie eine vCenter Server-Instanz anhängen und VMware Cloud Director so konfigurieren, dass beim Zugriff auf die vCenter Server-Instanz die Proxy-Konfiguration verwendet wird. Sie können auch eine NSX Data Center

for vSphere-Lösung über einen Proxy anhängen. VMware Cloud Director unterstützt keine Proxy-Konfigurationen für NSX-T Data Center. Sie benötigen keine zusätzlichen SSL-Konfigurationen oder eine zusätzliche Proxy-Konfiguration für den Platform Services Controller, bei dem die vCenter Server-Instanz registriert ist.

Voraussetzungen

- Wenn Sie VMware Cloud Director zum Überprüfen der vCenter- und vSphere-SSO-Zertifikate konfiguriert haben, stellen Sie sicher, dass die vCenter Server-Zertifikate auf VMware Cloud Director hochgeladen wurden. Informationen zu allgemeinen Systemeinstellungen finden Sie unter [Bearbeiten der allgemeinen Systemeinstellungen](#).
- Wenn Sie VMware Cloud Director zum Überprüfen von NSX Manager-Zertifikaten konfiguriert haben, stellen Sie sicher, dass die NSX Manager-Zertifikate auf VMware Cloud Director hochgeladen wurden. Informationen zu allgemeinen Systemeinstellungen finden Sie unter [Bearbeiten der allgemeinen Systemeinstellungen](#).

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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **vCenter Server-Instanzen** und dann auf **Hinzufügen**.
- 3 Wenn Sie über eine Multisite-VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Wenn der Endpoint nicht über ein vertrauenswürdiges Zertifikat verfügt, müssen Sie im Fenster **Vertrauenswürdigkeitszertifikat** bestätigen, dass Sie dem Endpoint vertrauen.

Wenn Sie in einer Multisite-Umgebung bei einer vCloud Director 10.0-Site angemeldet sind oder versuchen, eine vCenter Server-Instanz bei einer vCloud Director 10.0-Site zu registrieren, fügt VMware Cloud Director den Endpoint nicht dem zentralisierten Zertifikatspeicherbereich hinzu.
 - Um den Endpoint dem zentralisierten Zertifikatspeicherbereich hinzuzufügen und fortzufahren, klicken Sie auf **Vertrauenswürdigkeit**.
 - Wenn Sie diesem Endpoint nicht vertrauen, klicken Sie auf **Abbrechen** und wiederholen Sie [Schritt 5](#) bis [Schritt 9](#) mit einem vertrauenswürdigen Endpoint.
- 11 (Optional) Überspringen Sie das Hinzufügen der NSX Manager-Instanz, die der vCenter Server-Instanz zugeordnet ist, indem Sie die Umschaltoption **Einstellungen konfigurieren** deaktivieren, und klicken Sie auf **Weiter**.

Wenn VMware Cloud 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.

- 12 Wenn Sie einen für Mandanten dedizierten vCenter Server hinzufügen möchten, der nicht als Provider-VDC verwendet wird, aktivieren Sie die Option **Mandantenzugriff aktivieren**.

Nachdem Sie die vCenter Server-Instanz zu VMware Cloud Director hinzugefügt haben, werden die auf den Mandanten bezogenen Informationen in der Detailansicht der Instanz angezeigt.

- 13 Wenn Sie möchten, dass VMware Cloud Director Standard-Proxys für die vCenter Server-Instanz und die SSO-Dienste generiert, aktivieren Sie die Umschaltoption **Proxys generieren**.

Nachdem Sie die vCenter Server-Instanz zu VMware Cloud Director hinzugefügt haben, werden die Proxys auf der Registerkarte **Proxys** unter **vSphere-Ressourcen** angezeigt.

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

(Optional) Hinzufügen der verknüpften NSX Manager-Instanz

Wenn VMware Cloud 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** 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
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 VMware Cloud Director Mandantenportal</i> .
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 .

Option	Beschreibung
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 .

- 5 Klicken Sie auf **Weiter**.
- 6 Wenn der Endpoint nicht über ein vertrauenswürdiges Zertifikat verfügt, müssen Sie im Fenster **Vertrauenswürdigkeitszertifikat** bestätigen, dass Sie dem Endpoint vertrauen.

Wenn Sie in einer Multisite-Umgebung bei einer vCloud Director 10.0-Site angemeldet sind oder versuchen, eine NSX Manager-Instanz bei einer vCloud Director 10.0-Site zu registrieren, fügt VMware Cloud Director den Endpoint nicht dem zentralisierten Zertifikatspeicherbereich hinzu.
 - Um den Endpoint dem zentralisierten Zertifikatspeicherbereich hinzuzufügen und fortzufahren, klicken Sie auf **Vertrauenswürdigkeit**.
 - Wenn Sie diesem Endpoint nicht vertrauen, klicken Sie auf **Abbrechen** und wiederholen Sie [Schritt 2](#) bis [Schritt 4](#) mit einem vertrauenswürdigen Endpoint.
- 7 Aktivieren oder deaktivieren Sie die Einstellungen für die Zugriffskonfiguration.
- 8 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Registrierungsdaten und klicken Sie auf **Fertigstellen**.

Nächste Schritte

- [Zuweisen des NSX-Lizenzschlüssels in vCenter Server](#).
- [Erstellen eines virtuellen Provider-Datencenters](#).

Erkennen und Übernehmen von vApps

In der Standardkonfiguration erkennt ein Organisations-VDC VMs, die in einem vCenter Server-Ressourcenpool erstellt wurden, der dem VDC zugrunde liegt. Das System erstellt eine vereinfachte vApp, die dem Systemadministrator gehört und alle erkannten virtuellen Maschinen (VMs) enthält. Nachdem der Systemadministrator Ihnen die Berechtigung für den Zugriff auf eine erkannte vApp erteilt hat, können Sie auf die darin enthaltene VM verweisen, wenn Sie eine vApp zusammenstellen bzw. neu zusammenstellen, oder Sie können die vApp ändern, um sie zu übernehmen und zu importieren.

Erkannte vApps enthalten genau eine VM und unterliegen mehreren Einschränkungen, die nicht für in VMware Cloud Director erstellte vApps gelten. Unabhängig davon, ob Sie sie übernehmen oder nicht, können sie als VM-Quelle nützlich sein, die Sie beim Zusammenstellen oder Neuzusammenstellen einer vApp verwenden.

Jede erkannte vApp erhält einen Namen, der vom Namen der darin enthaltenen vCenter-VM abgeleitet ist, sowie ein Präfix, das von Ihrem Organisationsadministrator angegeben wird.

Wenn Sie zusätzliche vApps erkennen möchten, kann ein Systemadministrator mithilfe der VMware Cloud Director-API Organisations-VDCs erstellen, die angegebene Ressourcenpools eines Provider-VDC übernehmen. vCenter-VMs in diesen übernommenen Ressourcenpools werden im neuen VDC als erkannte vApps angezeigt und stehen für die Übernahme zur Verfügung.

Hinweis Virtuelle Maschinen mit IDE-Festplatten werden nur in ausgeschaltetem Zustand erkannt.

Wenn eine oder mehrere vCenter-VMs nicht von VMware Cloud Director erkannt werden, können Sie die möglichen Gründe mit der vCenter Server-VM-Erkennung untersuchen. Weitere Informationen finden Sie unter *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

Aktivieren der VM-Erkennung

Die VM-Erkennung ist standardmäßig aktiviert. Um die VM-Erkennung zu deaktivieren, muss ein Systemadministrator das Kontrollkästchen **VM-Erkennung aktiviert** auf der Registerkarte **Systemeinstellungen > Allgemein** deaktivieren. Ein Organisationsadministrator kann mithilfe der VMware Cloud Director-API die VM-Erkennung für einzelne VDCs oder für alle VDCs in einer Organisation deaktivieren.

Verwenden einer VM aus einer erkannten vApp

Nachdem der Systemadministrator Ihnen Zugriff auf eine erkannte vApp gewährt hat, können Sie deren VM genau wie eine VM in jeder anderen vApp oder vApp-Vorlage verwenden. Sie können sie auch angeben, wenn Sie eine neue vApp erstellen. Sie können auch eine erkannte vApp klonen oder ihren Namen, ihre Beschreibung oder die Lease-Einstellungen ändern, ohne dass dies den Annahmeprozess auslöst.

Übernehmen einer erkannten vApp

Sie können eine erkannte vApp übernehmen, indem Sie das zugehörige vApp-Netzwerk ändern oder dieser vApp eine VM hinzufügen. Nachdem Sie eine erkannte vApp übernommen haben, wird sie vom System importiert und so behandelt, als sei sie in VMware Cloud Director erstellt worden. Wenn eine übernommene vApp mit einer vCloud-API-Anforderung abgerufen wird, enthält sie ein Element mit dem Namen `autoNature`. Dieses Element weist den Wert `false` auf, wenn die erkannte vApp übernommen oder in VMware Cloud Director erstellt wurde. Eine übernommene vApp kann nicht auf eine erkannte vApp zurückgesetzt werden.

Wenn Sie die in einer erkannten vApp enthaltene VM löschen oder verschieben, wird auch die enthaltene vApp entfernt. Dieses Verhalten gilt nicht für übernommene vApps.

Eine vApp, die zum Enthalten einer erkannten vCenter-VM erstellt wurde, gleicht einer vApp, die erstellt wird, wenn Sie eine VM manuell als vApp importieren, ist aber derart vereinfacht, dass Sie sie möglicherweise ändern müssen, bevor Sie sie in Ihrem VDC bereitstellen können. Beispielsweise müssen Sie möglicherweise ihre Netzwerk- und Speichereigenschaften bearbeiten und sonstige Anpassungen an die spezifischen Anforderungen Ihrer Organisation vornehmen.

Hinweis Wenn eine virtuelle Maschine übernommen wird, werden die in vCenter Server konfigurierten Einstellungen für Reservierung, Limit und Anteile von VMs nicht beibehalten. Importierte virtuelle Maschinen erhalten ihre Einstellungen für die Ressourcenzuweisung aus dem virtuellen Organisations-Datencenter, in dem sie sich befinden.

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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director registrieren, damit VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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-VMware Cloud 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 VMware Cloud 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 *VMware Cloud Director API-Programmierhandbuch* unter <https://code.vmware.com>.

Zugreifen auf vSphere-Komponenten über VMware Cloud Director-Proxys

VMware Cloud Director kann als HTTP-Proxy-Server zwischen VMware Cloud Director-Benutzern und der zugrunde liegenden vSphere-Umgebung fungieren.

Ein von VMware Cloud Director bereitgestellter Proxy ist ein Zugriffspunkt auf eine Datencenter-Komponente, zum Beispiel eine vCenter Server-Instanz, ein ESXi-Host oder eine NSX Manager-Instanz. Benutzer können sich mithilfe ihrer VMware Cloud Director-Konten bei der Benutzeroberfläche oder der API der Komponenten mit Proxys anmelden. Durch die Aktivierung und Deaktivierung eines von VMware Cloud Director bereitgestellten Proxys können Sie den Mandantenzugriff über diesen Proxy zulassen und beenden.

Die von VMware Cloud Director bereitgestellten Proxys unterscheiden sich von den Proxy-Konfigurationen innerhalb von VMware Cloud Director. Im Gegensatz zu von VMware Cloud Director bereitgestellten Proxys, die auf einen Mandanten beschränkt sind, befinden sich Proxy-Konfigurationen innerhalb von VMware Cloud Director auf der Anbieterebene, und es gibt keine Mandantenfähigkeit.

Sie können einen Proxy erstellen, wenn Sie eine vCenter Server-Instanz an VMware Cloud Director anhängen. Sie können dies auch zu einem späteren Zeitpunkt tun. Wenn die vCenter Server-Instanz einen externen Platform Services Controller verwendet, erstellt VMware Cloud Director auch für den Platform Services Controller einen Proxy. Mit über- und untergeordneten Proxys

können Sie bestimmte Proxys aus den Mandanten ausblenden oder Sie können Gruppen von untergeordneten Proxys über ihre übergeordneten Proxys aktivieren und deaktivieren. Weitere Informationen über das Erstellen eines Proxys nach dem Hinzufügen einer vCenter Server-Instanz zu VMware Cloud Director finden Sie unter [Hinzufügen eines Proxys für den Zugriff auf die zugrunde liegenden vCenter Server-Ressourcen](#).

Sie können Proxys auf der Registerkarte **Proxys** unter **vSphere-Ressourcen** bearbeiten, aktivieren, deaktivieren und löschen.

Hinweis Wenn Sie einen Proxy einer vCenter Server-Instanz 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.

Informationen zum Anzeigen und Verwalten von Zertifikaten und Zertifikatswiderrufslisten (CRLs) finden Sie unter [Verwalten der Proxy-Zertifikate und CRLs](#).

Hinzufügen eines Proxys für den Zugriff auf die zugrunde liegenden vCenter Server-Ressourcen

Sie können von VMware Cloud Director bereitgestellte Proxys erstellen, die Administratoren und Mandanten für den Zugriff auf die zugrunde liegende vSphere-Umgebung verwenden können, wie etwa vCenter Server-Instanzen, die zu VMware Cloud Director hinzugefügt wurden.

Wenn Sie automatisch einen vCenter Server-Proxy mit abgerufenen Zertifikaten und einem Fingerabdruck generieren möchten, können Sie dies über das Raster **vCenter Server-Instanzen** oder die vCenter Server-Detailansicht tun. Wenn der vCenter Server über einen externen Platform Services Controller verfügt, erstellt diese Option auch einen Proxy für den SSO-Endpoint.

In diesem Verfahren wird beschrieben, wie Sie manuell einen Proxy für eine vCenter Server-Instanz erstellen oder einen Proxy für einen ESXi-Host, eine externe Platform Services Controller-Instanz oder eine NSX Manager-Instanz erstellen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 3 Wählen Sie eine vCenter Server-Instanz aus.
- 4 Klicken Sie auf der Seite mit detaillierten vCenter Server-Informationen auf die Registerkarte **Proxys** und dann auf **Neu**.
- 5 Geben Sie einen Namen für den Proxy ein.
- 6 Wählen Sie abhängig von der Komponente, für die VMware Cloud Director ein Proxy sein soll, den Typ des Proxys aus.

Sie können diese Einstellung nach der Erstellung des Proxys nicht bearbeiten.

Sie können nur einen vCenter Server-Proxy erstellen. Wenn bereits ein vCenter Server-Proxy vorhanden ist und Sie einen neuen Proxy erstellen möchten, enthält das Dropdown-Menü **Typ** keine vCenter Server-Option.

- Wenn Sie einen vCenter Server-Proxy erstellen möchten, wählen Sie **vCenter** im Dropdown-Menü **Typ** aus und fahren Sie mit [Schritt 10](#) fort.
- Wenn Sie einen Proxy für einen ESXi-Host, NSX Manager oder SSO erstellen möchten, treffen Sie Ihre Auswahl im Dropdown-Menü und fahren Sie mit [Schritt 7](#) fort.

- 7 Geben Sie einen Namen, einen Zielhost und die URL für die Benutzeroberfläche des neuen Proxys ein.

Der Zielhost ist der Hostname oder die IP-Adresse der Komponente, für die VMware Cloud Director ein Proxy sein soll. Die URL für die Benutzeroberfläche des neuen Proxys ist die URL, auf die die Benutzeroberfläche von VMware Cloud Director verweist, wenn der Mandant den Proxy öffnet.

- 8 Wenn Sie möchten, dass der Proxy für die Mandanten sichtbar ist, aktivieren Sie die Option **Für Mandanten sichtbar**.
- 9 (Optional) Klicken Sie auf **Übergeordneten Proxy auswählen** und wählen Sie einen Proxy aus der Liste aus.
- 10 Klicken Sie auf **Speichern**.

Nächste Schritte

[Verwalten der Proxy-Zertifikate und CRLs.](#)

Verwalten der Proxy-Zertifikate und CRLs

Sie können die Proxy-Zertifikate und Zertifikatswiderrufslisten (Certificate Revocation Lists, CRLs) anzeigen, herunterladen und hochladen.

Voraussetzungen

Vergewissern Sie sich, dass Sie über von VMware Cloud Director bereitgestellte Proxys für mindestens eine vCenter Server-Instanz verfügen. Weitere Informationen finden Sie im [Zugreifen auf vSphere-Komponenten über VMware Cloud Director-Proxys](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Proxys** und wählen Sie einen Proxy aus.
- 3 Klicken Sie auf **Zertifikat verwalten**.
- 4 Laden Sie das Zertifikat und die CRL hoch oder herunter.
- 5 Klicken Sie auf **Speichern**.

Hinzufügen von Cloud-Ressourcen

Cloud-Ressourcen stellen eine Abstraktion der zugrunde liegenden vSphere-Ressourcen dar, die die Computing- und Speicherressourcen für VMware Cloud Director-VMs und -vApps sowie den Zugriff auf Speicher und die Netzwerkkonnektivität bereitstellen.

Cloud-Ressourcen sind u. a. virtuelle Provider- und Organisations-Datencenter, externe Netzwerke, virtuelle Organisations-Datencenter-Netzwerke und Netzwerkpools. Bevor Sie Cloud-Ressourcen zu VMware Cloud Director hinzufügen können, müssen Sie vSphere-Ressourcen hinzufügen.

Weitere Informationen zu Organisations-VDCs finden Sie unter [Kapitel 6 Verwalten von virtuellen Organisations-Datencentern](#).

Informationen zu VDC-Organisationsnetzwerken finden Sie im Kapitel *Verwalten von VDC-Organisationsnetzwerken* im *Handbuch für das VMware Cloud Director Mandantenportal*.

VMware Cloud Director 9.7 führt das SDDC oder eine dedizierte vCenter Server-Instanz als Cloud-Ressource ein, in der eine vollständige vCenter Server-Installation gekapselt ist. Der Anbieter kann einen dedizierten vCenter Server erstellen und aktivieren, ihn für Mandanten veröffentlichen und Proxys für verschiedene Komponenten der zugrunde liegenden vSphere-Umgebung erstellen und aktivieren. Um dedizierte vCenter Server-Instanzen und -Proxys zu erstellen, zu verwalten und für Mandanten zu veröffentlichen, können Sie das Service Provider Admin Portal oder die vCloud-OpenAPI verwenden. Weitere Informationen finden Sie unter [Kapitel 9 Verwalten dedizierter vCenter Server-Instanzen](#) oder *Erste Schritte mit VMware Cloud Director OpenAPI* auf <https://code.vmware.com>.

Provider-VDCs

Ein virtuelles Provider-Datencenter (VDC) kombiniert die Computing- und Arbeitsspeicherressourcen eines vCenter Server-Ressourcenpools mit den Speicherressourcen einer oder mehrerer Speicherrichtlinien aus einer einzelnen vCenter Server-Instanz. Für Netzwerkressourcen kann ein Provider-VDC entweder NSX Data Center for vSphere oder NSX-T Data Center verwenden.

- Sie können ein Provider-VDC erstellen und verwalten, das von einer angehängten vCenter Server-Instanz und deren zugehöriger NSX Manager-Instanz gestützt wird, indem Sie das Service Provider Admin Portal oder die vCloud-API verwenden.
- Sie können ein Provider-VDC erstellen und verwalten, das von einer angehängten vCenter Server-Instanz und einer NSX-T Manager-Instanz gestützt wird, indem Sie das Service Provider Admin Portal oder die vCloud-API verwenden.

Ein typisches VMware Cloud Director-System enthält mehrere Provider-VDCs, die so konfiguriert sind, dass sie verschiedenste Service-Level-Anforderungen erfüllen. Jedes Provider-VDC verfügt über einen primären Ressourcenpool. Sie können nicht primäre Ressourcenpools zur zugrunde liegenden vCenter Server-Instanz hinzufügen und daraus entfernen. Der primäre Ressourcenpool kann nicht entfernt werden.

Erstellen eines virtuellen Provider-Datencenters

Um vSphere-Computing-, -Arbeitsspeicher- und -Speicherressourcen für VMware Cloud Director verfügbar zu machen, erstellen Sie ein virtuelles Provider-Datencenter (Provider-VDC).

Bevor eine Organisation mit der Bereitstellung von VMs oder der Erstellung von Katalogen beginnen kann, muss der **Systemadministrator** ein Provider-VDC und die Organisations-VDCs erstellen, die deren Ressourcen nutzen. Die Beziehung der Provider-VDCs zu den von ihnen unterstützten Organisations-VDCs ist eine administrative Entscheidung. Die Entscheidung kann auf dem Umfang Ihrer Dienstangebote, der Kapazität sowie der geografischen Verteilung Ihrer vSphere-Infrastruktur und ähnlichen Erwägungen basieren. Da die Mandanten zur Verfügung stehenden vSphere-Kapazitäten und -Dienste durch ein Provider-VDC einschränkt werden, erstellen **Systemadministratoren** in der Regel Provider-VDCs, die verschiedene, nach Leistung, Kapazität und Funktionsumfang gemessene Dienstklassen enthalten. Den Mandanten können dann Organisations-VDCs mit speziellen Dienstklassen bereitgestellt werden, die über die Konfiguration des zugrunde liegenden Provider-VDC definiert werden.

Denken Sie vor dem Erstellen eines Provider-VDC über die vSphere-Funktionen nach, die Sie Ihren Mandanten anbieten möchten. Einige dieser Funktionen können im primären Ressourcenpool des Provider-VDC implementiert werden. Andere erfordern möglicherweise, dass Sie zusätzliche Ressourcenpools basierend auf speziell konfigurierten vSphere-Clustern erstellen und diese dem VDC hinzufügen, wie in [Hinzufügen eines Ressourcenpools zu einem virtuellen Provider-Datencenter](#) beschrieben.

Der Bereich der ESXi-Versionen, die auf Hosts in dem einen Ressourcenpool stützenden Cluster installiert sind, bestimmt darüber, welche Gastbetriebssysteme und virtuellen Hardwareversionen bestimmten VMs zur Verfügung stehen. Diese VMs werden in Organisations-VDCs bereitgestellt, die durch das Provider-VDC gestützt werden.

Voraussetzungen

- Melden Sie sich bei der Service Provider Admin Portal als **Systemadministrator** an.
- Stellen Sie sicher, dass Sie den primären Zielressourcenpool mit verfügbarer Kapazität in einem Cluster erstellt haben, der für die Verwendung von automatisiertem DRS konfiguriert ist. Sie können einen Ressourcenpool nur für ein Provider-VDC verwenden. Um einen Ressourcenpool zu erstellen, können Sie den vSphere Client verwenden.

Wenn Sie beabsichtigen, einen Ressourcenpool zu verwenden, der Teil eines Clusters ist, welcher vSphere-Hochverfügbarkeit (High Availability, HA) verwendet, müssen Sie wissen, wie vSphere-HA die Slotgröße berechnet. Weitere Informationen zu Slotgrößen und zur Anpassung des HA-Verhaltens von vSphere erhalten Sie in der Dokumentation zur *vSphere-Verfügbarkeit*.

- Wenn Sie NSX Data Center for vSphere für die Netzwerkressourcen des Provider-VDC verwenden:
 - Stellen Sie sicher, dass die vCenter Server-Instanz, die den primären Zielressourcenpool enthält, angehängt ist und über einen NSX Data Center for vSphere-Lizenzschlüssel verfügt.
 - Richten Sie die VXLAN-Infrastruktur in NSX Manager ein. Weitere Informationen finden Sie im relevanten *Administratorhandbuch für NSX*.

Wenn Sie in diesem Provider-VDC einen benutzerdefinierten VXLAN-Netzwerkpool statt des Standard-VXLAN-Netzwerkpools verwenden möchten, erstellen Sie jetzt diesen Netzwerkpool. Weitere Informationen finden Sie im [Erstellen eines Netzwerkpools, der von einer NSX Data Center for vSphere-Transportzone gestützt wird](#).

- Wenn Sie NSX-T Data Center für die Netzwerkressourcen des Provider-VDC verwenden:
 - [Hinzufügen eines externen Netzwerks, das von einem logischen NSX-T Data Center-Tier-0-Router gestützt wird](#)
 - [Erstellen eines Netzwerkpools, der von einer NSX-T Data Center-Transportzone gestützt wird](#)

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus.
- 3 Klicken Sie auf **Neu**.
- 4 Wenn Sie über eine Multisite-VMware Cloud Director-Bereitstellung verfügen, wählen Sie im Dropdown-Menü **Site** die Site aus, der Sie diese Provider-VDC-Instanz hinzufügen möchten, und klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für das Provider-VDC ein.
 Sie können diese Textfelder verwenden, um die vSphere-Funktionen anzugeben, die den von diesem Provider-VDC gestützten Organisations-VDCs zur Verfügung stehen, z. B. **vSphere HA** oder **Speicherrichtlinien mit IOPS-Unterstützung**.
- 6 (Optional) Um das Provider-VDC bei der Erstellung zu deaktivieren, deaktivieren Sie die Umschaltoption **Zustand**.
 Sie können die Computing- und Speicherressourcen eines deaktivierten VDCs nicht für die Erstellung von Organisations-VDCs verwenden.
- 7 Klicken Sie auf **Weiter**.

- 8 Um Ressourcenpools für das Provider-VDC bereitzustellen, wählen Sie eine vCenter Server-Instanz aus und klicken Sie auf **Weiter**.

Auf dieser Seite werden vCenter Server-Instanzen aufgeführt, die bei VMware Cloud Director registriert sind. Klicken Sie auf eine vCenter Server-Instanz, um deren verfügbaren Ressourcenpools anzuzeigen.

- 9 Wählen Sie einen Ressourcenpool aus, der als primärer Ressourcenpool für dieses Provider-VDC dienen soll.

Sie können einen Ressourcenpool für ein Provider-VDC verwenden. Wenn Sie einen Ressourcenpool einem Provider-VDC hinzufügen, stehen dieser Ressourcenpool und seine übergeordnete Kette nicht mehr für die Auswahl für andere Provider-VDCs zur Verfügung.

- 10 Wählen Sie die höchste virtuelle Hardwareversion aus, die vom Provider-VDC unterstützt werden soll, und klicken Sie auf **Weiter**.

Das System bestimmt die höchste virtuelle Hardwareversion, die von allen Hosts im Cluster unterstützt wird, der dem Ressourcenpool zugrunde liegt, und stellt diese Version als Standardwert im Dropdown-Menü **Höchste unterstützte Hardwareversion** bereit. Sie können diesen Standardwert verwenden oder eine niedrigere Hardwareversion aus dem Menü auswählen. Die angegebene Version wird als höchste virtuelle Hardwareversion verwendet, die einer VM zur Verfügung steht, die in einem von diesem Provider-VDC gestützten Organisations-VDC bereitgestellt wird. Wenn Sie eine niedrigere virtuelle Hardwareversion auswählen, werden einige Gastbetriebssysteme möglicherweise nicht für die Verwendung durch diese virtuellen Maschinen unterstützt. Nachdem Sie das Provider-VDC mit der ausgewählten Hardwareversion erstellt haben, können Sie nur ein Upgrade der Version durchführen; ein Downgrade ist nicht möglich.

Hinweis Die verfügbare Hardwareversion für das Provider-VDC hängt von der höchsten verfügbaren Version des ESXi-Hosts im Zielcluster ab. Wenn die höchste unterstützte Hardwareversion des ESXi-Hosts nicht zur Auswahl verfügbar ist, überprüfen Sie im vSphere Client, ob die Standardkompatibilität für die Erstellung virtueller Maschinen auf dem Datacenter auf **Datacenter-Einstellung und Hostversion verwenden** festgelegt ist. Sie können auch die standardmäßige Kompatibilitätseinstellung auf die höchste Hardwareversion festlegen, die Sie für den Cluster benötigen.

Die höchste unterstützte Hardwareversion der virtuellen Maschine in VMware Cloud Director 10.1.0 ist Version 15. Hardwareversion 15 ist verfügbar, wenn Sie sie in der vCenter Server-Instanz auf der Ebene des Clusters oder des Datacenters aktivieren.

- 11 Wählen Sie eine oder mehrere Speicherrichtlinien für das Provider-VDC aus und klicken Sie auf **Weiter**.

Alle vSphere-Speicherrichtlinien, die von dem ausgewählten Ressourcenpool unterstützt werden, werden aufgeführt.

12 Konfigurieren Sie den Netzwerkpool für dieses Provider-VDC.

Jedes Provider-VDC muss über einen Netzwerkpool verfügen. Das System kann einen Netzwerkpool mit einem Standardbereich erstellen. Sie können aber auch ein benutzerdefiniertes VXLAN verwenden, das auf einem spezifischen NSX Data Center for vSphere- oder einem Geneve-Pool basiert, der wiederum auf einer NSX-T Data Center-Transportzone basiert.

Option	Beschreibung
Einen Standard-VXLAN-Netzwerkpool erstellen	Das System erstellt einen VXLAN-Pool für dieses Provider-VDC.
Einen VXLAN-Netzwerkpool aus der Liste auswählen	Sie wählen einen Netzwerkpool aus einer Liste aus, sodass Sie einen benutzerdefinierten VXLAN-Pool verwenden, der auf einer bestimmten NSX-Transportzone basiert.
NSX-T Manager- und Geneve-Netzwerkpool auswählen	Sie wählen einen Netzwerkpool aus einer Liste aus, sodass Sie einen benutzerdefinierten VXLAN-Pool verwenden, der von einer NSX-T Data Center-Transportzone gestützt wird.

13 Überprüfen Sie Ihre Auswahl und klicken Sie auf **Fertigstellen**, um das Provider-VDC zu erstellen.

Nächste Schritte

Sie können sekundäre Ressourcenpools hinzufügen, mit denen das Provider-VDC spezialisierte Funktionen wie Edge-Cluster, Affinitätsgruppen und Hosts mit speziellen Konfigurationen bereitstellen kann, die von einigen Organisationen möglicherweise benötigt werden. Weitere Informationen finden Sie im [Hinzufügen eines Ressourcenpools zu einem virtuellen Provider-Datencenter](#).

Externe Netzwerke

Ein externes VMware Cloud Director-Netzwerk stellt eine Uplink-Schnittstelle bereit, die Netzwerke und virtuelle Maschinen im System mit einem Netzwerk außerhalb des Systems verbindet, z. B. einem VPN, einem Unternehmensintranet oder dem öffentlichen Internet. Nur ein **Systemadministrator** kann ein externes Netzwerk erstellen.

Wenn Sie mehrere vCenter Server-Instanzen im System registriert haben, können Sie mehrere externe Netzwerke erstellen, die jeweils von einem vSphere-Netzwerk oder einen logischen Tier-0-Router gestützt werden.

VMware Cloud Director unterstützt externe IPv4- und IPv6-Netzwerke.

Hinweis Der Bereich der IP-Adressen, den Sie beim Erstellen des externen Netzwerks definieren, wird entweder einem Edge-Gateway oder den virtuellen Maschinen zugewiesen, die mit diesem Netzwerk verbunden sind. Aus diesem Grund dürfen die IP-Adressen nicht außerhalb von VMware Cloud Director verwendet werden.

Externe Netzwerke gestützt von vSphere-Netzwerken

Externe Netzwerke können entweder durch ein einzelnes vSphere-Netzwerk oder durch mehrere vSphere-Netzwerke gestützt werden.

- Externe Netzwerke gestützt von einer einzelnen vSphere-Instanz

Damit jedem Benutzer des externen Netzwerks ein Satz nicht überlappender IP-Adressen im vSphere-Netzwerk zur Verfügung steht, muss der **Systemadministrator** die IP-Bereiche im zugrunde liegenden VLAN manuell konfigurieren.

- Externe Netzwerke gestützt von mehreren vSphere-Netzwerken

Ein externes Netzwerk kann von mehreren vSphere-Netzwerken gestützt werden. Dieser Ansatz kann die Verwaltung der IP-Adressen in VMware Cloud Director vereinfachen. Sie können die Eigenschaften eines externen Netzwerks ändern, um dessen stützende Netzwerke zu ändern.

Dieser Netzwerktyp weist mehrere Einschränkungen auf.

- Dem Netzwerk kann maximal ein vSphere-Netzwerk auf jeder im System registrierten VMware Cloud Director-Instanz zugrunde liegen.
- Die Switches von zugrunde liegenden Netzwerken müssen alle denselben Typ aufweisen, entweder vSphere Distributed Switch oder Standard-Switch.

Externe Netzwerke, die von einem logischen Tier-0-Router gestützt werden

Ein externes Netzwerk kann durch einen logischen NSX-T Data Center Tier-0-Router gestützt werden.

Hinweis Externe Netzwerke, die von Tier-0-Gateways (VRF-lite) in NSX-T Data Center gestützt werden, werden nicht unterstützt. Weitere Informationen zu VRF (Virtual Routing and Forwarding)-Gateways finden Sie unter *NSX-T Data Center-Administratorhandbuch*.

Hinzufügen eines externen Netzwerks, das von vSphere-Ressourcen gestützt wird

Wenn Sie ein externes Netzwerk hinzufügen, können Sie vSphere-Netzwerkressourcen registrieren, die von VMware Cloud Director verwendet werden können. Sie können VDC-Organisationsnetzwerke erstellen, die eine Verbindung mit externen Netzwerken herstellen.

Sie können ein externes IPv4- oder IPv6-Netzwerk hinzufügen. Ein externes IPv6-Netzwerk unterstützt sowohl IPv4- als auch IPv6-Subnetze, und ein externes IPv4-Netzwerk unterstützt sowohl IPv4- als auch IPv6-Subnetze.

Voraussetzungen

Stellen Sie sicher, dass eine vSphere-Portgruppe mit oder ohne VLAN-Trunking zur Verfügung steht. Elastische Portgruppen mit statischer Port-Bindung gewährleisten eine optimale Leistung.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Externe Netzwerke** und dann auf **Neu**.
- 3 Wählen Sie **vSphere-Ressourcen** und dann den Portgruppentyp zum Stützen des Netzwerks aus und klicken Sie auf **Weiter**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für das neue externe Netzwerk ein.
- 5 Wählen Sie die Portgruppen zum Stützen des externen Netzwerks aus und klicken Sie auf **Weiter**.
- 6 Konfigurieren Sie mindestens ein Subnetz und klicken Sie auf **Weiter**.
 - a Klicken Sie auf **Hinzufügen**, um das Subnetz hinzuzufügen.
 - b 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**.
 - c (Optional) Geben Sie die DNS-Einstellungen ein.
 - d Konfigurieren Sie einen statischen IP-Pool, indem Sie mindestens einen IP-Bereich oder eine IP-Adresse hinzufügen.
 - e Klicken Sie auf **OK**.
 - f (Optional) Wiederholen Sie diesen Schritt, um ein weiteres Subnetz hinzuzufügen.
- 7 Überprüfen Sie die Netzwerkeinstellungen und klicken Sie auf **Fertigstellen**.

Nächste Schritte

Sie können ein VDC-Organisationsnetzwerk erstellen, das eine Verbindung mit einem externen Netzwerk herstellt.

Hinzufügen eines externen Netzwerks, das von einem logischen NSX-T Data Center-Tier-O-Router gestützt wird

Um NSX-T Data Center-Netzwerkressourcen zur Verwendung durch VMware Cloud Director zu registrieren, fügen Sie ein externes Netzwerk hinzu, das von einem logischen Tier-O-Router gestützt wird.

Verfahren

- 1 Erstellen Sie einen logischen Tier-O-Router.
 - Erstellen Sie den Tier-O-Router in NSX-T Manager.
 - a Melden Sie sich mit Administratorrechten bei der NSX-T Manager-Instanz an.
 - b Klicken Sie auf **Netzwerk**, dann auf **Tier-O-Gateways** und anschließend auf **Tier-O-Gateway hinzufügen**.

- c Geben Sie einen Namen für den Tier-O-Router ein.
- d Wählen Sie einen Hochverfügbarkeitsmodus aus.

Hinweis Standardmäßig wird der Aktiv/Aktiv-Modus verwendet. Im Aktiv/Aktiv-Modus wird auf den Datenverkehr für alle Mitglieder Lastausgleich angewendet. Im Aktiv/Standby-Modus wird der Datenverkehr von einem gewählten aktiven Mitglied verarbeitet. Wenn das aktive Mitglied ausfällt, wird ein neues Mitglied aktiv.

- e Wählen Sie einen vorhandenen NSX-T-Edge-Cluster aus dem Dropdown-Menü aus, um diesen logischen Tier-O-Router zu stützen, und klicken Sie auf **Speichern**.
 - Erstellen Sie den logischen Tier-O-Router mithilfe der NSX-Richtlinien-API.
- 2 Melden Sie sich beim VMware Cloud Director Service Provider Admin Portal an.
 - 3 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - 4 Klicken Sie im linken Bereich auf **Externe Netzwerke** und dann auf **Neu**.
 - 5 Wählen Sie **NSX-T-Ressourcen (Tier-O-Router)** und dann einen registrierten NSX-T Manager zur Stützung des Netzwerks aus. Klicken Sie anschließend auf **Weiter**.
 - 6 Geben Sie einen Namen und optional eine Beschreibung für das neue externe Netzwerk ein.
 - 7 Wählen Sie einen Tier-O-Router für die Verbindung mit dem externen Netzwerk aus und klicken Sie auf **Weiter**.
 - 8 Konfigurieren Sie mindestens ein Subnetz und klicken Sie auf **Weiter**.
 - a Klicken Sie auf **Hinzufügen**, um das Subnetz hinzuzufügen.
 - b Geben Sie die CIDR-Einstellungen (Classless Inter-Domain Routing) für das Netzwerk ein.
 - c (Optional) Geben Sie die DNS-Einstellungen ein.
 - d Konfigurieren Sie einen statischen IP-Pool, indem Sie mindestens einen IP-Bereich oder eine IP-Adresse hinzufügen.
 - e Klicken Sie auf **OK**.
 - f (Optional) Um ein weiteres Subnetz hinzuzufügen, wiederholen Sie die Schritte [8.a](#) bis [8.e](#).
 - 9 Überprüfen Sie die Netzwerkeinstellungen und klicken Sie auf **Fertigstellen**.

Nächste Schritte

Verwenden Sie den Tier-O-Router, um einen Uplink zum externen Netzwerk zu erstellen.

Netzwerkpools

Bei einem Netzwerkpool handelt es sich um eine Gruppe undifferenzierter Netzwerke, die in einem Organisations-VDC für die Erstellung von vApp-Netzwerken und bestimmten Typen von VDC-Organisationsnetzwerken zur Verfügung gestellt werden.

Ein Netzwerkpool wird von vSphere-Netzwerkressourcen wie VLAN-IDs oder Portgruppen, von NSX Data Center for vSphere-Ressourcen oder von NSX-T Data Center-Ressourcen gestützt.

In VMware Cloud Director werden anhand von Netzwerkpools NAT-geroutete und interne VDC-Organisationsnetzwerke sowie alle vApp-Netzwerke erstellt. Der Netzwerk-Datenverkehr in den einzelnen Netzwerken eines Pools wird auf Layer 2 von allen anderen Netzwerken isoliert.

Jedes Organisations-VDC in VMware Cloud Director kann über einen Netzwerkpool verfügen. 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.

VXLAN-Netzwerkpools

Jedes Provider-VDC, das von NSX Data Center for vSphere gestützt wird, enthält einen VXLAN-Netzwerkpool.

Wenn Sie ein Provider-VDC erstellen, das von NSX Data Center for vSphere gestützt wird, können Sie dieses Provider-VDC einem vorhandenen VXLAN-Netzwerkpool zuordnen oder einen VXLAN-Netzwerkpool für das Provider-VDC erstellen.

Der Name eines neu erstellten VXLAN-Netzwerkpools leitet sich vom Namen des enthaltenen Provider-VDC ab und wird bei der Erstellung des Pools zugewiesen. Sie können diesen Netzwerkpool nicht löschen oder ändern. Wenn Sie ein Provider-VDC umbenennen, wird dessen VXLAN-Netzwerkpool ebenfalls automatisch umbenannt.

Hinweis Um eine optimale Netzwerkleistung in Ihrer Infrastruktur zu gewährleisten, erstellen Sie einen VXLAN-Netzwerkpool und verknüpfen Sie ihn bei der Erstellung mit allen Provider-VDCs.

VMware Cloud Director-VXLAN-Netzwerke basieren auf dem VXLAN-Standard der IETF (Internet Engineering Task Force) und bieten mehrere Vorteile:

- Logische Netzwerke über Layer-3-Grenzen hinweg
- Logische Netzwerke, die sich auf einem einzelnen Layer 2 über mehrere Racks erstrecken
- Broadcast Containment
- Höhere Systemleistung
- Größere Skala (bis zu 16 Millionen Netzwerkadressen)

Weitere Informationen zu VXLAN-Netzwerken in einer VMware Cloud Director-Umgebung finden Sie im *Administratorhandbuch für NSX*.

Erstellen eines Netzwerkpools, der von einer NSX Data Center for vSphere-Transportzone gestützt wird

Um eine NSX Data Center for vSphere-Transportzone zur Verwendung durch VMware Cloud Director zu registrieren, fügen Sie einen VXLAN-gestützten Netzwerkpool hinzu.

Voraussetzungen

Erstellen Sie eine NSX Data Center for vSphere-Transportzone auf jedem vCenter Server, der bei VMware Cloud Director registriert ist. Weitere Informationen finden Sie im *Administratorhandbuch für NSX*.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Netzwerkpools** aus und klicken Sie dann auf **Neu**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für den neuen Netzwerkpool ein und klicken Sie auf **Weiter**.
- 4 Wählen Sie **VXLAN-gestützt** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie eine vCenter Server-Instanz aus, um die VXLAN-Transportzone anzugeben, die von diesem Netzwerkpool verwendet werden soll, und klicken Sie auf **Weiter**.
- 6 Wählen Sie eine NSX Data Center for vSphere-Transportzone zur Stützung des neuen Netzwerkpools aus und klicken Sie auf **Weiter**.

Hinweis Um einen allgemeinen Netzwerkpool für ein VDC-übergreifendes Netzwerk zu erstellen, wählen Sie eine Transportzone des Typs **UNIVERSAL_VXLAN** aus.

- 7 Überprüfen Sie die Einstellungen für den Netzwerkpool und klicken Sie auf **Fertigstellen**.

Nächste Schritte

Erstellen Sie ein VDC-Organisationsnetzwerk, das vom Netzwerkpool gestützt wird, oder verknüpfen Sie den Netzwerkpool mit einem Organisations-VDC und erstellen Sie vApp-Netzwerke.

Geneve-Netzwerkpools

Jedes Provider-VDC, das von NSX-T Data Center gestützt wird, enthält einen Geneve-Netzwerkpool.

Geneve ist der Netzwerkvirtualisierungsstandard, der die Overlay-Funktion in NSX-T Data Center bereitstellt.

Wenn Sie ein Provider-VDC erstellen, das von NSX-T Data Center gestützt wird, können Sie dieses Provider-VDC einem vorhandenen Geneve-Netzwerkpool zuordnen oder einen Geneve-Netzwerkpool für das Provider-VDC erstellen.

VMware Cloud Director-Geneve-Netzwerke bieten zahlreiche Vorteile.

- Logische Netzwerke über Layer-3-Grenzen hinweg
- Logische Netzwerke, die sich auf einem einzelnen Layer 2 über mehrere Racks erstrecken
- Broadcast Containment
- Höhere Systemleistung

- Größere Skala (bis zu 16 Millionen Netzwerkadressen)

Erstellen eines Netzwerkpools, der von einer NSX-T Data Center-Transportzone gestützt wird

Um eine NSX-T Data Center-Transportzone zur Verwendung durch VMware Cloud Director zu registrieren, erstellen Sie einen Geneve-gestützten Netzwerkpool.

Voraussetzungen

Erstellen Sie eine Overlay-gestützte NSX-T Data Center-Transportzone. Weitere Informationen zur Erstellung von Transportzonen und zur generischen Netzwerkvirtualisierungskapselung, die als Geneve-Overlay (Generic Network Virtualization Encapsulation) bezeichnet wird, finden Sie in der *Produktdokumentation zu NSX-T Data Center*.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Netzwerkpools** aus und klicken Sie dann auf **Neu**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für den neuen Netzwerkpool ein und klicken Sie auf **Weiter**.
- 4 Wählen Sie **Geneve-gestützt** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie eine NSX-T Manager-Instanz aus, um die Transportzone für diesen Netzwerkpool bereitzustellen, und klicken Sie auf **Weiter**.
- 6 Wählen Sie eine NSX-T-Transportzone aus und klicken Sie auf **Weiter**.
- 7 Überprüfen Sie die Einstellungen für den Netzwerkpool und klicken Sie auf **Fertigstellen**.

Nächste Schritte

Erstellen Sie ein VDC-Organisationsnetzwerk, das vom Netzwerkpool gestützt wird, oder verknüpfen Sie den Netzwerkpool mit einem Organisations-VDC und erstellen Sie vApp-Netzwerke.

Erstellen eines Netzwerkpools, der durch VLAN-IDs gestützt wird

Um vSphere-VLAN-IDs zur Verwendung durch VMware Cloud Director zu registrieren, fügen Sie einen VLAN-gestützten Netzwerkpool hinzu. Ein VLAN-gestützter Netzwerkpool bietet Sicherheit, Skalierbarkeit und Leistung für VDC-Organisationsnetzwerke.

Voraussetzungen

Stellen Sie sicher, dass eine Reihe von VLAN-IDs und ein vSphere Distributed Switch in vSphere zur Verfügung stehen. Bei den VLAN-IDs muss es sich um gültige IDs handeln, die in dem physischen Switch, an den die ESXi-Server angeschlossen sind, konfiguriert sind.

Vorsicht Die VLANs müssen auf der Ebene von Layer 2 isoliert sein. Wenn die VLANs nicht ordnungsgemäß isoliert sind, kann die Netzwerkkonnektivität beeinträchtigt bzw. unterbrochen werden.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Netzwerkpools** aus und klicken Sie dann auf **Neu**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für den neuen Netzwerkpool ein und klicken Sie auf **Weiter**.
- 4 Wählen Sie die Option **VLAN-basiert** und klicken Sie dann auf **Weiter**.
- 5 Wählen Sie eine vCenter Server-Instanz aus, um den Distributed Virtual Switch anzugeben, der von diesem Netzwerkpool verwendet werden soll, und klicken Sie auf **Weiter**.
- 6 Geben Sie einen VLAN-ID-Bereich ein und klicken Sie auf **Weiter**.
- 7 Wählen Sie einen Distributed Switch für den Netzwerkpool aus und klicken Sie auf **Weiter**.
- 8 Überprüfen Sie die Einstellungen für den Netzwerkpool und klicken Sie auf **Fertigstellen**.

Nächste Schritte

Erstellen Sie ein VDC-Organisationsnetzwerk, das vom Netzwerkpool gestützt wird, oder verknüpfen Sie den Netzwerkpool mit einem Organisations-VDC und erstellen Sie vApp-Netzwerke.

Erstellen eines Netzwerkpools, der durch vSphere-Portgruppen gestützt wird

Um vSphere-Portgruppen zur Verwendung durch VMware Cloud Director zu registrieren, fügen Sie einen von Portgruppen gestützten Netzwerkpool hinzu. Im Gegensatz zu anderen Typen von Netzwerkpools erfordert ein von einer Portgruppe gestützter Netzwerkpool keinen vSphere Distributed Switch und kann Portgruppen unterstützen, die Distributed Switches von Drittanbietern zugeordnet sind.

Vorsicht Die Portgruppen müssen von allen anderen Portgruppen auf Layer 2 isoliert sein. Die Portgruppen müssen physisch oder unter Verwendung von VLAN-Tags isoliert sein. Wenn die Portgruppen nicht ordnungsgemäß isoliert sind, kann die Netzwerkkonnektivität unterbrochen werden.

Voraussetzungen

Stellen Sie sicher, dass in der vSphere-Umgebung eine oder mehrere Portgruppen zur Verfügung stehen. Die Portgruppen müssen auf allen ESXi-Hosts im Cluster verfügbar sein, und jede Portgruppe darf nur ein einziges VLAN verwenden. Portgruppen mit oder ohne VLAN-Trunking werden unterstützt.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Netzwerkpools** aus und klicken Sie dann auf **Neu**.
- 3 Geben Sie einen Namen und optional eine Beschreibung für den neuen Netzwerkpool ein und klicken Sie auf **Weiter**.

- 4 Wählen Sie **Portgruppen-gestützt** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie eine vCenter Server-Instanz aus, um Portgruppen bereitzustellen, die von diesem Netzwerkpool verwendet werden sollen, und klicken Sie auf **Weiter**.
- 6 Wählen Sie eine oder mehrere Portgruppen aus und klicken Sie auf **Weiter**.
Sie können für jede Portgruppe ein Netzwerk erstellen.
- 7 Überprüfen Sie die Einstellungen für den Netzwerkpool und klicken Sie auf **Fertigstellen**.

Nächste Schritte

Erstellen Sie ein VDC-Organisationsnetzwerk, das vom Netzwerkpool gestützt wird, oder verknüpfen Sie den Netzwerkpool mit einem Organisations-VDC und erstellen Sie vApp-Netzwerke.

Anzeigen der vCenter Server-Instanzen

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

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.

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 VMware Cloud Director.
Status	Der Status des vCenter Server kann „Normal“, „Warnung“ und „Kritisch“ lauten.
Zustand	Aktiviert oder deaktiviert. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren einer vCenter Server-Instanz .
Verbindung	Mit VMware Cloud 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.

	Beschreibung
Nutzung	Für dedizierte vCenter Server-Instanzen ist Mandantenzugriff aktiviert. Der Anbieter kann verschiedene Ressourcenpools einer freigegebenen vCenter Server-Instanz über mehrere Provider-VDCs hinweg verwenden und diese Ressourcenpools dann verschiedenen Mandanten zuteilen. Weitere Informationen finden Sie im Kapitel 9 Verwalten dedizierter vCenter Server-Instanzen .
Clusterzustand	Zusammenfassung der Systemzustände aller Cluster in der vCenter Server-Instanz. Beim Zusammenfassen der Systemzustände aller Cluster wird der Cluster mit dem schlechtesten Zustand angezeigt.
Cluster	Anzahl der Cluster in der vCenter Server-Instanz.
VMs	Anzahl der VMs in der vCenter Server-Instanz.
Ausgeführte VMs	Anzahl der ausgeführten VMs in der vCenter Server-Instanz.
CPU	Menge der aktiv genutzten virtuellen CPU als Prozentsatz der insgesamt verfügbaren vCenter Server-CPU.
Arbeitsspeicher	Menge des aktiv genutzten virtuellen Arbeitsspeichers als Prozentsatz des insgesamt verfügbaren vCenter Server-Arbeitsspeichers.
Speicher	Menge des aktiv genutzten virtuellen Speichers als Prozentsatz des insgesamt verfügbaren vCenter Server-Speichers.

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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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 Datencenter in VMware Cloud Director bereitzustellen, müssen Sie die vCenter Server-Instanz aktivieren.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 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 in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 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 VMware Cloud Director-Datenbank die Informationen über die zugrunde liegenden vCenter Server-Ressourcen zu aktualisieren, müssen Sie die vCenter Server-Instanz aktualisieren.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.

- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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 Ändern Sie den Hostnamen und die Administratoranmeldedaten von NSX Manager und klicken Sie auf **Speichern**.
- 5 (Optional) Um VDC-übergreifende Netzwerke für die von dieser vCenter Server-Instanz gestützten virtuellen Datencenter zu ermöglichen, aktivieren Sie die Umschaltoption und geben Sie die Steuerungs-VM-Eigenschaften und einen Namen für den Netzwerkanbieter-Bereich ein.

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

Parameter	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 VMware Cloud Director Mandantenportal</i> .

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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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**.

Konfigurieren und Verwalten von Bereitstellungen mit mehreren Standorten

Mithilfe der Multisite-Funktion von VMware Cloud Director kann ein Dienstanbieter oder Mandant mehrerer geografisch verteilter VMware Cloud Director-Installationen (Servergruppen) diese Installationen und die zugehörigen Organisationen als einzelne Elemente verwalten und überwachen.

Wenn Sie zwei VMware Cloud Director-Standorte verknüpfen, können diese Standorte als Einzelentität verwaltet werden. Weiterhin ermöglichen Sie Organisationen an diesen Standorten, Verknüpfungen untereinander zu erstellen. Wenn eine Organisation Mitglied einer Verknüpfung ist, können Benutzer der Organisation das VMware Cloud Director Tenant Portal für den Zugriff auf Organisations-Assets an jedem Mitgliedsstandort verwenden, obwohl jede Mitgliedsorganisation und dazugehörige Assets lokal zum jeweiligen Standort gehören.

Hinweis Sie müssen die VMware Cloud Director-API zum Zuweisen von Standorten verwenden. Die Sites müssen dieselbe VMware Cloud Director-API-Version aufweisen oder um eine Version auseinanderliegen. Beispiel: Sie können einen Standort mit VMware Cloud Director 10.0 (API-Version 33.0) einem Standort mit VMware Cloud Director der Version 9.7, 10.0 oder 10.1 und den jeweiligen API-Versionen 32.0, 33.0 oder 34.0 zuweisen.

Nachdem Sie zwei Standorte verknüpft haben, können Sie mit der VMware Cloud Director-API oder dem VMware Cloud Director Tenant Portal Organisationen zuweisen, welche jene Standorte in Anspruch nehmen. Weitere Informationen finden Sie im *VMware Cloud Director API-Programmierhandbuch* und im *Handbuch für das VMware Cloud Director Mandantenportal*.

Ein Standort oder eine Organisation kann eine unbegrenzte Anzahl an Verknüpfungen mit einem gleichgeordneten Standort oder einer gleichgeordneten Organisation aufweisen, wobei jedoch jede Verknüpfung aus genau zwei Mitgliedern besteht. Jeder Standort oder jede Organisation muss über einen eigenen privaten Schlüssel verfügen. Mitglieder von Verknüpfungen können eine vertrauenswürdige Beziehung durch den Austausch von öffentlichen Schlüsseln einrichten. Diese werden verwendet, um signierte Anforderungen von einem Mitglied an ein anderes zu überprüfen.

Jeder Standort in einer Verknüpfung wird durch den Umfang einer Servergruppe VMware Cloud Director (eine Gruppe von Servern, die eine VMware Cloud Director -Datenbank gemeinsam nutzen) definiert. Jede Organisation in einer Verknüpfung belegt einen einzelnen Standort. Der Administrator der Organisation steuert den Zugriff von Benutzern und Gruppen der Organisation auf Assets an jedem Mitgliedsstandort.

Standortobjekte und Standortverknüpfungen

Bei der Installation oder Aktualisierung wird ein `site`-Objekt erstellt, das die lokale VMware Cloud Director-Servergruppe darstellt. Ein Systemadministrator mit Berechtigungen für mehrere VMware Cloud Director-Servergruppen kann diese als eine Verknüpfung von VMware Cloud Director-Standorten konfigurieren.

Verknüpfungen von Organisationen

Nach Abschluss der Standortverknüpfung können Organisationsadministratoren an jedem Mitgliedsstandort mit der Verknüpfung ihrer Organisationen beginnen.

Hinweis Sie können eine `system`-Organisation keiner Mandantenorganisation zuordnen. Die `system`-Organisation an jedem beliebigen Standort kann nur mit der `system`-Organisation an einem anderen Standort verknüpft werden.

Benutzer- und Gruppenidentitäten

Verknüpfungen von Standorten und Organisationen müssen denselben Identitätsanbieter verwenden. Benutzer- und Gruppenidentitäten für alle Organisationen in der Verknüpfung müssen über diesen Identitätsanbieter verwaltet werden.

Mit Ausnahme der Systemorganisation, die den integrierten VMware Cloud Director-Identitätsanbieter verwenden muss, können die Verknüpfungen den für sie am besten geeigneten Identitätsanbieter auswählen. .

Steuerung des Standortzugriffs für Organisationsbenutzer und -gruppen

Organisationsadministratoren können ihren Identitätsanbieter zur Erstellung von Benutzer- oder Gruppenzugriffstoken konfigurieren, die an allen oder nur an bestimmten Mitgliedsstandorten gültig sind. Während die Benutzer- und Gruppenidentitäten in allen Mitgliedsorganisationen identisch sein müssen, sind Benutzer- und Gruppenrechte durch die Rollen beschränkt, denen jene Benutzer und Gruppen in jeder Mitgliedsorganisation zugewiesen sind. Die Zuweisung einer Rolle zu einem Benutzer oder zu einer Gruppe erfolgt für eine Organisation lokal, wie auch jegliche benutzerdefinierten Rollen, die Sie erstellen.

Anforderungen an den Lastausgleichsdienst

Für eine effektive Implementierung einer Bereitstellung mit mehreren Standorten müssen Sie einen Lastausgleichsdienst konfigurieren, der an einem institutionellen Endpunkt (z. B. `https://vcloud.example.com`) eingehende Anfragen an die Endpunkte für jedes Mitglied der Standortverknüpfung (z. B. `https://us.vcloud.example.com` und `https://uk.vcloud.example.com`) verteilt. Wenn eine Site mehrere Zellen aufweist, müssen Sie einen Lastausgleichsdienst konfigurieren, der eingehende Anforderungen an alle zugehörigen Zellen verteilt, damit eine Anforderung an `https://us.vcloud.example.com` von `https://cell1.us.vcloud.example.com`, `https://cell2.us.vcloud.example.com` usw. verarbeitet werden kann.

Status der Mitglieder der Verknüpfung

Nachdem Sie eine Verknüpfung von Standorten oder Organisationen erstellt haben, ruft das lokale System in regelmäßigen Abständen den Status jedes Mitglieds der Remoteverknüpfung ab und aktualisiert diesen Status in der VMware Cloud Director-Datenbank des lokalen Standorts. Der Mitgliederstatus ist im `Status`-Element eines `SiteAssociationMember` oder `OrgAssociationMember` sichtbar. Dieses Element kann einen von drei Werten aufweisen:

ACTIVE

Die Verknüpfung wurde von beiden Parteien hergestellt und die Kommunikation mit der Remoteseite war erfolgreich.

ASYMMETRIC

Die Verknüpfung wurde am lokalen Standort hergestellt, aber der Remotestandort hat noch nicht reagiert.

UNREACHABLE

Eine Verknüpfung wurde von beiden Parteien erstellt, aber der Remotestandort ist derzeit nicht im Netzwerk erreichbar.

Der Prozess mit dem Mitgliederstatus „Taktsignal“ wird mit der Identität des standortübergreifenden Systembenutzers ausgeführt, einem lokalen VMware Cloud Director-Benutzerkonto, das in der Systemorganisation während der VMware Cloud Director-Installation erstellt wurde. Obwohl dieses Konto Mitglied der Systemorganisation ist, verfügt es nicht über Administratorrechte. Es verfügt lediglich über die Berechtigung `Multisite: System Operations`, mit der es eine VMware Cloud Director-API-Anforderung zum Abrufen des Status des Remotemitglieds einer Standortverknüpfung durchführen kann.

Ressourcenlisten für mehrere Standorte

Wenn Sie mit VMware Cloud 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 VMware Cloud Director Ressourcenlisten für mehrere Standorte. Ab Version 10.0 unterstützt VMware Cloud Director Ressourcenlisten für mehrere Standorte, die Organisationen enthalten.

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 Organisationen, Organisations-VDCs, Organisations-VDC-Vorlagen, Anbieter-VDCs, Cloud-Zellen, Edge-Gateways, externe Netzwerke, Netzwerkpools und VM-Größenrichtlinien 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 Service Provider Admin Portal oder die vCloud API verwenden. Informationen zur Verwendung des Service Provider Admin Portal finden Sie unter [Erstellen eines virtuellen Provider-Datencenters](#). Informationen zur Verwendung der vCloud API finden Sie im *VMware Cloud Director API-Programmierhandbuch*.

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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus.
- 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus.
- 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 in der oberen Navigationsleiste unter **Ressourcen 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. Die höchste unterstützte Hardwareversion der virtuellen Maschine in VMware Cloud Director 10.1.0 ist Version 15. Hardwareversion 15 ist verfügbar, wenn Sie sie in der vCenter Server-Instanz auf der Ebene des Clusters oder des Datencenters aktivieren.

- 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 zum selben vCenter Server-Datencenter.
- Die Provider-VDCs im Ziel enthalten nur elastische Organisations-VDCs.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus.
- 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 VMware Cloud Director-Objekten im Datenspeicher verwendet wird. Dazu gehören:</p> <ul style="list-style-type: none"> ■ In VMware Cloud 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 Server	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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.

- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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.

Aktivieren der VM-Verschlüsselung für Speicherrichtlinien eines virtuellen Provider-Datencenters

Sie können einem Provider-VDC eine Speicherrichtlinie mit aktivierter Verschlüsselung hinzufügen. Sie können VMs und Festplatten verschlüsseln, indem Sie eine VM oder Festplatte einer Speicherrichtlinie zuordnen, die über die VM-Verschlüsselungsfunktion verfügt.

Ab VMware Cloud Director 10.1 können Sie die Sicherheit Ihrer Daten mithilfe der VM-Verschlüsselung verbessern. Bei der Verschlüsselung wird nicht nur Ihre virtuelle Maschine geschützt, sondern auch die Festplatten und andere Dateien der virtuellen Maschine. Sie können die Funktionen von Speicherrichtlinien und den Verschlüsselungsstatus von VMs und Festplatten in der API und der Benutzeroberfläche anzeigen. Sie können alle in der jeweiligen vCenter Server-Version unterstützten Vorgänge auf verschlüsselten VMs und Festplatten durchführen.

Aktivieren der VM-Verschlüsselung

Um VMs in VMware Cloud Director zu verschlüsseln, müssen Sie mindestens einen Key Management Server (KMS) auf der vCenter Server-Instanz konfigurieren und die VMs und Festplatten einer Speicherrichtlinie zuordnen, die über die VM-Verschlüsselungsfunktion verfügt.

- 1 Fügen Sie in vCenter Server einen KMS-Cluster hinzu. Eine vCenter Server-Instanz kann mehrere KMS-Cluster enthalten. Informationen zum Einrichten eines Schlüsselverwaltungsserver-Clusters finden Sie im Abschnitt [Einrichten des Schlüsselmanagementserver-Clusters](#) im Handbuch *vSphere-Sicherheit*.
- 2 Aktivieren Sie in vCenter Server die Verschlüsselung für eine Speicherrichtlinie. Weitere Informationen finden Sie im Abschnitt [Erstellen einer Speicherrichtlinie für die Verschlüsselung](#) im Handbuch *vSphere-Sicherheit*.
- 3 Fügen Sie im VMware Cloud Director Service Provider Admin Portal die Richtlinie mit aktivierter Verschlüsselung einem Provider-VDC hinzu. Weitere Informationen finden Sie im [Hinzufügen einer VM-Speicherrichtlinie zu einem virtuellen Provider-Datencenter](#).

- 4 Fügen Sie im VMware Cloud Director Service Provider Admin Portal die Richtlinie mit aktivierter Verschlüsselung einem Organisations-VDC hinzu. Weitere Informationen finden Sie im [Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC](#).
- 5 Im VMware Cloud Director Tenant Portal können Mandanten die VM oder die Festplatte einer Speicherrichtlinie mit aktivierter VM-Verschlüsselung zuordnen.
- 6 Um eine VM oder Festplatte zu entschlüsseln, können Mandanten diese VM oder Festplatte einer Speicherrichtlinie zuordnen, für die die Verschlüsselung nicht aktiviert ist.

Einschränkungen bei der VM-Verschlüsselung

Die folgenden Aktionen werden in VMware Cloud Director 10.1 nicht unterstützt.

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

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

Identifizieren einer VM-Verschlüsselungsspeicherfunktion

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

Sie können alle Speicherfunktionen in der Spalte **Funktionen** unter **Ressourcen > vSphere-Ressourcen > Speicherrichtlinien** anzeigen. Diese Spalte zeigt die VM-Verschlüsselung, die Tag-basierte Zuordnung, vSAN und die IOPS-Begrenzung der Speicherfunktionen an. Um die vollständige Liste der Speicherfunktionen anzuzeigen, erweitern Sie die Zeile, indem Sie auf den Pfeil links neben dem Namen der Speicherrichtlinie klicken.

Sie können die Informationen zur Speicherfunktion auch auf der Registerkarte **Speicherrichtlinien** eines Provider-VDC anzeigen.

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.

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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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**.

Aktivieren der Einstellung „E/A-Vorgänge pro Sekunde“

Sie können die Einstellung „E/A-Vorgänge pro Sekunde“ (IOPS) für eine Speicherrichtlinie aktivieren, sodass Mandanten IOPS-Limits pro Festplatte festlegen können.

Die verwaltete Lese-/Schreibleistung von physischen Speichergeräten und virtuellen Festplatten wird in Einheiten mit der Bezeichnung IOPS definiert, mit denen die Lese-/Schreibvorgänge pro Sekunde gemessen werden. Um die E/A-Leistung zu begrenzen, muss eine Provider-VDC-Speicherrichtlinie, die Speichergeräte mit aktivierter IOPS-Zuteilung beinhaltet, eine Organisations-VDC-Speicherrichtlinie unterstützen. Anschließend kann ein Mandant Festplatten konfigurieren, die die Einstellung verwenden, um eine festgelegte E/A-Leistung anzufordern. Ein mit IOPS-Unterstützung konfiguriertes Speicherprofil liefert seinen Standard-IOPS-Wert an alle Festplatten, die es verwenden. Dies umfasst Festplatten, die nicht für die Anforderung eines bestimmten IOPS-Werts konfiguriert sind. Eine Festplatte, die dafür konfiguriert ist, einen bestimmten IOPS-Wert anzufordern, kann ein Speicherprofil, dessen maximaler IOPS-Wert unter dem angeforderten Wert liegt, oder ein Speicherprofil, für das keine IOPS-Unterstützung konfiguriert ist, nicht verwenden.

Hinweis Der tatsächliche E/A-Durchsatz, den die virtuellen Maschinen erkennen, ist eine Kombination aus Blockgröße und IOPS. Wenn die VMs unterschiedliche Blockgrößen verwenden, wird ihr Durchsatz unterschiedlich sein, auch wenn IOPS auf dieselbe Zahl begrenzt sind. Weitere Informationen zum Verwalten von Speicher-E/A-Ressourcen finden Sie im Handbuch *vSphere-Ressourcenverwaltung*.

- 1 Fügen Sie IOPS-Kapazitäten in vCenter Server zu einem oder mehreren Datenspeichern hinzu.
- 2 Erstellen Sie in vCenter Server eine Speicherrichtlinie, die die Datenspeicher mit hinzugefügten IOPS-Kapazitäten verwendet.
- 3 Fügen Sie mithilfe des VMware Cloud Director Service Provider Admin Portal oder der VMware Cloud Director-API die Speicherrichtlinie einem oder mehreren Provider-VDCs hinzu.
- 4 Wenn Sie das Service Provider Admin Portal oder die VMware Cloud Director-API verwenden, veröffentlichen Sie die Speicherrichtlinie in einem oder mehreren Organisations-VDCs.
- 5 Aktualisieren Sie mithilfe der VMware Cloud Director-API die Organisations-VDC-Speicherrichtlinie, um die IOPS-Begrenzung zu aktivieren und den maximalen IOPS-Wert, den standardmäßigen IOPS-Wert usw. festzulegen.

Sie können die IOPS-Begrenzung auf einer vorhandenen Speicherrichtlinie aktivieren.

- 1 Fügen Sie IOPS-Kapazitäten in vCenter Server zu allen Datenspeichern hinzu, die mit der Speicherrichtlinie verknüpft sind, die Sie ändern möchten.
- 2 Stellen Sie mithilfe des VMware Cloud Director Service Provider Admin Portal oder der VMware Cloud Director-API sicher, dass die entsprechende Provider-VDC-Speicherrichtlinie die IOPS-Kapazität als ungleich null meldet.
- 3 Aktualisieren Sie mithilfe der VMware Cloud Director-API die Organisations-VDC-Speicherrichtlinie, um die IOPS-Begrenzung zu aktivieren und den maximalen IOPS-Wert, den standardmäßigen IOPS-Wert usw. festzulegen.

Wenn Sie IOPS-Begrenzung für die Speicherrichtlinie eines Organisations-VDC aktivieren, verwenden Mandanten das VMware Cloud Director Tenant Portal, um die IOPS-Grenzwerte pro Festplatte festzulegen.

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. VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.

- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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

VMware Cloud 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.

VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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](#).
- 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 VMware Cloud Director Service Provider Admin Portal können Sie VMware Cloud Director-Organisationen erstellen, konfigurieren und verwalten.

Verwenden Sie das VMware Cloud 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](#)
- [Aktivieren oder Deaktivieren einer Organisation](#)
- [Löschen einer Organisation](#)
- [Konfigurieren von Katalogen für eine Organisation](#)
- [Konfigurieren von Richtlinien für eine Organisation](#)
- [Mandantenspeicher migrieren](#)

Wissenswertes über Leases

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

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

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

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

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

Erstellen einer Organisation

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

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.

- a Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.

Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.

- 2 Klicken Sie auf **Neu**.

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.

Aktivieren oder Deaktivieren einer Organisation

Wenn Sie eine Organisation deaktivieren, können sich die Benutzer nicht mehr bei der Organisation anmelden, und die Sitzungen der Benutzer, die aktuell angemeldet sind, werden beendet. Zu diesem Zeitpunkt innerhalb der Organisation ausgeführte vApps werden weiterhin ausgeführt.

Systemadministratoren können auch deaktivierten Organisationen Ressourcen zuweisen, Netzwerke hinzufügen usw.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf das Optionsfeld neben dem Namen der Organisation und klicken Sie dann auf **Aktivieren** oder **Deaktivieren**.

Löschen einer Organisation

Löschen Sie eine Organisation, um sie endgültig aus VMware Cloud Director zu entfernen.

Voraussetzungen

Sie können eine Organisation erst dann löschen, wenn Sie sie deaktiviert und alle Organisations-VDCs, Vorlagen, Mediendateien und vApps in der Organisation gelöscht haben.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.
- 2 Klicken Sie auf das Optionsfeld neben dem Namen der Organisation und dann auf **Löschen**.
- 3 Klicken Sie zur Bestätigung auf **Ja**.

Konfigurieren von Katalogen für eine Organisation

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

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - a Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.
- 2 Wählen Sie eine Organisation aus und wählen Sie auf der Registerkarte **Konfigurieren** die Option **Katalog** aus.

- 3 Um die Freigabe- und Veröffentlichungseinstellungen zu ändern, klicken Sie auf **Bearbeiten**.

Option	Beschreibung
Gemeinsame Nutzung	Ermöglicht Organisationsadministratoren, Kataloge dieser Organisation für andere Organisationen in dieser Instanz von VMware Cloud 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 VMware Cloud Director zu veröffentlichen.
Abonnieren von externen Katalogen zulassen	Ermöglicht Organisationsadministratoren, Kataloge außerhalb dieser Instanz von VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - Wählen Sie im linken Fensterbereich die Option **Organisationen** aus.

Die Liste der vorhandenen Organisationen wird in einer Rasteransicht angezeigt.
- Wählen Sie eine Organisation und dann die Registerkarte **Richtlinien** aus.
- Klicken Sie auf **Bearbeiten**, 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.
Laufzeitablaufaktion	Gibt an, wie abgelaufene ausgeführte vApps verarbeitet werden. Durch das Anhalten einer vApp werden alle virtuellen Maschinen angehalten, und ihr aktueller Status wird durch Schreiben des Arbeitsspeichers auf die Festplatte beibehalten. Beim Ausschalten werden alle virtuellen Maschinen und untergeordneten vApps sofort angehalten.
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.

Mandantenspeicher migrieren

Sie können alle vApps, unabhängigen Festplatten und Katalogelemente einer oder mehrerer Organisationen von einem oder mehreren Datenspeichern zu anderen Datenspeichern migrieren.

Bevor Sie einen Datenspeicher stilllegen, müssen Sie alle in diesem Datenspeicher abgelegten Elemente auf einen neuen Datenspeicher migrieren. Sie möchten möglicherweise auch eine Organisation zu einem neuen Datenspeicher migrieren, der über mehr Speicherkapazität verfügt oder eine neuere Speichertechnologie wie VMware vSAN verwendet.

Wichtig Die Migration des Mandantenspeichers ist ein ressourcenintensiver Vorgang, der über einen langen Zeitraum ausgeführt werden kann, besonders dann, wenn viele Assets migriert werden müssen. Weitere Informationen zum Migrieren des Mandantenspeichers finden Sie unter <https://kb.vmware.com/kb/2151086>.

Voraussetzungen

- Bestimmen Sie die Speicherrichtlinien, die von den Organisations-VDCs der Zielorganisationen verwendet werden. Weitere Informationen finden Sie im [Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC](#).
- Stellen Sie für jede Speicherrichtlinie mit einem zu migrierenden Quelldatenspeicher sicher, dass mindestens ein Zieldatenspeicher vorhanden ist, auf den migriert werden kann. Sie können Zieldatenspeicher erstellen oder vorhandene verwenden. Weitere Informationen zur Ermittlung der Datenspeicher in den von den Zielorganisationen verwendeten Speicherrichtlinien finden Sie in der Dokumentation zu *vSphere-Speicher*.

Verfahren

- 1 Melden Sie sich bei der VMware Cloud Director Service Provider Admin Portal als **Systemadministrator** oder mit einer Rolle an, die die Berechtigung **Organisation: Mandantenspeicher migrieren** aufweist.
- 2 Starten Sie den Assistenten **Mandantenspeicher migrieren**.
 - Wählen Sie unter **Cloud-Ressourcen** die Option **Organisationen** aus und klicken Sie auf **Mandantenspeicher migrieren**.
 - Wählen Sie unter **vSphere-Ressourcen** die Option **Datenspeicher** aus und klicken Sie auf **Mandantenspeicher migrieren**.
- 3 Wählen Sie eine oder mehrere Organisationen mit Speicherelementen aus, die Sie migrieren möchten, und klicken Sie auf **Weiter**.
- 4 Wählen Sie mindestens einen zu migrierenden Quelldatenspeicher aus und klicken Sie auf **Weiter**.
Der Assistent listet alle Datenspeicher im System auf.
- 5 Wählen Sie einen oder mehrere Zieldatenspeicher aus und klicken Sie auf **Weiter**.

- 6 Überprüfen Sie die Seite **Bereit zum Abschließen** und klicken Sie dann auf **Beenden**, um die Migration zu starten.

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 VM-Größen- und VM-Platzierungsrichtlinien
- 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
- Konfigurieren von VDC-übergreifenden Netzwerken
- 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 Ressourcenpoolsebene 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 der CPU-Grenzwert einer VM nicht in einer VM-Größenrichtlinie 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 VM-Größenrichtlinie der VM.	Unbegrenzt	Unbegrenzt	vCPU-Geschwindigkeit multipliziert mit der Anzahl der vCPUs	Benutzerdefiniert
CPU-Reservierung der VM	Basierend auf der VM-Größenrichtlinie 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 VM-Größenrichtlinie der VM.	Unbegrenzt	Unbegrenzt	vRAM	Benutzerdefiniert
VM-RAM-Reservierung	Basierend auf der VM-Größenrichtlinie 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

Umwandeln eines veralteten VDC-Zuteilungsmodells in ein flexibles Zuteilungsmodell

Sie fügen eine VM-Platzierungs- und VM-Größenrichtlinie mit einem elastischen oder nicht elastischen Zuweisungspoolmodell, einem Pay-As-You-Go-Modell oder einem Reservierungspoolmodell hinzu. Wenn die VM-Platzierungs- oder VM-Größenrichtlinie nicht mit dem vorhandenen VDC-Zuweisungsmodell kompatibel ist, können Sie das VDC in ein flexibles Organisations-VDC umwandeln.

VM-Richtlinienkonformität

Die Umwandlung eines veralteten VDC hat keine Nichtkonformität der VM zur Folge. Wenn ein Administrator die Computing-Werte der VM oder die VM-Gruppenmitgliedschaft einer VM direkt in der vCenter Server-Instanz ändert, kann es zu einer Nichtkonformität der VM mit der zugewiesenen VM-Platzierungs- oder VM-Größenrichtlinie kommen. Es kann bei einer VM folglich auch zu einer Nichtkonformität kommen, wenn ein Benutzer mit den notwendigen Berechtigungen die Reservierungs- und Grenzwerte der VM mithilfe der vCloud-API ändert. Wenn eine nicht konforme VM vorhanden ist, wird auf der VMware Cloud Director Tenant Portal-Benutzeroberfläche eine Warnmeldung angezeigt. Der Mandant kann detaillierte Informationen über die Ursache für die Nichtkonformität anzeigen und die Konformität der VM wiederherstellen, wodurch die Richtlinien erneut auf die VM angewendet werden.

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 VMware Cloud 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.

Zuweisungsmodell	Vorgeschlagene Verwendung
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 VMware Cloud 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 VMware Cloud Director 9.7 können **Systemadministratoren** virtuelle Organisations-Datencenter (VDC) unter Verwendung des Flex-Zuweisungsmodells erstellen. Mit der Kombination aus Flex-Zuweisung und VM-Größenrichtlinien 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.

In VMware Cloud Director 10.0 und höher können alle Nicht-Flex-Organisations-VDCs in Flex-VDCs umgewandelt werden.

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

Parameter	Beschreibung
Elasticity	Aktivieren oder deaktivieren Sie die Funktion des elastischen Pools.
Include VM Memory Overhead	Schließen Sie den Arbeitsspeicher-Overhead in diesem VDC ein oder aus. Wenn der Wert auf „true“ festgelegt ist, können Sie möglicherweise nicht die vollständige Kapazität des VDC verwenden, da der Arbeitsspeicher-Overhead jeder eingeschalteten VM auch aus der verfügbaren Kapazität des VDC entnommen wird. Wenn der Wert auf „false“ festgelegt ist, wird der Arbeitsspeicher-Overhead vom Provider-VDC und nicht von der zugeteilten Kapazität des VDC übernommen.

Parameter	Beschreibung
CPU allocation	Die diesem VDC zugeteilte CPU-Menge in MHz oder GHz. Die CPU-Zuteilung definiert die CPU-Kapazität des VDC. Die gesamte CPU-Nutzung aller VMs, die im VDC ausgeführt werden, darf diesen Wert nicht überschreiten.
CPU limit	Der CPU-Grenzwert definiert das CPU-Kontingent eines VDC. In den meisten Fällen ist der CPU-Grenzwert gleich der zugeteilten CPU-Kapazität des VDC. In manchen Fällen müssen Sie möglicherweise dem VDC keine CPU zuweisen, wie im Pay-As-You-Go-Modell. In diesem Fall müssen Sie ein Kontingent für den gesamten CPU-Verbrauch festlegen, indem Sie die CPU-Zuteilung auf Null und den CPU-Grenzwert auf einen Wert ungleich Null festlegen. Sie können diese Einstellung auch verwenden, um ein unbegrenztes CPU-Kontingent zuzulassen. Wenn der Wert auf „unbegrenzt“ gesetzt ist, erhalten die Backing-Ressourcenpools des VDC in vCenter Server unbegrenzte CPU.
CPU resources guaranteed	Der Prozentsatz der CPU-Zuteilung, der physisch für das VDC reserviert ist.
vCPU speed	Die standardmäßige vCPU-Geschwindigkeit für VMs im VDC.
Memory allocation	Die Menge an Arbeitsspeicher in MB oder GB, die diesem VDC zugeteilt ist. Dieser Parameter definiert die gesamte RAM-Kapazität des VDC. Der insgesamt konfigurierte Arbeitsspeicher von allen VMs, die im VDC ausgeführt werden, darf diesen Wert nicht überschreiten.
Memory resources guaranteed	Der Prozentsatz der Arbeitsspeicherzuteilung, der physisch für das VDC reserviert ist.
Maximum number of VMs	Die maximale Anzahl der VMs im VDC.

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

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

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.

Als Systemadministrator können Sie Organisations-VDCs mit Zuweisungspool als elastisch oder nicht elastisch konfigurieren. Elastizität ist eine globale Einstellung, die alle Organisations-VDCs mit Zuweisungspool betrifft. Weitere Informationen finden Sie im [Bearbeiten der allgemeinen Systemeinstellungen](#).

Standardmäßig ist bei Organisations-VDCs mit Zuweisungspool ein elastischer Zuweisungspool aktiviert. Bei Systemen, die von VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 Anteileinstellungen 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 *VMware Cloud Director API-Programmierhandbuch*.

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 VMware Cloud 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 Anteileneinstellungen 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 *VMware Cloud Director API-Programmierhandbuch*.

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 VM-Größen- und VM-Platzierungsrichtlinien

Sie können die Ressourcenzuteilung und -platzierung der virtuellen Maschine (VM) auf einem bestimmten Cluster oder Host mithilfe von VM-Größen- und VM-Platzierungsrichtlinien steuern.

In VMware Cloud Director 10.0 werden die Begriffe „VM-Platzierungsrichtlinie“ und „VM-Größenrichtlinie“ eingeführt.

VMware Cloud Director **Systemadministratoren** erstellen und verwalten VM-Größenrichtlinien auf globaler Ebene und können einzelne Richtlinien für ein oder mehrere Organisations-VDCs veröffentlichen. Die VM-Platzierungsrichtlinien werden für jedes Provider-VDC erstellt und verwaltet, da eine VM-Platzierungsrichtlinie auf der Ebene des Provider-VDC angewendet wird. Wenn Sie eine Richtlinie in einem Organisations-VDC veröffentlichen, steht die Richtlinie den Benutzern in der Organisation zur Verfügung. Beim Erstellen und Verwalten von virtuellen Maschinen im Organisations-VDC können Mandanten die verfügbaren Richtlinien virtuellen Maschinen zuweisen. Mandanten und Benutzer im Organisations-VDC können die spezifische Konfiguration einer VM-Platzierungs- oder VM-Größenrichtlinie nicht anzeigen.

VM-Platzierungs- und VM-Größenrichtlinien stellen einen Mechanismus dar, mit dem Cloud-Anbieter differenzierte Dienstebenen definieren und anbieten können, z. B. ein CPU-intensives Profil oder ein Profil mit hoher Arbeitsspeicherauslastung. Wenn Sie mehrere VM-Platzierungs- und VM-Größenrichtlinien in einem Organisations-VDC veröffentlichen, können Mandantenbenutzer beim Erstellen und Verwalten von virtuellen Maschinen im Organisations-VDC zwischen allen benutzerdefinierten Richtlinien und der Standardrichtlinie auswählen. Die Standardrichtlinie des Systems wird für jedes VDC automatisch erzeugt. **Systemadministratoren** können die Standardrichtlinie des Systems im VDC löschen und eine andere benutzerdefinierte Richtlinie als Standardrichtlinie kennzeichnen. In der Standardrichtlinie sind keine Werte definiert und alle Konfigurationen virtueller Maschinen sind zulässig.

VM-Platzierungsrichtlinie

Eine VM-Platzierungsrichtlinie definiert die Platzierung einer virtuellen Maschine auf einem Host oder einer Gruppe von Hosts. Hierbei handelt es sich um einen Mechanismus für **Cloud-Anbieteradministratoren**, der zum Erstellen einer benannten Hostgruppe innerhalb eines Provider-VDC verwendet werden kann. Die benannte Hostgruppe ist eine Teilmenge der Hosts innerhalb der Provider-VDC-Cluster, die basierend auf Kriterien wie Leistungsebenen oder Lizenzierung ausgewählt werden kann. Eine VM-Platzierungsrichtlinie definiert VM-Host-Affinitätsregeln, die sich direkt auf die Platzierung von Mandantenarbeitslasten auswirken. Administratoren definieren oder veröffentlichen benannte Hostgruppen mithilfe von VM-Gruppen in vCenter Server. Eine VM-Gruppe weist eine direkte Affinität zu einer Hostgruppe auf und stellt die Hostgruppe dar, zu der die Affinität besteht.

Sie definieren die VM-Platzierungsrichtlinie auf der Ebene des Provider-VDC. Eine VM-Platzierungsrichtlinie enthält die folgenden Attribute:

- Name (muss im Provider-VDC eindeutig sein)
- Beschreibung
- Ein Satz aus einer oder mehreren VM-Gruppen, die aus den zugrunde liegenden Clustern im Provider-VDC ausgewählt wurden. Sie können eine VM-Gruppe pro Cluster auswählen.

Eine VM-Platzierungsrichtlinie ist während der Erstellung einer virtuellen Maschine optional und ein Mandant kann einer virtuellen Maschine nur eine VM-Platzierungsrichtlinie zuweisen.

Wenn ein Mandant eine virtuelle Maschine im Organisations-VDC erstellt und die VM-Platzierungsrichtlinie auswählt, fügt VMware Cloud Director die virtuelle Maschine der VM-Gruppe hinzu, auf die in der Richtlinie verwiesen wird. Daher erstellt VMware Cloud Director die virtuelle Maschine auf dem entsprechenden Host.

Eine VM-Platzierungsrichtlinie kann keine oder eine VM-Gruppe aus jedem Cluster enthalten. Beispielsweise kann die VM-Platzierungsrichtlinie *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 VM-Platzierungsrichtlinie zuweisen, fügt das Platzierungsmodul diese virtuelle Maschine zur entsprechenden VM-Gruppe des Clusters hinzu, auf dem sie sich befindet. Wenn Sie z. B. eine virtuelle Maschine auf dem Cluster *oracle_cluster1* bereitstellen möchten und die VM-Platzierungsrichtlinie *oracle_license* dieser virtuellen Maschine zuweisen, fügt das Platzierungsmodul die virtuelle Maschine der VM-Gruppe *oracle_license1* hinzu.

VM-Größenrichtlinie

Eine VM-Größenrichtlinie definiert die Computing-Ressourcenzuteilung für virtuelle Maschinen innerhalb eines Organisations-VDC. Die Computing-Ressourcenzuweisung umfasst CPU- und Arbeitsspeicherzuweisung, Reservierungen, Grenzwerte und Anteile.

Mit VM-Größenrichtlinien können VMware Cloud 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
- Zusätzliche Konfigurationen:

Der `extraConfigs`-API-Parameter stellt eine Zuordnung zwischen Schlüssel-Wert-Paaren dar, die als zusätzliche Konfigurationswerte auf eine virtuelle Maschine angewendet werden. Sie können eine Richtlinie mit zusätzlichen Konfigurationen nur mit Nutzung der vCloud-API erstellen. Vorhandene zusätzliche Konfigurationen werden auf der Service Provider Admin Portal-Benutzeroberfläche unter **Zusätzliche Konfigurationen** in der detaillierten Ansicht für VM-Größenrichtlinien angezeigt.

Sie definieren die VM-Größenrichtlinien auf globaler Ebene. Weitere Informationen zu den Attributen von VM-Größenrichtlinien finden Sie unter [Attribute von VM-Größenrichtlinien](#).

VMware Cloud Director erzeugt eine VM-Standardgrößenrichtlinie für alle VDCs. Die VM-Standardgrößenrichtlinie enthält nur einen Namen und eine Beschreibung, während alle verbleibenden Richtlinienattribute leer sind.

Sie können auch eine andere VM-Größenrichtlinie als Standardrichtlinie für ein Organisations-VDC definieren. Die VM-Standardgrößenrichtlinie steuert die Ressourcenzuteilung und die Nutzung der virtuellen Maschinen, die von Mandanten im Organisations-VDC erstellt werden, es sei denn, ein Mandant weist der virtuellen Maschine eine andere spezifische VM-Größenrichtlinie zu.

Cloud-Anbieter können eine maximale VM-Größenrichtlinie definieren, um die maximale Anzahl der Computing-Ressourcen zu begrenzen, die Mandanten einzelnen virtuellen Maschinen innerhalb eines Organisations-VDC zuweisen können. Wenn die maximale VM-Größenrichtlinie einem Organisations-VDC zugewiesen ist, fungiert sie als Obergrenze für die Computing-Ressourcenkonfiguration für alle virtuellen Maschinen innerhalb des Organisations-VDC. Die maximale VM-Größenrichtlinie steht Mandantenbenutzern beim Erstellen einer virtuellen Maschine nicht zur Verfügung. Wenn Sie eine VM-Größenrichtlinie als maximale Richtlinie definieren, kopiert VMware Cloud Director intern den Inhalt der Richtlinie und verwendet den kopierten Inhalt als maximale VM-Größenrichtlinie. Dies führt dazu, dass das Organisations-VDC nicht von der anfänglich verwendeten VM-Größenrichtlinie abhängt.

Mithilfe von VM-Größenrichtlinien können Cloud-Anbieter die Nutzung von Computing-Ressourcen für alle virtuellen Maschinen 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 VM-Größenrichtlinien 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 VM-Größenrichtlinien in einem Organisations-VDC.
- 3 Definieren Sie optional eine der VM-Größenrichtlinien als Standardrichtlinie für das Organisations-VDC.

Zu den verfügbaren Richtlinienvorgängen für Cloud-Anbieter gehören:

- Um die Platzierung einer virtuellen Maschine auf einem Host oder einer Gruppe von Hosts zu definieren, erstellen Sie eine Platzierungsrichtlinie. Weitere Informationen finden Sie im [Erstellen einer VM-Platzierungsrichtlinie](#).
- Um die physische Computing-Ressourcenzuteilung für Mandantenarbeitslasten zu steuern, erstellen Sie eine Größenrichtlinie. Weitere Informationen finden Sie im [Erstellen einer VM-Größenrichtlinie](#).
- Veröffentlichen einer VM-Platzierungs- oder VM-Größenrichtlinie für ein oder mehrere Organisations-VDCs. Weitere Informationen finden Sie unter [Hinzufügen einer VM-Platzierungsrichtlinie zu einem Organisations-VDC](#)
- Festlegen einer VM-Platzierungs- oder VM-Größenrichtlinie als Standardeinstellung.
- Bearbeiten einer VM-Platzierungs- oder VM-Größenrichtlinie. Sie können lediglich den Namen und die Beschreibung der Richtlinie in der VMware Cloud Director-Benutzeroberfläche bearbeiten.
- Rückgängigmachen der Veröffentlichung einer VM-Platzierungs- oder VM-Größenrichtlinie in einem Organisations-VDC.

- Löschen einer VM-Platzierungs- oder VM-Größenrichtlinie. Weitere Informationen finden Sie unter [Löschen einer VM-Platzierungsrichtlinie](#) und [Löschen einer VM-Größenrichtlinie](#).

Benutzer mit der Berechtigung **ORG_VDC_MANAGE_COMPUTE_POLICIES** können VM-Platzierungs- oder VM-Größenrichtlinien erstellen, aktualisieren und veröffentlichen.

In der folgenden Tabelle werden die verfügbaren VM-Platzierungs- und VM-Größenrichtlinienvorgänge für Mandantenbenutzer aufgelistet:

Tabelle 6-1. VM-Platzierungs- und VM-Größenrichtlinienvorgänge für Mandantenbenutzer

Vorgang	Beschreibung
Weisen Sie während der Erstellung einer virtuellen Maschine der virtuellen Maschine eine Richtlinie zu.	<p>Mandantenbenutzer, die zum Erstellen von virtuellen Maschinen in einem Organisations-VDC berechtigt sind, können virtuelle Maschinen mithilfe des VMware Cloud Director Tenant Portal optional VM-Größen- und VM-Platzierungsrichtlinien zuweisen. Folglich steuern die in der VM-Größenrichtlinie definierten Parameter die CPU- und Arbeitsspeichernutzung der virtuellen Maschine. Mandanten müssen während der Erstellung einer virtuellen Maschine keine VM-Platzierungs- oder VM-Größenrichtlinien zuweisen. Wenn ein Mandant eine VM-Größenrichtlinie nicht explizit für die Zuweisung zu einer virtuellen Maschine auswählt, wird die VM-Standardgrößenrichtlinie auf die virtuelle Maschine angewendet.</p> <p>Wenn Sie keine VM-Platzierungsrichtlinie erstellen, ist die VM-Platzierungsrichtlinienoption für die Mandanten nicht sichtbar. Wenn der Mandant eine Platzierungsrichtlinie mit Größeninformationen auswählt, wird die VM-Größenrichtlinienoption für den Mandanten ausgeblendet. Sie können eine VM-Platzierungsrichtlinie mit Größeninformationen nur mithilfe der vCloud-API erstellen.</p> <p>Ist nur eine VM-Größenrichtlinie vorhanden, wird die VM-Größenrichtlinienoptionen den Mandanten nicht angezeigt.</p> <p>Wenn der Systemadministrator die Attribute vCPU-Anzahl, Kerne pro Socket und Arbeitsspeicher in einer VM-Größenrichtlinie festlegt und ein Mandant die Richtlinie auswählt, werden diese Werte angezeigt, können aber nicht bearbeitet werden.</p>
Weisen Sie eine Richtlinie zu einer vorhandenen virtuellen Maschine zu.	<p>Mandantenbenutzer mit der Berechtigung zum Verwalten von virtuellen Maschinen in einem Organisations-VDC können die VM-Größen- und VM-Platzierungsrichtlinien einer vorhandenen virtuellen Maschine mithilfe des VMware Cloud Director Tenant Portal zuweisen oder ändern. Wenn ein Mandant die VM-Platzierungsrichtlinie ändert, wird die virtuelle Maschine gemäß der in der neuen VM-Platzierungsrichtlinie definierten VM-Host-Affinitätsregel auf einen neuen Host verschoben. Wenn ein Mandant eine VM-Größenrichtlinie ändert, konfiguriert das System die virtuelle Maschine neu, um Computing-Ressourcen zu nutzen, die in der neuen VM-Größenrichtlinie angegeben sind.</p>

Der Workflow zum Arbeiten mit VM-Platzierungs- und VM-Größenrichtlinien gestaltet sich folgendermaßen.

- 1 Ein **Systemadministrator** erstellt eine oder mehrere VM-Platzierungsrichtlinien. Weitere Informationen finden Sie im [Erstellen einer VM-Platzierungsrichtlinie](#).
- 2 Ein **Systemadministrator** erstellt eine oder mehrere VM-Größenrichtlinien. Weitere Informationen finden Sie im [Erstellen einer VM-Größenrichtlinie](#).

Der Name einer VM-Größenrichtlinie ist auf einer einzelnen VMware Cloud Director-Site eindeutig. Der Name einer VM-Platzierungsrichtlinie ist innerhalb des Provider-VDC-Geltungsbereichs der Richtlinie eindeutig.

- Ein **Systemadministrator** veröffentlicht die VM-Platzierungs- und VM-Größenrichtlinien für ein oder mehrere Organisations-VDCs. Weitere Informationen finden Sie im [Hinzufügen einer VM-Platzierungsrichtlinie zu einem Organisations-VDC](#).

Eine veröffentlichte VM-Platzierungsrichtlinie steht Mandantenbenutzern in den Organisations-VDCs während der Erstellung und Bearbeitung von virtuellen Maschinen zur Verfügung.

- Beim Erstellen oder Aktualisieren einer virtuellen Maschine können Mandanten die vCloud-API oder das VMware Cloud Director Tenant Portal verwenden, um einer virtuellen Maschine eine VM-Größen- und VM-Platzierungsrichtlinie zuzuweisen.

Attribute von VM-Größenrichtlinien

Wenn Sie eine VM-Größenrichtlinie erstellen, können Sie eine Teilmenge aller verfügbaren Attribute angeben. Das einzige obligatorische Attribut ist der Name der VM-Größenrichtlinie.

Es gibt zwei Arten von Parametern in einer VM-Größenrichtlinie.

- Individuelle VM-Größenkonfiguration – Sie konfigurieren vorab den angegebenen RAM, die vCPU-Anzahl und die Kerne pro Socket für die VMs unter der aktuellen Richtlinie.
- Einschränkungen für den maximalen Verbrauch an Ressourcen – Sie konfigurieren vorab eine Beschränkung für die Nutzung von Arbeitsspeicher und CPU durch eine einzelne VM unter der aktuellen Richtlinie.

Die folgende Tabelle listet alle Attribute auf, die Sie innerhalb einer VM-Größenrichtlinie definieren können.

Tabelle 6-2. VDC-Computing-Richtlinienattribute

VDC-Computing-Richtlinienattribut	API-Parameter	Beschreibung
Name	name	Obligatorischer Parameter, der als Bezeichner für die VM-Größenrichtlinie verwendet wird.
Description	description	Stellt eine kurze Beschreibung der VM-Größenrichtlinie dar.
vCPU Speed	cpuSpeed	Definiert die vCPU-Geschwindigkeit eines Kernels in MHz oder GHz.
vCPU Count	cpuCount	Definiert die Anzahl der für eine VM konfigurierten vCPUs. Dies ist eine VM-Hardwarekonfiguration. Wenn ein Mandant die VM-Größenrichtlinie einer VM zuweist, wird diese Anzahl zur konfigurierten Anzahl von vCPUs für die VM.

Tabelle 6-2. VDC-Computing-Richtlinienattribute (Fortsetzung)

VDC-Computing-Richtlinienattribut	API-Parameter	Beschreibung
Cores Per Socket	coresPerSocket	<p>Die Anzahl der Kerne pro Socket für eine VM. Dies ist eine VM-Hardwarekonfiguration.</p> <p>Die Anzahl der vCPUs, die in der VM-Größenrichtlinie definiert ist, muss durch die Anzahl der Kerne pro Socket teilbar sein.</p> <p>Wenn die Anzahl der vCPUs nicht durch die Anzahl der Kerne pro Socket teilbar ist, wird die Anzahl der Kerne pro Socket ungültig.</p>
CPU Reservation Guarantee	cpuReservationGuarantee	<p>Legt fest, wie viele CPU-Ressourcen einer VM reserviert sind.</p> <p>Die zugewiesene CPU für eine VM entspricht der Anzahl der vCPUs multipliziert mit der vCPU-Geschwindigkeit in MHz.</p> <p>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.</p>
CPU Limit	cpuLimit	<p>Definiert den CPU-Grenzwert in MHz oder GHz für eine VM.</p> <p>Wenn er in der VDC-Computing-Richtlinie nicht definiert ist, ist der CPU-Grenzwert die vCPU-Geschwindigkeit multipliziert mit der Anzahl der vCPUs.</p>
CPU Shares	cpuShares	<p>Definiert die Anzahl der CPU-Anteile für eine VM.</p> <p>Anteile kennzeichnen die relative Bedeutung einer VM innerhalb eines virtuellen Datencenters. Falls eine VM doppelt so viele CPU-Anteile wie eine andere VM hat, darf sie doppelt so viel CPU verbrauchen, wenn beide um Ressourcen konkurrieren.</p> <p>Wenn sie in der VDC-Computing-Richtlinie nicht definiert sind, werden normale Anteile auf die VM angewendet.</p>
Memory	memory	<p>Definiert den für eine VM konfigurierten Arbeitsspeicher in MB oder GB. Dies ist eine VM-Hardwarekonfiguration.</p> <p>Wenn ein Mandant die VM-Größenrichtlinie einer VM zuweist, erhält die VM die Menge an Arbeitsspeicher, die durch dieses Attribut definiert wird.</p>
Memory Reservation Guarantee	memoryReservationGuarantee	<p>Definiert die reservierte Menge an Arbeitsspeicher, die für eine VM konfiguriert ist.</p> <p>Der Wert des Attributs liegt zwischen 0 und 100 %.</p>
Memory Limit	memoryLimit	<p>Definiert den Arbeitsspeichergrenzwert in MB oder GB für eine VM.</p> <p>Wenn er in der VM-Größenrichtlinie nicht definiert ist, entspricht der Arbeitsspeichergrenzwert dem zugewiesenen Arbeitsspeicher für die VM.</p>

Tabelle 6-2. VDC-Computing-Richtlinienattribute (Fortsetzung)

VDC-Computing-Richtlinienattribut	API-Parameter	Beschreibung
Memory Shares	memoryShares	Definiert die Anzahl der Arbeitsspeicheranteile für eine VM. Anteile kennzeichnen die relative Bedeutung einer VM innerhalb eines virtuellen Datencenters. Falls eine VM doppelt so viele Arbeitsspeicheranteile wie eine andere VM hat, darf sie doppelt so viel Arbeitsspeicher verbrauchen, wenn beide um Ressourcen konkurrieren. Wenn sie in der VDC-Computing-Richtlinie nicht definiert sind, werden normale Anteile auf die VM angewendet.
Extra Configuration	extraConfigs	Stellt eine Zuordnung zwischen Schlüssel-Wert-Paaren dar, die als zusätzliche Konfigurationswerte auf eine VM angewendet werden. Sie können eine Richtlinie mit zusätzlichen Konfigurationen nur über die vCloud-API erstellen. Vorhandene zusätzliche Konfigurationen werden auf der Service Provider Admin Portal-Benutzeroberfläche unter Zusätzliche Konfigurationen in der detaillierten Ansicht für VM-Größenrichtlinien angezeigt.

Erstellen einer VM-Platzierungsrichtlinie

Eine VM-Platzierungsrichtlinie ist eine VDC-Computing-Richtlinie, die einen Verweis auf eine Provider-VDC-Richtlinie enthält. Sie können eine VM-Platzierungsrichtlinie verwenden, um die Platzierung einer VM auf einem bestimmten Host, einer Gruppe von Hosts oder einem Cluster zu definieren.

Voraussetzungen

- Stellen Sie sicher, dass mindestens ein Provider-VDC in Ihrer Umgebung vorhanden ist.
- Stellen Sie sicher, dass Sie über mindestens eine VM-Gruppe in Ihrer Umgebung verfügen.

Eine VM-Gruppe ist eine Sammlung von VMs, die Sie mit einer Hostgruppe mit positiven oder negativen Affinitäten verknüpfen können. Über eine positive Affinitätsregel veranlassen Sie die Platzierung einer Gruppe von VMs auf einem bestimmten Host. Eine Anti-Affinitätsregel oder negative Affinitätsregel platziert eine Gruppe von VMs auf verschiedenen Hosts, wodurch verhindert wird, dass alle VMs gleichzeitig ausfallen, wenn ein einzelner Host ausfällt. Sie können eine VM-Gruppe über die vCenter Server-Benutzeroberfläche oder die VMware Cloud Director-API erstellen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus.
- 3 Klicken Sie auf ein Provider-VDC in der Liste.
- 4 Klicken Sie auf die Registerkarte **VM Platzierungsrichtlinien** und dann auf **Neu**.

- 5 (Optional) Aktivieren Sie auf der Seite **Was ist die VM-Platzierungsrichtlinie** des Assistenten das Kontrollkästchen, um die Informationen zur VM-Platzierungsrichtlinie nicht mehr anzuzeigen.
- 6 Klicken Sie auf **Weiter**.
- 7 Geben Sie für die VM-Platzierungsrichtlinie einen Namen und optional eine Beschreibung ein.
- 8 Wählen Sie die VM-Gruppen oder logischen VM-Gruppen aus, mit denen die VM verknüpft werden soll, und klicken Sie auf **Weiter**.

Wenn Sie mehr als eine logische Gruppe auswählen und ein Mandant diese Richtlinie auf eine VM anwendet, wird die VM Mitglied aller VM-Gruppen, die in den ausgewählten logischen VM-Gruppen enthalten sind. Die VM ist auf eine Kombination aller Affinitäten konditioniert, die für die VMs in diesen Gruppen gelten.

Sie können eine logische Inline-VM-Gruppe erstellen, indem Sie eine VM-Gruppe pro Cluster auswählen. Diese logische VM-Gruppe hat keinen Namen und kann nur für die ausgewählte VM-Platzierungsrichtlinie verwendet werden.

- 9 Überprüfen Sie die Einstellungen für die VM-Platzierungsrichtlinie und klicken Sie auf **Beenden**.

Nächste Schritte

- [Erstellen einer VM-Größenrichtlinie](#).
- [Hinzufügen einer VM-Platzierungsrichtlinie zu einem Organisations-VDC](#).

Hinzufügen einer VM-Platzierungsrichtlinie zu einem Organisations-VDC

Wenn Sie eine VM-Platzierungsrichtlinie erstellen, ist sie für Mandanten nicht sichtbar. Sie können eine VM-Platzierungsrichtlinie in einem Organisations-VDC veröffentlichen, um sie den Mandanten zur Verfügung zu stellen.

Durch das Veröffentlichen einer VM-Platzierungsrichtlinie in einem Organisations-VDC wird die Richtlinie für Mandanten sichtbar. Der Mandant kann die Richtlinie auswählen, wenn Sie eine neue eigenständige VM oder eine VM aus einer Vorlage erstellen, eine VM bearbeiten, eine VM zu einer vApp hinzufügen und eine vApp aus einer vApp-Vorlage erstellen. Sie können eine VM-Platzierungsrichtlinie, die für Mandanten verfügbar ist, nicht löschen.

Voraussetzungen

- Stellen Sie sicher, dass mindestens ein Organisations-VDC in Ihrer Umgebung vorhanden ist. Weitere Informationen finden Sie im [Erstellen eines virtuellen Organisations-Datencenters](#).
- Vergewissern Sie sich, dass Sie über mindestens eine VM-Platzierungsrichtlinie verfügen. Weitere Informationen finden Sie im [Erstellen einer VM-Platzierungsrichtlinie](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.

- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- 3 Wählen Sie ein Organisations-VDC aus und klicken Sie auf die Registerkarte **VM-Platzierungsrichtlinien**.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Wählen Sie die VM-Platzierungsrichtlinien aus, die Sie zum Organisations-VDC hinzufügen möchten, und klicken Sie auf **OK**.

Nächste Schritte

- Wählen Sie eine Richtlinie aus und klicken Sie auf **Entfernen**, um die Veröffentlichung der Richtlinie rückgängig zu machen.
- Wählen Sie eine VM-Platzierungsrichtlinie aus und klicken Sie auf **Als Standard festlegen**, damit diese Richtlinie während einer VM- und vApp-Erstellung sowie VM-Bearbeitung als Standardoption für die Mandanten angezeigt wird. Wenn mehrere VM-Platzierungsrichtlinien für ein Organisations-VDC veröffentlicht wurden, kann der Mandant eine andere Richtlinie als die Standardrichtlinie auswählen.

Löschen einer VM-Platzierungsrichtlinie

Wenn eine VM-Platzierungsrichtlinie nicht für Mandanten veröffentlicht wird, können Sie sie aus dem Provider-VDC löschen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über mindestens eine VM-Platzierungsrichtlinie in Ihrer Umgebung verfügen.
- Vergewissern Sie sich, dass die VM-Platzierungsrichtlinie keinem Organisations-VDC hinzugefügt ist. Sie können keine VM-Platzierungsrichtlinien löschen, die für Mandanten verfügbar sind.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus.
- 3 Klicken Sie auf ein Provider-VDC in der Liste.
- 4 Klicken Sie auf die Registerkarte **VM-Platzierungsrichtlinien** und wählen Sie eine VM-Platzierungsrichtlinie aus.
- 5 Klicken Sie auf **Löschen**.

Erstellen einer VM-Größenrichtlinie

Sie können eine VM-Größenrichtlinie erstellen, um den Mandanten vordefinierte CPU- und Arbeitsspeicher-Nutzungseinschränkungen zur Verfügung zu stellen, die sie auf einzelne VMs in einem Organisations-VDC anwenden können.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **VM-Größenrichtlinien**.
- 3 Klicken Sie auf **Neu**.
- 4 Geben Sie für die VM-Größenrichtlinie einen Namen und optional eine Beschreibung ein.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie auf der Seite **CPU** die CPU-Zuteilungseinstellungen aus, die Sie auf die Richtlinie anwenden möchten, und klicken Sie auf **Weiter**.
- 7 Wählen Sie die Einstellungen für die Arbeitsspeicherzuteilung aus, die Sie auf die Richtlinie anwenden möchten, und klicken Sie auf **Weiter**.
- 8 Überprüfen Sie die Einstellungen für die VM-Größenrichtlinie und klicken Sie auf **Beenden**.

Nächste Schritte

- Nachdem Sie eine VM-Größenrichtlinie erstellt haben, können Sie nur den Namen und die Beschreibung der VM-Größenrichtlinie bearbeiten. Weitere Informationen finden Sie im [Bearbeiten einer VM-Größenrichtlinie](#).
- [Hinzufügen einer VM-Größenrichtlinie zu einem Organisations-VDC](#).
- [Erstellen einer VM-Platzierungsrichtlinie](#).

Hinzufügen einer VM-Größenrichtlinie zu einem Organisations-VDC

Wenn Sie eine VM-Größenrichtlinie erstellen, ist sie für Mandanten nicht sichtbar. Sie können eine VM-Größenrichtlinie in einem Organisations-VDC veröffentlichen, um sie den Mandanten zur Verfügung zu stellen.

Durch das Veröffentlichen einer VM-Größenrichtlinie in einem Organisations-VDC wird die Richtlinie für Mandanten sichtbar. Der Mandant kann die Richtlinie auswählen, wenn Sie eine neue eigenständige VM oder eine VM aus einer Vorlage erstellen, eine VM bearbeiten, eine VM zu einer vApp hinzufügen und eine vApp aus einer vApp-Vorlage erstellen. Sie können eine VM-Größenrichtlinie, die für Mandanten verfügbar ist, nicht löschen.

Voraussetzungen

- Stellen Sie sicher, dass mindestens ein Organisations-VDC in Ihrer Umgebung vorhanden ist. Weitere Informationen finden Sie im [Erstellen eines virtuellen Organisations-Datencenters](#).
- Vergewissern Sie sich, dass Sie über mindestens eine VM-Größenrichtlinie verfügen. Weitere Informationen finden Sie im [Erstellen einer VM-Größenrichtlinie](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Organisations-VDCs**.

- 3 Wählen Sie ein Organisations-VDC aus und klicken Sie auf die Registerkarte **VM-Größenrichtlinien**.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Wählen Sie die VM-Größenrichtlinien aus, die Sie zum Organisations-VDC hinzufügen möchten, und klicken Sie auf **OK**.

Nächste Schritte

- Wählen Sie eine Richtlinie aus und klicken Sie auf **Entfernen**, um die Veröffentlichung der Richtlinie rückgängig zu machen.
- Wählen Sie eine VM-Größenrichtlinie aus und klicken Sie auf **Als Standard festlegen**, damit diese Richtlinie während einer VM- und vApp-Erstellung und VM-Bearbeitung als Standardoption für die Mandanten angezeigt wird. Wenn mehrere VM-Größenrichtlinien für ein Organisations-VDC veröffentlicht wurden, kann der Mandant eine andere Richtlinie als die Standardrichtlinie auswählen.

Bearbeiten einer VM-Größenrichtlinie

Nachdem Sie eine VM-Größenrichtlinie erstellt haben, können Sie nur den Namen und die Beschreibung bearbeiten. Das Bearbeiten der CPU- und Arbeitsspeicherparameter wird nicht unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass mindestens ein Organisations-VDC in Ihrer Umgebung vorhanden ist. Weitere Informationen finden Sie im [Erstellen eines virtuellen Organisations-Datencenters](#).
- Vergewissern Sie sich, dass Sie über mindestens eine VM-Größenrichtlinie verfügen. Weitere Informationen finden Sie im [Erstellen einer VM-Größenrichtlinie](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **VM-Größenrichtlinien**.
- 3 Klicken Sie auf den Namen der VM-Größenrichtlinie, die Sie bearbeiten möchten.
- 4 Um den Namen und die Beschreibung der Richtlinie zu bearbeiten, klicken Sie auf **Bearbeiten**.
- 5 Klicken Sie auf **Speichern**.

Nächste Schritte

[Hinzufügen einer VM-Größenrichtlinie zu einem Organisations-VDC](#)

Löschen einer VM-Größenrichtlinie

Sie können VM-Größenrichtlinien löschen, die nicht für Mandanten veröffentlicht werden.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über mindestens eine VM-Größenrichtlinie in Ihrer Umgebung verfügen.
- Vergewissern Sie sich, dass die VM-Größenrichtlinie keinem Organisations-VDC hinzugefügt ist. Sie können keine VM-Größenrichtlinien löschen, die für Mandanten verfügbar sind.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **VM-Größenrichtlinien**.
- 3 Wählen Sie eine VM-Größenrichtlinie aus und klicken Sie auf **Löschen**.

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 finden Sie im [Erstellen eines virtuellen Provider-Datencenters](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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

Option	Beschreibung	Zuweisungsmodell
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
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	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. Bei einem Zuweisungspool-Zuweisungsmodell bestimmt der garantierte Prozentsatz auch, welcher Prozentsatz der Arbeitsspeicherzuweisung für dieses virtuelle Organisations-Datencenter zugesichert werden soll.	<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.

VMware Cloud 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**.

VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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-Zieldencenter gehören, verschieben Sie sie in ein anderes virtuelles Organisations-Datencenter.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 VMware Cloud Director-Installation ausgeweitet wird, besteht möglicherweise der Bedarf, einem bestehenden virtuellen Organisations-Datencenter einen aussagekräftigeren Namen oder eine Beschreibung zuzuweisen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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.

Aktivieren der VM-Verschlüsselung für Speicherrichtlinien eines Organisations-VDC

Sie können einem Organisations-VDC eine Speicherrichtlinie mit aktivierter Verschlüsselung hinzufügen. Sie können VMs und Festplatten verschlüsseln, indem Sie eine VM oder Festplatte einer Speicherrichtlinie zuordnen, die über die VM-Verschlüsselungsfunktion verfügt.

Ab VMware Cloud Director 10.1 können Sie die Sicherheit Ihrer Daten mithilfe der VM-Verschlüsselung verbessern. Bei der Verschlüsselung wird nicht nur Ihre virtuelle Maschine geschützt, sondern auch die Festplatten und andere Dateien der virtuellen Maschine. Sie können die Funktionen von Speicherrichtlinien und den Verschlüsselungsstatus von VMs und Festplatten in der API und der Benutzeroberfläche anzeigen. Sie können alle in der jeweiligen vCenter Server-Version unterstützten Vorgänge auf verschlüsselten VMs und Festplatten durchführen.

Wenn das Provider-VDC über eine Speicherrichtlinie mit aktivierter VM-Verschlüsselung verfügt, können Sie die Richtlinie mit aktivierter Verschlüsselung einem Organisations-VDC hinzufügen. Weitere Informationen finden Sie unter [Aktivieren der VM-Verschlüsselung für Speicherrichtlinien eines virtuellen Provider-Datencenters](#) und [Hinzufügen einer VM-Speicherrichtlinie zu einem Organisations-VDC](#). Anschließend können Mandanten mithilfe des VMware Cloud Director Tenant Portal eine VM oder Festplatte einer Speicherrichtlinie mit aktivierter VM-Verschlüsselung zuordnen.

Einschränkungen bei der VM-Verschlüsselung

Die folgenden Aktionen werden in VMware Cloud Director 10.1 nicht unterstützt.

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

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

Identifizieren einer VM-Verschlüsselungsspeicherfunktion

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

Sie können alle Speicherfunktionen in der Spalte **Funktionen** unter **Ressourcen > vSphere-Ressourcen > Speicherrichtlinien** anzeigen. Diese Spalte zeigt die VM-Verschlüsselung, die Tag-basierte Zuordnung, vSAN und die IOPS-Begrenzung der Speicherfunktionen an. Um die vollständige Liste der Speicherfunktionen anzuzeigen, erweitern Sie die Zeile, indem Sie auf den Pfeil links neben dem Namen der Speicherrichtlinie klicken.

Sie können die Informationen zur Speicherfunktion auch auf der Registerkarte **Speicher** eines Organisations-VDC anzeigen.

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 in der oberen Navigationsleiste unter **Ressourcen 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 Datencenter 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 in der oberen Navigationsleiste unter **Ressourcen 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.

VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 VMware Cloud 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 VMware Cloud Director Mandantenportal*.

Konfigurieren von VDC-übergreifenden Netzwerken

Durch die Funktion für VDC-übergreifende Netzwerke können Organisationen mit virtuellen Datencentern, die durch mehrere vCenter Server-Instanzen gestützt werden, Layer-2-Netzwerke über bis zu vier virtuelle Datencenter ausweiten. VDC-übergreifende Netzwerke basieren auf Cross-vCenter NSX und können mehrere VMware Cloud Director-Sites umfassen.

VDC-übergreifendes Netzwerk erfordert NSX Data Center for vSphere.

Mit VDC-übergreifenden Netzwerken können Organisationen bis zu vier virtuelle Datencenter gruppieren und Ausgänge sowie ausgeweitete Layer-2-Netzwerke in jeder Gruppe konfigurieren.

Die teilnehmenden virtuellen Organisations-Datencenter können zu unterschiedlichen VMware Cloud Director-Sites gehören. Weitere Informationen finden Sie im [Konfigurieren und Verwalten von Bereitstellungen mit mehreren Standorten](#).

Organisationen können mithilfe von VDC-übergreifenden Netzwerken Hochverfügbarkeitslösungen oder verteilte Systemarchitekturen implementieren, in denen eine Anwendung über mehrere virtuelle Datencenter oder Sites verteilt werden kann.

Der **Systemadministrator** muss für jedes virtuelle Datencenter die zugrunde liegende Cross-vCenter NSX-Umgebung und die VMware Cloud Director-Server konfigurieren sowie VDC-übergreifende Netzwerke aktivieren.

- 1 Konfigurieren Sie eine der NSX Manager-Instanzen als primäre NSX Manager-Instanz. Siehe *Installationshandbuch zu Cross-vCenter NSX*.
 - a Stellen Sie den NSX-Cluster auf der primären NSX Manager-Instanz bereit.
 - b Bereiten Sie die ESXi-Hosts auf der primären NSX Manager-Instanz vor.
 - c Konfigurieren Sie VXLAN auf der primären NSX Manager-Instanz.
 - d Weisen Sie der NSX Manager-Instanz die primäre Rolle zu.
 - e Erstellen Sie einen Pool für die Segment-IP-Adresse für die globale Transportzone.

- f Fügen Sie eine globale Transportzone hinzu.
- 2 Konfigurieren Sie die restlichen NSX Manager-Instanzen als sekundäre NSX Manager-Instanzen. Siehe *Installationshandbuch zu Cross-vCenter NSX*.
 - a Bereiten Sie die ESXi-Hosts auf jeder sekundären NSX Manager-Instanz vor.
 - b Konfigurieren Sie VXLAN auf jeder sekundären NSX Manager-Instanz.
 - c Weisen Sie jeder NSX Manager-Instanz die sekundäre Rolle zu.
 - d Verbinden Sie die ESXi-Cluster mit der globalen Transportzone.
- 3 Konfigurieren Sie die Eigenschaften der Steuerungs-VM für jede NSX Manager-Instanz. Weitere Informationen finden Sie im [Bearbeiten der NSX Manager-Einstellungen](#).
- 4 Erstellen Sie mithilfe einer globalen Transportzone aus jeder vCenter Server-Instanz einen durch VXLAN gestützten Netzwerkpool. Weitere Informationen finden Sie unter [Erstellen eines Netzwerkpools, der von einer NSX Data Center for vSphere-Transportzone gestützt wird](#).

Hinweis Für Multisite-Bereitstellungen müssen Sie einen durch VXLAN gestützten Netzwerkpool an jeder VMware Cloud Director-Site erstellen.

- 5 Aktivieren Sie VDC-übergreifende Netzwerke auf jedem Organisations-VDC. Weitere Informationen finden Sie im [Bearbeiten der Netzwerkeinstellungen eines Organisations-VDCs](#).
- 6 Wenn die Organisation über virtuelle Datacenter an mehreren Sites verfügt, stellen Sie sicher, dass an den verschiedenen VMware Cloud Director-Sites unterschiedliche Installations-IDs verwendet werden. Wenn VMware Cloud Director-Sites vorhanden sind, die mit derselben Installations-ID konfiguriert sind, finden Sie weitere Informationen im Kapitel [Erneutes Erzeugen von MAC-Adressen für ausgeweitete Multisite-Netzwerke](#) im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

Der **Organisationsadministrator** kann jetzt Datacenter-Gruppen, Ausgänge und ausgeweitete Netzwerke erstellen und konfigurieren. Informationen zur Verwaltung von VDC-übergreifenden Netzwerken finden Sie im *Handbuch für das VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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.

VMware Cloud 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 NSX Data Center for vSphere-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.

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

Verfahren

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

- 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: a Wählen Sie das Dienstprotokoll aus. b Geben Sie die Portnummern für die Quell- und Zielports ein oder Beliebige an und klicken Sie auf Behalten .
Auf das Plussymbol (+) klicken	Wählen Sie einen vordefinierten Dienst oder eine vordefinierte Dienstgruppe aus oder definieren Sie einen neuen Dienst oder eine neue Dienstgruppe: a Wählen Sie ein oder mehrere Objekte aus und fügen Sie sie dem Filter hinzu. b 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.

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

Wichtig IP-Adressgruppen (IP Sets), MAC-Adressgruppen (MAC Sets) und Sicherheitsgruppen, die entweder IP Sets oder MAC Sets enthalten, sind keine gültigen Eingabeparameter.


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

Bearbeiten einer Distributed Firewall-Regel

Verwenden Sie in einer VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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 VMware Cloud Director-Umgebung bietet die Möglichkeit, Sätze und Gruppen von bestimmten Entitäten zu definieren, die Sie dann beim Angeben weiterer netzwerkbezogener Konfigurationen verwenden können, z. B. in Firewallregeln.

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

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

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 Dienstinstellungen 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	<ul style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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 Diensteeinstellungen eines Edge-Gateways im Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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-Zielfatencenter 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 Diensteeinstellungen 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 in der oberen Navigationsleiste unter Ressourcen 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 Diensteeinstellungen eines Edge-Gateways im Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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 Diensteeinstellungen 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 in der oberen Navigationsleiste unter Ressourcen 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 Diensteeinstellungen eines Edge-Gateways im Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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 **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 Diensteeinstellungen 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 in der oberen Navigationsleiste unter Ressourcen 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 in der oberen Navigationsleiste unter Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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.




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 in der oberen Navigationsleiste unter **Ressourcen 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“.
- 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**.
 - 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.
 - 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“.
- 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**.
 - 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.
 - 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

- Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- Klicken Sie im linken Bereich auf **Organisations-VDCs**.
- Klicken Sie auf das Optionsfeld neben dem gewünschten virtuellen Organisations-Datencenter und klicken Sie auf **Firewall verwalten**.
- Klicken Sie auf die Registerkarte **Gruppierungsobjekte > Sicherheitsgruppen**.
- Wählen Sie die Sicherheitsgruppe aus, die Sie löschen möchten.
- Klicken Sie auf die Schaltfläche **Löschen** ()
- 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 in der oberen Navigationsleiste unter **Ressourcen 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 Schaltfläche **Erstellen** () und geben Sie einen Namen für das Sicherheitstag ein.
- 5 (Optional) Geben Sie eine Beschreibung für das Sicherheitstag ein.

- 6 (Optional) Weisen Sie das Sicherheitstag einer virtuellen Maschine oder einer Gruppe virtueller Maschinen zu.

Im Dropdown-Menü **Objekte dieses Typs durchsuchen** ist standardmäßig **Virtuelle Maschinen** ausgewählt.

- a Wählen Sie im linken Bereich eine virtuelle Maschine aus.
- b Klicken Sie auf den rechten Pfeil, um das Sicherheitstag der ausgewählten virtuellen Maschine zuzuweisen.

Die virtuelle Maschine wechselt in den rechten Bereich und wird dem Sicherheitstag zugewiesen.

- 7 Wenn Sie mit der Zuweisung des Tags zu den ausgewählten virtuellen Maschinen fertig sind, klicken Sie auf **Behalten**.

Ergebnisse

Das Sicherheitstag wird erstellt und wird den ausgewählten virtuellen Maschinen zugewiesen, wenn Sie diese Option ausgewählt haben.

Nächste Schritte


Sicherheitstags wurden für die Verwendung mit einer Sicherheitsgruppe konzipiert. Weitere Informationen zum Erstellen von Sicherheitsgruppen finden Sie unter [Erstellen einer Sicherheitsgruppe](#).

Ändern der Zuweisung von Sicherheitstags

Nachdem Sie ein Sicherheitstag erstellt haben, können Sie es manuell virtuellen Maschinen zuweisen. Sie können ein Sicherheitstag auch bearbeiten, um es von den virtuellen Maschinen zu entfernen, denen Sie es bereits zugewiesen haben.

Wenn Sie Sicherheitstags erstellt haben, können Sie sie virtuellen Maschinen zuweisen. Sie können Sicherheitstags zum Gruppieren von virtuellen Maschinen verwenden, um Firewallregeln zu schreiben. So können Sie z. B. einer Gruppe von virtuellen Maschinen mit sehr vertraulichen Daten ein Sicherheitstag zuweisen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 in der Liste der Sicherheitstags das Sicherheitstag aus, das Sie bearbeiten möchten, und klicken Sie auf die Schaltfläche **Bearbeiten** ()

- 5 Wählen Sie im linken Fensterbereich virtuelle Maschinen aus und weisen Sie ihnen das Sicherheitstag zu, indem Sie auf den Rechtspfeil klicken.
Den virtuellen Maschinen im rechten Fensterbereich wird das Sicherheitstag zugewiesen.
- 6 Wählen Sie im rechten Fensterbereich virtuelle Maschinen aus und entfernen Sie das Tag von ihnen, indem Sie auf den Linkspfeil klicken.
Den virtuellen Maschinen im linken Fensterbereich ist kein Sicherheitstag zugewiesen.
- 7 Wenn Sie alle gewünschten Änderungen hinzugefügt haben, klicken Sie auf **Behalten**.

Ergebnisse

Das Sicherheitstag wird den ausgewählten virtuellen Maschinen zugewiesen.

Nächste Schritte

Sicherheitstags wurden für die Verwendung mit einer Sicherheitsgruppe konzipiert. Weitere Informationen zum Erstellen von Sicherheitsgruppen finden Sie unter [Erstellen einer Sicherheitsgruppe](#).

Anzeigen von angewendeten Sicherheitstags

Sie können die Sicherheitstags anzeigen, die auf virtuelle Maschinen in Ihrer Umgebung angewendet wurden. Sie können auch die Sicherheitstags anzeigen, die auf Sicherheitsgruppen in Ihrer Umgebung angewendet werden.

Voraussetzungen

Ein Sicherheitstag muss erstellt und auf eine virtuelle Maschine oder auf eine Sicherheitsgruppe angewendet worden sein.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 aus der Liste der Sicherheitstags das Sicherheitstag aus, das Sie bearbeiten möchten.
- 5 Klicken Sie auf die Schaltfläche **Bearbeiten** ()
- 6 Bearbeiten Sie den Namen und die Beschreibung der Sicherheitstags.
- 7 Weisen Sie das Tag den virtuellen Maschinen zu, die Sie auswählen, oder entfernen Sie die Zuweisung von den ausgewählten virtuellen Maschinen.
- 8 Klicken Sie zum Speichern der Änderungen auf **Behalten**.

Nächste Schritte


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

Löschen eines Sicherheitstags

Sie können ein benutzerdefiniertes Sicherheitstag löschen.

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

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 aus der Liste der Sicherheitstags das Sicherheitstag aus, das Sie löschen möchten.
- 5 Klicken Sie auf die Schaltfläche **Löschen** ().
- 6 Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Ergebnisse

Das Sicherheitstag wird gelöscht.

Nächste Schritte

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

Verwalten von NSX Data Center for vSphere-Edge-Gateways

7

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

Ab VMware Cloud 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 NSX Data Center for vSphere-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 VMware Cloud 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 NSX Data Center for vSphere-Edge-Clustern](#)
- [Hinzufügen eines NSX Data Center for vSphere-Edge-Gateways](#)
- [Konfigurieren von NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Clustern

Um die Computing-Arbeitslasten von den Netzwerkarbeitslasten zu isolieren, unterstützt VMware Cloud Director das Edge-Cluster-Objekt. 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.

Ab 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 VMware Cloud 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 `EdgeClusters`-Methoden von VMware Cloud Director OpenAPI verwenden. Weitere Informationen finden Sie unter *Erste Schritte mit VMware Cloud Director 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 `VdcNetworkProfile`-Methoden von VMware Cloud Director OpenAPI verwenden. Weitere Informationen finden Sie unter *Erste Schritte mit VMware Cloud Director 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 NSX Data Center for vSphere-Edge-Gateways

Ein NSX Data Center for vSphere-Edge-Gateway verbindet ein geroutetes VDC-Organisationsnetzwerk mit anderen Netzwerken und kann Dienste wie Lastausgleich, Netzwerkadressübersetzung (NAT) und eine Firewall bereitstellen.

Ab VMware Cloud Director 9.7 werden NSX Data Center for vSphere-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 NSX Data Center for vSphere-Edge-Gateways finden Sie unter *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 NSX Data Center for vSphere-Edge-Clustern](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways** und dann auf **Neu**.
- 3 Wählen Sie das von NSX-V gestützte Organisations-VDC aus, 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 Konfiguration des Edge-Gateways für Ihre Systemressourcen aus und klicken Sie auf **Weiter**.

Konfiguration	Beschreibung
Kompakt	Benötigt weniger Arbeitsspeicher- und Rechenressourcen.
Groß	Bietet größere Kapazität und höhere Leistung als die Konfiguration „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**.
 - Klicken Sie auf das Optionsfeld neben dem Namen des externen Zielnetzwerks und auf das Optionsfeld neben der IP-Zieladresse.
 - (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 eingeben.
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 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. VMware Cloud Director konfiguriert die entsprechende Gateway-Schnittstelle mit den sekundären Adressen automatisch während des Zuteilungsvorgangs. Wenn eine oder mehrere der IP-Adressen außerhalb von VMware Cloud 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 NSX Data Center for vSphere-Edge-Gateway-Diensten

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

Verwalten einer NSX Data Center for vSphere-Edge-Gateway-Firewall

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

Informationen zum Schützen des Datenverkehrs zwischen virtuellen Maschinen in einem virtuellen Organisations-Datencenter finden Sie unter [Verwalten der 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 NSX Data Center for vSphere Edge-Gateways

Sie können die Registerkarte **Firewall** des Edge-Gateways verwenden, um Firewallregeln für das betreffende Edge-Gateway hinzuzufügen. Sie können mehrere NSX Edge-Schnittstellen und mehrere IP-Adressgruppen als Quelle und Ziel für diese Firewallregeln hinzufügen.

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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:

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

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

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

9 Klicken Sie auf **Änderungen speichern**.

Der Speichervorgang kann eine Minute dauern.

Ändern der Firewallregeln für NSX Data Center for vSphere-Edge-Gateways

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere-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 in der oberen Navigationsleiste unter **Ressourcen 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 von DHCP für NSX Data Center for vSphere-Edge-Gateways

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

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

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

- Überwacht die interne Schnittstelle des Edge-Gateways zum Zweck der DHCP-Erkennung.
- Verwendet die IP-Adresse der internen Schnittstelle des Edge-Gateways als standardmäßige Gateway-Adresse für alle Clients.
- Die Broadcast- und Subnetzmaskenwerte der internen Schnittstelle werden für das Containernetzwerk verwendet.

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

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

Hinweis Wenn die DNS-Einstellungen eines für DHCP 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 NSX Data Center for vSphere-Edge-Gateways benötigten IP-Pools konfigurieren. DHCP automatisiert die Zuweisung von IP-Adressen zu virtuellen Maschinen, die mit VDC-Organisationsnetzwerken verbunden sind.

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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.

Option	Beschreibung
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

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

Hinzufügen von DHCP-Bindungen

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

Voraussetzungen

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

Verfahren

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

3 Klicken Sie auf **Änderungen speichern**.

Konfigurieren von DHCP-Relay für NSX Data Center for vSphere-Edge-Gateways

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

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

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

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

Hinweis

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

Angeben einer DHCP-Relay-Konfiguration für ein NSX Data Center for vSphere-Edge-Gateway

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

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


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


Voraussetzungen

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 VMware Cloud Director-Umgebung konfigurieren Sie die Regel immer aus der Perspektive des virtuellen Datencenters Ihrer Organisation. Eine SNAT-Regel übersetzt die IP-Quelladresse von Paketen, die von einem VDC-Organisationsnetzwerk an ein externes Netzwerk oder an ein anderes VDC-Organisationsnetzwerk gesendet werden. Eine DNAT-Regel übersetzt die IP-Adresse und optional den Port von Paketen, die von einem VDC-Organisationsnetzwerk empfangen werden und aus einem externen Netzwerk oder einem anderen VDC-Organisationsnetzwerk stammen.

Voraussetzungen

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 oder wählen Sie die zugeteilte IP-Adresse aus der Liste aus. 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.

Option	Beschreibung
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.
Quell-IP-Adresse	Wenn Sie möchten, dass die Regel nur für den Datenverkehr zu einer bestimmten Domäne angewendet wird, geben Sie eine IP-Adresse für diese Domäne oder einen IP-Adressbereich im CIDR-Format ein. Wenn Sie dieses Textfeld leer lassen, gilt die DNAT-Regel für alle IP-Adressen innerhalb des lokalen Subnetzes.
Quellport	(Optional) Geben Sie eine Portnummer für die Quelle ein.
Beschreibung	(Optional) Geben Sie eine aussagekräftige Beschreibung für die DNAT-Regel ein.
Aktiviert	Aktivieren Sie diese Option, um diese Regel zu aktivieren.
Protokollierung aktivieren	Aktivieren Sie diese Option, damit die Adressübersetzung dieser Regel protokolliert wird.

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

Option	Beschreibung
Angewendet auf	Wählen Sie die Schnittstelle aus, auf die die Regel angewendet werden soll.
Ursprüngliche(r) Quell-IP/Quellbereich	Geben Sie die ursprüngliche IP-Adresse oder den Bereich von IP-Adressen ein, der auf diese Regel angewendet werden soll, oder wählen Sie die zugewiesene IP-Adresse aus der Liste aus. Bei diesen Adressen handelt es sich um die IP-Adressen der virtuellen Maschinen, für die Sie die SNAT-Regel konfigurieren, damit diese Datenverkehr an das externe Netzwerk senden können.
Übersetzte(r) Quell-IP/Quellbereich	Geben Sie die erforderliche IP-Adresse ein. Bei dieser Adresse handelt es sich immer um die öffentliche IP-Adresse des Gateways, für das Sie die SNAT-Regel konfigurieren. Gibt die IP-Adresse an, in die Quelladressen (die virtuellen Maschinen) in ausgehenden Paketen übersetzt werden, wenn sie Datenverkehr an das externe Netzwerk senden.

Option	Beschreibung
Ziel-IP-Adresse	(Optional) Wenn Sie möchten, dass die Regel nur für den Datenverkehr zu einer bestimmten Domäne angewendet wird, geben Sie eine IP-Adresse für diese Domäne oder einen IP-Adressbereich im CIDR-Format ein. Wenn Sie dieses Textfeld leer lassen, gilt die SNAT-Regel für alle Ziele außerhalb des lokalen Subnetzes.
Zielport	(Optional) Geben Sie eine Portnummer für das Ziel ein.
Beschreibung	(Optional) Geben Sie eine aussagekräftige Beschreibung für die SNAT-Regel ein.
Aktiviert	Aktivieren Sie diese Option, um diese Regel zu aktivieren.
Protokollierung aktivieren	Aktivieren Sie diese Option, damit die Adressübersetzung dieser Regel protokolliert wird.

- 6 Klicken Sie auf **Behalten**, um die Regel der Tabelle auf dem Bildschirm hinzuzufügen.
- 7 Wiederholen Sie die Schritte, um weitere Regeln zu konfigurieren.
- 8 Klicken Sie auf **Änderungen speichern**, um die Regeln im System zu speichern.

Nächste Schritte

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

Konfiguration für erweitertes Routing

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

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

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

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

Angeben von Standard-Routing-Konfigurationen für das NSX Data Center for vSphere-Edge-Gateway

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 Plussymbol (+) verwenden, um eine neue ID einzugeben. Diese Router-ID ist die erste Uplink-IP-Adresse des Edge-Gateways, die Routen zum Kernel für dynamisches Routing überträgt.

- b Konfigurieren Sie die Protokollierung, indem Sie die Option **Protokollierung aktivieren** aktivieren und die Protokollierungsebene auswählen.

- c Klicken Sie auf **OK**.

6 Klicken Sie auf **Änderungen speichern**.

Nächste Schritte

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

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

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

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

Hinzufügen einer statischen Route


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

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

Voraussetzungen

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere Edge-Gateways](#).

Konfigurieren des OSPF-Protokolls

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

besteht im Austausch von Routing-Informationen zwischen Edge-Gateways in VMware Cloud Director.

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


Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere Edge-Gateways](#).

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

Konfigurieren des BGP-Protokolls

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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> <p>Vorsicht Eine Regel des Typs <code>Alle blockieren</code> wird am Ende der Filter erzwungen.</p> <p>Fügen Sie einen Filter zur Tabelle hinzu, indem Sie auf das Plussymbol (+) klicken und die Optionen konfigurieren. Klicken Sie auf Behalten, um jeden Filter zu speichern.</p> <ul style="list-style-type: none"> ■ Wählen Sie die Richtung aus, um anzugeben, ob Sie den Datenverkehr zu oder von einem Nachbarn filtern. ■ Wählen Sie die Aktion, um anzugeben, ob Sie Datenverkehr zulassen oder verweigern. ■ Geben Sie das Netzwerk an, das Sie zu oder von einem Nachbarn filtern möchten. Geben Sie <code>ANY</code> oder ein Netzwerk im CIDR-Format ein. ■ Geben Sie das IP-Präfix-GE und IP-Präfix-LE ein, um die Schlüsselwörter <code>le</code> und <code>ge</code> in der Liste der IP-Präfixe zu verwenden.

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

Nächste Schritte

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


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


Konfigurieren der Route Redistribution

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

die Route Redistribution mit protokollübergreifender Routenfreigabe konfigurieren. Sie können die Route Redistribution für ein NSX Data Center for vSphere-Edge-Gateway konfigurieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 > Route Redistribution**.
- 3 Verwenden Sie die Protokolloptionen, um die Protokolle zu aktivieren, für die Sie Route Redistribution aktivieren möchten.
- 4 Fügen Sie IP-Präfixe zur Tabelle auf dem Bildschirm hinzu.
 - a Klicken Sie auf die Schaltfläche **Hinzufügen** ().
 - b Geben Sie einen Namen und die IP-Adresse des Netzwerks im CIDR-Format ein.
 - c Klicken Sie auf **Behalten**.

- 5 Geben Sie Neuverteilungskriterien für jedes IP-Präfix an, indem Sie auf die Schaltfläche **Hinzufügen** () klicken, die Kriterien im Dialogfeld angeben und auf **Behalten** klicken.

Einträge in der Tabelle werden nacheinander verarbeitet. Mithilfe der Aufwärts- und Abwärtspfeile können Sie die Reihenfolge anpassen.

Option	Beschreibung
Präfixname	Wählen Sie ein bestimmtes IP-Präfix aus, um diese Kriterien darauf anzuwenden, oder wählen Sie Alle aus, um die Kriterien auf alle 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.

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

Der Lastausgleich für ein NSX Data Center for vSphere-Edge-Gateway wird in der externen Schnittstelle konfiguriert, da das Edge-Gateway den Lastausgleich für den eingehenden Datenverkehr vom externen Netzwerk durchführt. Wenn Sie virtuelle Server für den Lastausgleich konfigurieren, geben Sie eine der verfügbaren IP-Adressen an, über die Sie in Ihrem Organisations-VDC verfügen.

Strategien und Konzepte für den Lastausgleich

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

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

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

Virtueller Server

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

Serverpool

Gruppe von Back-End-Servern.

Serverpoolmitglied

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

Dienstüberwachung

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

Anwendungsprofil

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

Übersicht über die Einrichtung

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

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

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

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

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

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

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

Konfigurieren des Lastausgleichsdiensts

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 HTTP 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.

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 in der oberen Navigationsleiste unter **Ressourcen 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.
HTTP-Umleitungs-URL	(HTTP und HTTPS) Geben Sie die URL ein, an die der Datenverkehr, der an der Zieladresse ankommt, umgeleitet werden soll.

Option	Beschreibung
Persistenz	<p>Geben Sie einen Persistenzmechanismus für das Profil an.</p> <p>Persistenz verfolgt und speichert Sitzungsdaten, wie z. B. das spezifische Poolmitglied, das eine Clientanforderung bearbeitet hat. Dadurch wird sichergestellt, dass die Clientanforderungen während des Lebenszyklus einer Sitzung oder während nachfolgender Sitzungen demselben Poolmitglied zugeordnet werden. Zu den Optionen gehören:</p> <ul style="list-style-type: none"> ■ Quell-IP <p>Quell-IP-Persistenz verfolgt Sitzungen basierend auf der IP-Quelladresse. Wenn ein Client eine Verbindung zu einem virtuellen Server anfordert, der die Persistenz der Quelladressen-Affinität unterstützt, überprüft der Lastausgleichsdienst, ob dieser Client zuvor eine Verbindung hergestellt hat, und wenn ja, gibt er den Client an dasselbe Poolmitglied zurück.</p> ■ MSRDP <p>(Nur TCP) MSRDP-Persistenz (Microsoft Remote Desktop Protocol) behält persistente Sitzungen zwischen Windows-Clients und -Servern bei, die den RDP-Dienst (Remote Desktop Protocol) von Microsoft ausführen. Das empfohlene Szenario für die Aktivierung der MSRDP-Persistenz ist die Erstellung eines Lastausgleichspools, der aus Mitgliedern besteht, die ein Windows Server-Gastbetriebssystem ausführen, wobei alle Mitglieder zu einem Windows-Cluster gehören und an einem Windows-Sitzungsverzeichnis teilnehmen.</p> ■ SSL-Sitzungs-ID <p>Persistenz der SSL-Sitzungs-ID ist verfügbar, wenn Sie SSL-Passthrough aktivieren. Persistenz der SSL-Sitzungs-ID stellt sicher, dass wiederholte Verbindungen vom selben Client an denselben Server gesendet werden. Persistenz der SSL-Sitzungs-ID ermöglicht die Wiederaufnahme der SSL-Sitzung, wodurch die Verarbeitungszeit sowohl für den Client als auch für den Server gespeichert wird.</p>
Cookiename	<p>(HTTP und HTTPS) Wenn Sie Cookie als Mechanismus für die Persistenz angegeben haben, geben Sie den Cookienamen ein. Die Cookiepersistenz verwendet ein Cookie, um die Sitzung eindeutig zu identifizieren, wenn ein Client zum ersten Mal auf die Site zugreift. Der Lastausgleichsdienst verweist auf dieses Cookie, wenn die Verbindung nachfolgender Anforderungen in der Sitzung hergestellt wird, sodass sie alle an den gleichen virtuellen Server weitergeleitet werden.</p>

Option	Beschreibung
Modus	<p>Wählen Sie den Modus aus, mit dem das Cookie eingefügt werden soll. Die folgenden Modi werden unterstützt:</p> <ul style="list-style-type: none"> ■ Einfügen <p>Das Edge-Gateway sendet ein Cookie. Wenn der Server ein oder mehrere Cookies sendet, empfängt der Client ein zusätzliches Cookie (Server-Cookies und Edge-Gateway-Cookie). Wenn der Server keine Cookies sendet, empfängt der Client nur das Edge-Gateway-Cookie.</p> ■ Präfix <p>Wählen Sie diese Option aus, wenn Ihr Client nur ein Cookie unterstützt.</p> <p>Hinweis Alle Browser akzeptieren mehrere Cookies. Möglicherweise verfügen Sie jedoch über eine proprietäre Anwendung mit einem proprietären Client, der nur ein Cookie unterstützt. Der Webserver sendet wie üblich sein Cookie. Das Edge-Gateway fügt seine Cookieinformationen in den Server-Cookiewert ein (als Präfix). Diese hinzugefügten Cookieinformationen werden entfernt, wenn das Edge-Gateway sie an den Server sendet.</p> ■ App-Sitzung Für diese Option sendet der Server kein Cookie. Stattdessen sendet er die Informationen zur Benutzersitzung als URL. Beispiel: <code>http://example.com/admin/UpdateUserServlet;jsessionid=0I24B9ASD7BSSD</code>, wobei <code>jsessionid</code> die Benutzersitzungsinformationen bezeichnet und für die Persistenz verwendet wird. Es ist nicht möglich, die Persistenztabelle der App-Sitzung zur Fehlerbehebung anzuzeigen.
Läuft ab in (Sekunden)	<p>Geben Sie eine Zeitdauer in Sekunden ein, für die die Persistenz wirksam bleibt. Dies muss eine positive Ganzzahl im Bereich von 1-86400 sein.</p> <p>Hinweis Beim L7-Lastausgleich mit TCP-Quell-IP-Persistenz kommt es zu einer Zeitüberschreitung des Persistenzeintrags, wenn in einem bestimmten Zeitraum keine neuen TCP-Verbindungen hergestellt werden, selbst wenn die bestehenden Verbindungen noch aktiv sind.</p>
HTTP-Header 'X-Forwarded-For' einfügen	<p>(HTTP und HTTPS) Wählen Sie HTTP-Header 'X-Forwarded-For' einfügen für das Identifizieren der Ursprungs-IP-Adresse eines Clients aus, der eine Verbindung zu einem Webserver über den Lastausgleichsdienst herstellt.</p> <p>Hinweis Die Verwendung dieses Headers wird nicht unterstützt, wenn Sie SSL-Passthrough aktiviert haben.</p>
Pool-seitiges SSL aktivieren	<p>(Nur HTTPS) Wählen Sie Pool-seitiges SSL aktivieren aus, um das Zertifikat, die Zertifizierungsstellen oder die CRLs zu definieren, die zur Authentifizierung des Lastausgleichsdiensts über die Serverseite auf der Registerkarte „Pool-Zertifikate“ verwendet werden.</p>

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

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


Nächste Schritte

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

Erstellen einer Dienstüberwachung

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

Verfahren

- Öffnen Sie „Edge-Gateway-Dienste“.
 - Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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**.
- Navigieren Sie zu **Lastausgleichsdienst > Dienstüberwachung**.
- Klicken Sie auf die Schaltfläche **Erstellen** ().
- Geben Sie einen Namen für die Dienstüberwachung ein.

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

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

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. <i>sticky</i> ist wie <i>follow</i> , aber ist an die angegebene IP-Adresse gebunden. <i>stickyport</i> stellt sicher, dass sich der Port nicht ändert.
pagesize= <i>INTEGER:INTEGER</i>	Gibt die erforderlichen minimalen und maximalen Seitengrößen in Bytes an.
warning=DOUBLE	Gibt die Antwortzeit in Sekunden an, nach der ein Warnstatus gemeldet wird.
critical=DOUBLE	Gibt die Antwortzeit in Sekunden an, nach der ein kritischer Status gemeldet wird.

Tabelle 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 <i>any</i> verwendet.
quit= <i>STRING</i>	Sendet eine Zeichenfolge an den Server, um die Verbindung ordnungsgemäß zu schließen.
refuse=ok warn crit	Akzeptiert TCP-Zurückweisungen mit dem Status <i>ok</i> , <i>warn</i> oder <i>crit</i> . Verwendet standardmäßig den Status <i>crit</i> .
mismatch=ok warn crit	Akzeptiert erwartete Zeichenfolgenkonflikte mit dem Status <i>ok</i> , <i>warn</i> oder <i>crit</i> . Verwendet standardmäßig den Status <i>warn</i> .
jail	Blendet die Ausgabe im TCP-Socket aus.
maxbytes= <i>INTEGER</i>	Schließt die Verbindung, wenn mehr als die angegebene Anzahl an Byte empfangen werden.
delay= <i>INTEGER</i>	Wartet die angegebene Anzahl von Sekunden zwischen dem Senden der Zeichenfolge und dem Abrufen einer Antwort.
certificate= <i>INTEGER</i> [, <i>INTEGER</i>]	Gibt an, wie viele Tage ein Zertifikat mindestens gültig sein muss. Der erste Wert ist <i>#days</i> für „warning“, und der zweite Wert ist „critical“ (wenn nicht angegeben, -0).
ssl	Verwendet SSL für die Verbindung.
warning= <i>DOUBLE</i>	Gibt die Antwortzeit in Sekunden an, nach der ein Warnstatus gemeldet wird.
critical= <i>DOUBLE</i>	Gibt die Antwortzeit in Sekunden an, nach der ein kritischer Status gemeldet wird.


Nächste Schritte

Fügen Sie Serverpools für Ihren Lastausgleichsdienst hinzu. Weitere Informationen finden Sie unter [Hinzufügen eines Serverpools für den Lastausgleich](#).

Hinzufügen eines Serverpools für den Lastausgleich

Sie können einen Serverpool hinzufügen, um Back-End-Server flexibel und effizient zu verwalten und freizugeben. Ein Pool dient zur Verwaltung von Lastausgleichs-Verteilungsmethoden und ist mit einer Dienstüberwachung für Integritätsprüfungsparameter verbunden.


Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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.


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 in der oberen Navigationsleiste unter **Ressourcen 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>.

Nächste Schritte


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

Hinzufügen eines virtuellen Servers

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

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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.
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](#).

Nächste Schritte

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

Sicherer Zugriff mit virtuellen privaten Netzwerken

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

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

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

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

- Zwischen VDC-Organisationsnetzwerken in derselben Organisation
- Zwischen VDC-Organisationsnetzwerken in verschiedenen Organisationen
- Zwischen einem VDC-Organisationsnetzwerk und einem externen Netzwerk

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

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

Konfigurieren von SSL VPN-Plus

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

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

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

Voraussetzungen

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

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

Verfahren

1 Navigieren zum Bildschirm „SSL-VPN Plus“

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

2 Konfigurieren der SSL-VPN-Servereinstellungen

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

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

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

4 Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem NSX Data Center for vSphere-Edge-Gateway

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

5 Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem NSX Data Center for vSphere-Edge-Gateway

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

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

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

7 Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients

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

8 Bearbeiten der SSL VPN-Plus-Client-Konfiguration

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

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

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

Navigieren zum Bildschirm „SSL-VPN Plus“

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere-Edge-Gateway](#).

Konfigurieren der SSL-VPN-Servereinstellungen

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

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

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

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

Voraussetzungen

- Vergewissern Sie sich, dass die unter [Konfigurieren von SSL VPN-Plus](#) beschriebenen Voraussetzungen erfüllt sind.

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

Verfahren

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

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

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

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

Nächste Schritte

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

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

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

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


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

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

Voraussetzungen

- Navigieren zum Bildschirm „SSL-VPN Plus“.
- Konfigurieren der SSL-VPN-Servereinstellungen.

Verfahren

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

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

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

Ergebnisse

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

Nächste Schritte

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

Hinzufügen eines privaten Netzwerks für die Verwendung mit SSL VPN-Plus auf einem NSX Data Center for vSphere-Edge-Gateway

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


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

- SSL VPN-Plus ermöglicht Remotebenutzern den Zugriff auf private Netzwerke, basierend auf der Reihenfolge von oben nach unten, in der die IP-Pools in der Tabelle auf dem Bildschirm angezeigt werden. Nachdem Sie die privaten Netzwerke zur Tabelle auf dem Bildschirm hinzugefügt haben, können Sie ihre Positionen in der Tabelle mit den Pfeiltasten nach oben und unten anpassen.
- Wenn Sie für ein privates Netzwerk „TCP-Optimierung aktivieren“ auswählen, funktionieren möglicherweise einige Anwendungen wie z. B. FTP im aktiven Modus nicht innerhalb dieses Subnetzes. Zum Hinzufügen eines 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 NSX Data Center for vSphere-Edge-Gateway.

Verfahren

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

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

Option	Aktion
TCP-Optimierung aktivieren	<p>(Optional) Zur bestmöglichen Optimierung der Internetgeschwindigkeit müssen Sie, wenn Sie für das Senden des Datenverkehrs Über Tunnel auswählen, auch die Option TCP-Optimierung aktivieren auswählen.</p> <p>Durch die Auswahl dieser Option wird die Leistung von TCP-Paketen innerhalb des VPN-Tunnels verbessert, nicht jedoch die Leistung des UDP-Datenverkehrs.</p> <p>Bei einem konventionellen SSL-VPN-Tunnel mit Vollzugriff werden TCP/IP-Daten in einem zweiten TCP/IP-Stack zwecks Verschlüsselung über das Internet übertragen. Diese konventionelle Methode kapselt die Daten der Anwendungsschicht in zwei getrennte TCP-Streams. Wenn Paketverluste auftreten, was selbst unter optimalen Internetbedingungen passieren kann, kommt es zu einer Leistungsbeeinträchtigung mit der Bezeichnung „TCP-over-TCP Meltdown“. Bei Vorliegen von „TCP-over-TCP Meltdown“ korrigieren zwei TCP-Instrumente dasselbe einzelne Paket von IP-Daten, was den Netzwerkdurchsatz beeinträchtigt und Verbindungszeitüberschreitungen verursacht. Durch die Auswahl von TCP-Optimierung aktivieren wird verhindert, dass dieses TCP-over-TCP-Problem auftritt.</p> <hr/> <p>Hinweis Wenn Sie die TCP-Optimierung aktivieren, gilt Folgendes:</p> <ul style="list-style-type: none"> ■ Sie müssen die Portnummern eingeben, für die der Internetdatenverkehr optimiert werden soll. ■ Der SSL VPN-Server öffnet die TCP-Verbindung im Namen des VPN-Clients. Wenn der SSL-VPN-Server die TCP-Verbindung öffnet, wird die erste automatisch generierte Edge-Firewallregel angewendet, mit der alle über das Edge-Gateway geöffneten Verbindungen übergeben werden können. Nicht optimierter Datenverkehr wird durch die regulären Edge-Firewallregeln ausgewertet. Mit der standardmäßig generierten TCP-Regel werden beliebige Verbindungen zugelassen. <hr/>
Ports	<p>Wenn Sie Über Tunnel auswählen, geben Sie einen Bereich von Portnummern ein, die für den Remotebenutzer für den Zugriff auf interne Server geöffnet sein sollen, wie z. B. 20–21 für FTP-Datenverkehr und 80–81 für HTTP-Datenverkehr.</p> <p>Um Benutzern uneingeschränkten Zugriff zu gewähren, lassen Sie das Feld leer.</p> <hr/>
Status	Aktivieren oder deaktivieren Sie das private Netzwerk.

4 Klicken Sie auf **Änderungen speichern**, um die Konfiguration im System zu speichern.

Nächste Schritte

Fügen Sie einen Authentifizierungsserver hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem NSX Data Center for vSphere-Edge-Gateway](#).

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

Konfigurieren eines Authentifizierungsdiensts für SSL VPN-Plus auf einem NSX Data Center for vSphere-Edge-Gateway

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

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

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

Voraussetzungen

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

Verfahren

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

3 Konfigurieren Sie die Einstellungen des Authentifizierungsservers.

a (Optional) Aktivieren und konfigurieren Sie die Kennwortrichtlinie.

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

b (Optional) Aktivieren und konfigurieren Sie die Kontosperrungsrichtlinie.

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

c Aktivieren Sie im Abschnitt „Status“ diesen Authentifizierungsserver.

- d (Optional) Konfigurieren Sie die sekundäre Authentifizierung.

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

- e Klicken Sie auf **Behalten**.

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

Nächste Schritte

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

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

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


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

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

Voraussetzungen

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

Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** auf **Benutzer**.
- 2 Klicken Sie auf die Schaltfläche **Erstellen** ()

3 Konfigurieren Sie die folgenden Optionen für den Benutzer:

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

4 Wiederholen Sie die Schritte, um weitere Benutzer hinzuzufügen.

Nächste Schritte

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

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

Hinzufügen eines Installationspakets des SSL VPN-Plus-Clients

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


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


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

Voraussetzungen

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

Verfahren

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

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

- 4 Wählen Sie die Installationsparameter für Windows aus.

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

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

5 Klicken Sie auf **Behalten**.

Nächste Schritte

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

Bearbeiten der SSL VPN-Plus-Client-Konfiguration

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

Voraussetzungen

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

Verfahren

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

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

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

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

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

Voraussetzungen

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

Verfahren

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

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

Option	Beschreibung
Erzwungene Zeitüberschreitung aktivieren	Aktivieren Sie diese Einstellung, damit das System die Verbindung zu Remotebenutzern trennt, nachdem der Zeitraum verstrichen ist, den Sie im Feld Erzwungene Zeitüberschreitung angegeben haben.
Erzwungene Zeitüberschreitung	Geben Sie das Zeitlimit in Minuten ein. Dieses Feld wird angezeigt, wenn die Umschaltoption Erzwungene Zeitüberschreitung aktivieren aktiviert ist.

3 Klicken Sie auf **Änderungen speichern**.

Konfigurieren von IPsec-VPN

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

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

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

Die folgenden IPsec-VPN-Algorithmen werden unterstützt:

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

- DH-14 (Diffie-Hellman-Gruppe 14)

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

Wie im Thema *Überblick über IPsec-VPN* im *NSX-Administratorhandbuch* beschrieben, wird die maximale Anzahl unterstützter Tunnel auf einem Edge-Gateway von seiner konfigurierten Größe bestimmt: „Kompakt“, „Groß“, „Vollständig“, „Vollständig-4“.

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

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

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

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

Verfahren

1 Navigieren zum Bildschirm „IPsec-VPN“

Im Bildschirm **IPsec-VPN** können Sie den IPsec-VPN-Dienst für ein NSX Data Center for vSphere-Edge-Gateway konfigurieren.

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

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

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

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

4 Angeben der globalen IPsec-VPN-Einstellungen

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

Navigieren zum Bildschirm „IPsec-VPN“

Im Bildschirm **IPsec-VPN** können Sie den IPsec-VPN-Dienst für ein NSX Data Center for vSphere-Edge-Gateway konfigurieren.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere-Edge-Gateway](#).

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

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

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


- Die lokalen und Peer-Subnetze geben die Netzwerke an, mit denen das VPN eine Verbindung herstellt. Wenn Sie diese Subnetze in den Konfigurationen für IPsec-VPN-Sites angeben, geben Sie einen Netzwerkbereich und keine bestimmte IP-Adresse ein. Verwenden Sie das CIDR-Format, z. B. **192.168.99.0/24**.

- Die Peer-ID ist ein Bezeichner, der das Remotegerät eindeutig identifiziert, das die VPN-Verbindung beendet. In der Regel ist dies die öffentliche IP-Adresse. Bei Peers mit Zertifikatsauthentifizierung muss diese ID als Distinguished Name im Peer-Zertifikat festgelegt sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. NSX empfiehlt die Verwendung des FQDN oder der öffentlichen IP-Adresse des Remotegeräts als Peer-ID. Wenn die IP-Adresse des Peers aus einem anderen VDC-Organisationsnetzwerk stammt, geben Sie die native IP-Adresse des Peers ein. Wenn NAT für den Peer konfiguriert wurde, geben Sie die private IP-Adresse des Peers ein.
- Der Peer-Endpoint gibt die öffentliche IP-Adresse des Remotegeräts an, zu dem Sie eine Verbindung herstellen. Der Peer-Endpoint kann eine andere Adresse als die Peer-ID haben, wenn das Gateway des Peers nicht direkt über das Internet erreicht werden kann, sondern über ein anderes Gerät verbunden wird. Wenn NAT für den Peer konfiguriert wurde, geben Sie die öffentliche IP-Adresse ein, die das Gerät für NAT verwendet.
- Mit der lokalen ID wird die öffentliche IP-Adresse des Edge-Gateways des Organisations-VDCs angegeben. Sie können eine IP-Adresse oder einen Hostnamen zusammen mit der Firewall des Edge-Gateways eingeben.
- Der lokale Endpoint gibt das Netzwerk im Organisation-VDC an, in dem das Edge-Gateway überträgt. In der Regel stellt das externe Netzwerk des Edge-Gateways den lokalen Endpunkt dar.

Voraussetzungen

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

Verfahren

- 1 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>
Lokaler Endpoint	<p>Geben Sie das Netzwerk ein, das der lokale Endpoint für diese Verbindung ist.</p> <p>Der lokale Endpoint gibt das Netzwerk im Organisation-VDC an, in dem das Edge-Gateway überträgt. In der Regel ist das externe Netzwerk der lokale Endpoint.</p> <p>Wenn Sie unter Verwendung eines vorinstallierten Schlüssels einen IP-zu-IP-Tunnel hinzufügen, können die lokale ID und die ID des lokalen Endpoints identisch sein.</p>
Lokale Subnetze	<p>Geben Sie die Netzwerke ein, die von den Sites gemeinsam genutzt werden sollen, und verwenden Sie zur Eingabe mehrerer Subnetze ein Komma als Trennzeichen.</p> <p>Geben Sie einen Netzwerkbereich (keine spezifische IP-Adresse) ein, indem Sie die IP-Adresse im CIDR-Format eingeben, z. B. 192.168.99.0/24.</p>

Option	Aktion
Peer-ID	<p>Geben Sie eine Peer-ID ein, um die Peer-Site eindeutig zu identifizieren.</p> <p>Die Peer-ID ist ein Bezeichner, der das Remotegerät eindeutig identifiziert, das die VPN-Verbindung beendet. In der Regel ist dies die öffentliche IP-Adresse.</p> <p>Bei Peers mit Zertifikatsauthentifizierung muss die ID der Distinguished Name im Peer-Zertifikat sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. Eine Best Practice für NSX besteht darin, die öffentliche IP-Adresse oder den FQDN des Remotegeräts als Peer-ID zu verwenden.</p> <p>Wenn die IP-Adresse des Peers aus einem anderen VDC-Organisationsnetzwerk stammt, geben Sie die native IP-Adresse des Peers ein. Wenn NAT für den Peer konfiguriert wurde, geben Sie die private IP-Adresse des Peers ein.</p>
Peer-Endpoint	<p>Geben Sie die IP-Adresse oder den FQDN der Peer-Site ein, also die öffentliche Adresse des Remotegeräts, mit dem Sie eine Verbindung herstellen.</p> <p>Hinweis Wenn NAT für den Peer konfiguriert wurde, geben Sie die öffentliche IP-Adresse ein, die das Gerät für NAT verwendet.</p>
Peer-Subnetze	<p>Geben Sie das Remotenetzwerk ein, mit dem das VPN eine Verbindung herstellt, und verwenden Sie zur Eingabe mehrerer Subnetze ein Komma als Trennzeichen.</p> <p>Geben Sie einen Netzwerkbereich (keine spezifische IP-Adresse) ein, indem Sie die IP-Adresse im CIDR-Format eingeben, z. B. 192.168.99.0/24.</p>
Verschlüsselungsalgorithmus	<p>Wählen Sie den Typ des Verschlüsselungsalgorithmus im Dropdown-Menü aus.</p> <p>Hinweis Der Verschlüsselungstyp, den Sie auswählen, muss mit dem Verschlüsselungstyp übereinstimmen, der auf dem VPN-Gerät der Remote-Site konfiguriert ist.</p>
Authentifizierung	<p>Wählen Sie eine Authentifizierung aus. Zu den Optionen gehören:</p> <ul style="list-style-type: none"> ■ PSK <p>„Vorinstallierter Schlüssel“ (Pre-Shared Key, PSK) gibt an, dass der vom Edge-Gateway und der Peer-Site gemeinsam verwendete geheime Schlüssel für die Authentifizierung verwendet wird.</p> ■ Zertifikat <p>Die Authentifizierung mittels Zertifikat gibt an, dass das auf globaler Ebene definierte Zertifikat für die Authentifizierung verwendet wird. Diese Option ist nicht verfügbar, es sei denn, Sie haben auf der Registerkarte IPsec-VPN im Bildschirm Globale Konfiguration das globale Zertifikat konfiguriert.</p>
Gemeinsam verwendeten Schlüssel ändern	<p>(Optional) Wenn Sie die Einstellungen einer vorhandenen Verbindung aktualisieren, können Sie diese Option aktivieren, um das Feld Vorinstallierter Schlüssel zur Verfügung zu stellen und den gemeinsam verwendeten Schlüssel zu aktualisieren.</p>

Option	Aktion
Vorinstallierter Schlüssel	<p>Wenn Sie PSK als Authentifizierungstyp ausgewählt haben, geben Sie eine alphanumerische geheime Zeichenfolge ein. Diese Zeichenfolge darf maximal 128 Byte lang sein.</p> <p>Hinweis Der gemeinsam verwendete Schlüssel muss mit dem Schlüssel übereinstimmen, der auf dem VPN-Gerät der Remote-Site konfiguriert ist. Eine Best Practice besteht darin, einen gemeinsam verwendeten Schlüssel zu konfigurieren, wenn anonyme Sites eine Verbindung zum VPN-Dienst herstellen.</p>
Gemeinsam verwendeten Schlüssel anzeigen	(Optional) Aktivieren Sie diese Option, damit der gemeinsam verwendete Schlüssel auf dem Bildschirm angezeigt wird.
Diffie-Hellman-Gruppe	<p>Wählen Sie das kryptographische Schema aus, das es der Peer-Site und dem Edge-Gateway ermöglicht, über einen ungesicherten Kommunikationskanal einen gemeinsamen geheimen Schlüssel einzurichten.</p> <p>Hinweis Die Diffie-Hellman-Gruppe muss mit dem übereinstimmen, was auf dem VPN-Gerät der Remote-Site konfiguriert ist.</p>
Erweiterung	<p>(Optional) Geben Sie eine der folgenden Optionen ein:</p> <ul style="list-style-type: none"> ■ <code>securelocaltrafficbyip=IP-Adresse</code> zum Umleiten des lokalen Datenverkehrs des Edge-Gateways über den IPSec-VPN-Tunnel. <p>Dies ist der Standardwert.</p> <ul style="list-style-type: none"> ■ <code>passthroughSubnets=PeerSubnet/IPAddress</code>, um überlappende Subnetze zu unterstützen.

4 Klicken Sie auf **Behalten**.

Nächste Schritte

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

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

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

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

Voraussetzungen

- [Navigieren zum Bildschirm „IPsec-VPN“](#).
- Stellen Sie sicher, dass mindestens eine IPsec-VPN-Verbindung für dieses Edge-Gateway konfiguriert ist. Weitere Informationen finden Sie in den unter [Konfigurieren von IPsec-VPN-Site-Verbindungen für das NSX Data Center for vSphere-Edge-Gateway](#) beschriebenen Schritten.

Verfahren

- 1 Klicken Sie auf der Registerkarte „**IPsec-VPN**“ auf die Option **Aktivierungsstatus**.
- 2 Klicken Sie auf **IPSec-VPN-Dienststatus**, um den IPSec-VPN-Dienst zu aktivieren.
- 3 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

Der IPSec-VPN-Dienst des Edge-Gateways ist aktiv.

Angeben der globalen IPsec-VPN-Einstellungen

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

Für Sites, deren Peer-Endpoint auf **Beliebig** festgelegt ist, wird ein globaler vorinstallierter Schlüssel verwendet.

Voraussetzungen

- Wenn Sie die Zertifikatsauthentifizierung aktivieren möchten, stellen Sie sicher, dass auf dem Bildschirm **Zertifikate** mindestens ein Dienstzertifikat sowie entsprechende von einer Zertifizierungsstelle signierte Zertifikate angezeigt werden. Selbstsignierte Zertifikate können nicht für IPSec-VPNs verwendet werden. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).
- [Navigieren zum Bildschirm „IPsec-VPN“](#).

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere-Edge-Gateways in einer VMware Cloud Director-Umgebung unterstützen L2 VPN. Mit L2 VPN können Sie Ihr Organisations-VDC erweitern, indem Sie ermöglichen, dass virtuelle Maschinen Netzwerkkonnektivität unter Verwendung derselben IP-Adresse über geografische Grenzen hinweg beibehalten. Sie können den L2 VPN-Dienst auf einem Edge-Gateway konfigurieren.

NSX Data Center for vSphere stellt die L2 VPN-Funktionen eines Edge-Gateways bereit. Mit L2 VPN kann ein Tunnel zwischen zwei Sites konfiguriert werden. Virtuelle Maschinen verbleiben im selben Subnetz, obwohl sie zwischen diesen Sites verschoben werden. Daher können Sie das Organisations-VDC erweitern, indem Sie sein Netzwerk mit L2 VPN ausdehnen. Ein Edge-Gateway auf einer Site kann alle Dienste für virtuelle Maschinen auf der anderen Site bereitstellen.

Um den L2 VPN-Tunnel zu erstellen, konfigurieren Sie einen L2 VPN-Server und einen L2 VPN-Client. Wie im *Administratorhandbuch für NSX* beschrieben, ist der L2 VPN-Server das Ziel-Edge-Gateway und der L2 VPN-Client das Quell-Edge-Gateway. Nach dem Konfigurieren der L2 VPN-Einstellungen auf jedem Edge-Gateway müssen Sie den L2 VPN-Dienst sowohl auf dem Server als auch auf dem Client aktivieren.

Hinweis Auf den Edge-Gateways muss ein geroutetes VDC-Organisationsnetzwerk vorhanden sein, das als Teilschnittstelle erstellt wurde.

Verfahren

1 Navigieren zum Bildschirm „L2 VPN“

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

2 Konfigurieren des NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Server

Der L2 VPN-Server ist der Ziel-NSX Edge, mit dem der L2 VPN-Client eine Verbindung herstellen wird.

3 Konfigurieren des NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Client

Der L2 VPN-Client ist das quellseitige NSX Edge-Gateway, das die Kommunikation mit dem zielseitigen NSX Edge-Gateway, dem L2 VPN-Server, initiiert.

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

Wenn die erforderlichen L2 VPN-Einstellungen konfiguriert sind, können Sie den L2 VPN-Dienst auf dem Edge-Gateway aktivieren.

Navigieren zum Bildschirm „L2 VPN“

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Server](#).

Konfigurieren des NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Server

Der L2 VPN-Server ist der Ziel-NSX Edge, mit dem der L2 VPN-Client eine Verbindung herstellen wird.

Wie im *Administratorhandbuch für NSX* beschrieben, können Sie mehrere Peer-Sites mit diesem L2 VPN-Server verbinden.

Hinweis Änderungen an den Site-Konfigurationseinstellungen führen dazu, dass das Edge-Gateway alle vorhandenen Verbindungen trennt und erneut herstellt.

Voraussetzungen

- Stellen Sie sicher, dass das Edge-Gateway über ein geroutetes VDC-Organisationsnetzwerk verfügt, das als Teilschnittstelle auf dem Edge-Gateway konfiguriert ist.
- [Navigieren zum Bildschirm „L2 VPN“](#).
- Wenn Sie ein Dienstzertifikat an die L2 VPN-Verbindung binden möchten, vergewissern Sie sich, dass das Serverzertifikat bereits auf das Edge-Gateway hochgeladen wurde. Weitere Informationen finden Sie unter [Hinzufügen eines Dienstzertifikats zum Edge-Gateway](#).

- Sie müssen die Listener-IP des Servers, den Listener-Port, den Verschlüsselungsalgorithmus und mindestens eine Peer-Site konfiguriert haben, bevor Sie den L2 VPN-Dienst aktivieren können.

Verfahren

- 1 Wählen Sie auf der Registerkarte **L2 VPN** die Option **Server** für den L2 VPN-Modus aus.
- 2 Konfigurieren Sie auf der Registerkarte **Server – Global** die globalen Konfigurationsdetails des L2 VPN-Servers.

Option	Aktion
Listener-IP	Wählen Sie die primäre oder sekundäre IP-Adresse einer externen Schnittstelle des Edge-Gateways aus.
Listener-Port	Bearbeiten Sie den angezeigten Wert entsprechend den Anforderungen Ihrer Organisation. Der Standardport für den L2 VPN-Dienst ist 443.
Verschlüsselungsalgorithmus	Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation zwischen dem Server und dem Client aus.
Details des Dienstzertifikats	Klicken Sie auf Serverzertifikat ändern , um das Zertifikat auszuwählen, das an den L2 VPN-Server gebunden werden soll. Aktivieren Sie im Fenster Serverzertifikat ändern die Option Serverzertifikat überprüfen , wählen Sie in der Liste ein Serverzertifikat aus und klicken Sie auf OK .

- 3 Zur Konfiguration der Peer-Sites klicken Sie auf die Registerkarte **Server-Sites**.

- 4 Klicken Sie auf die Schaltfläche **Hinzufügen** ().

- 5 Konfigurieren Sie die Einstellungen für eine L2 VPN-Peer-Site.

Option	Aktion
Aktiviert	Aktivieren Sie diese Peer-Site.
Name	Geben Sie einen eindeutigen Namen für die Peer-Site ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung ein.
Benutzer-ID	Geben Sie den Benutzernamen und das Kennwort ein, mit denen die Peer-Site authentifiziert werden soll.
Kennwort	
Kennwort bestätigen	Die Benutzeranmeldedaten auf der Peer-Site müssen mit den Anmeldedaten auf der Clientseite identisch sein.

Option	Aktion
Ausgeweitete Schnittstellen	Wählen Sie mindestens eine Teilschnittstelle aus, die mit dem Client ausgeweitet werden soll. Die zur Auswahl stehenden Teilschnittstellen sind die VDC-Organisationsnetzwerke, die als Teilschnittstellen auf dem Edge-Gateway konfiguriert sind.
Adresse des Egress-Optimierungs-Gateways	(Optional) Wenn das Standard-Gateway für virtuelle Maschinen auf beiden Sites das gleiche ist, geben Sie die Gateway-IP-Adressen der Teilschnittstellen ein, für die der Datenverkehr lokal weitergeleitet oder über den L2 VPN-Tunnel blockiert werden soll.

6 Klicken Sie auf **Behalten**.

Nächste Schritte

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

Konfigurieren des NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Client

Der L2 VPN-Client ist das quellseitige NSX Edge-Gateway, das die Kommunikation mit dem zieleitigen 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.

Option	Beschreibung
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.

- (Optional) Um erweiterte Optionen zu konfigurieren, klicken Sie auf die Registerkarte **Client – Erweitert**.
- 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.

- Um die Validierung der Serverzertifizierung zu aktivieren, klicken Sie auf **Zertifikat der Zertifizierungsstelle ändern** und wählen Sie das entsprechende CA-Zertifikat aus.

Nächste Schritte

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

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

Wenn die erforderlichen L2 VPN-Einstellungen konfiguriert sind, können Sie den L2 VPN-Dienst auf dem Edge-Gateway aktivieren.

Hinweis Wenn HA bereits auf diesem Edge-Gateway konfiguriert ist, müssen Sie sicherstellen, dass für das Edge-Gateway mehr als eine interne Schnittstelle konfiguriert ist. Wenn nur eine einzige Schnittstelle vorhanden ist und diese bereits durch die HA-Funktion verwendet wurde, schlägt die L2 VPN-Konfiguration für dieselbe interne Schnittstelle fehl.

Voraussetzungen

- Wenn dieses Edge-Gateway ein L2 VPN-Server ist, d. h. das Ziel-NSX-Edge, müssen Sie sicherstellen, dass die erforderlichen L2 VPN-Servereinstellungen und mindestens eine L2 VPN-Peer-Site konfiguriert sind. Weitere Informationen finden Sie in den unter [Konfigurieren des NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Server](#) beschriebenen Schritten.
- Wenn dieses Edge-Gateway ein L2 VPN-Client ist, d. h. das Quell-NSX-Edge, müssen Sie sicherstellen, dass die L2 VPN-Clienteneinstellungen konfiguriert sind. Weitere Informationen finden Sie in den unter [Konfigurieren des NSX Data Center for vSphere-Edge-Gateways als L2 VPN-Client](#) beschriebenen Schritten.
- [Navigieren zum Bildschirm „L2 VPN“](#).

Verfahren

- 1 Klicken Sie auf der Registerkarte **L2 VPN** auf die Umschaltfläche **Aktivieren**.
- 2 Klicken Sie auf **Änderungen speichern**.

Ergebnisse

Der L2 VPN-Dienst des Edge-Gateways wird aktiv.

Nächste Schritte

Erstellen Sie NAT- oder Firewallregeln auf der mit dem Internet verbundenen Seite der Firewall, um die Verbindung des L2 VPN-Servers mit dem L2 VPN-Client zu aktivieren.

Entfernen der L2 VPN-Dienstkonfiguration von einem NSX Data Center for vSphere-Edge-Gateway

Sie können die vorhandene L2 VPN-Dienstkonfiguration des Edge-Gateways entfernen. 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 VMware Cloud Director-Umgebung bietet die Möglichkeit, Secure Sockets Layer (SSL)-Zertifikate mit den für Ihre Edge-Gateways konfigurierten Tunneln SSL VPN-Plus und IPsec-VPN zu verwenden.

Die Edge-Gateways in Ihrer VMware Cloud Director-Umgebung unterstützen selbstsignierte Zertifikate, von einer Zertifizierungsstelle (CA) signierte Zertifikate und Zertifikate, die von einer Zertifizierungsstelle generiert und signiert wurden. Sie können CSRs (Certificate Signing Requests, Zertifikatsignieranforderungen) generieren, die Zertifikate importieren, die importierten Zertifikate verwalten und CRLs (Certificate Revocation Lists, Zertifikatswiderrufslisten) erstellen.

Informationen zur Verwendung von Zertifikaten mit Ihrem Organisations-VDC

Sie können Zertifikate für die folgenden Netzwerkbereiche in Ihrem VMware Cloud Director-Organisations-VDC verwalten.

- IPsec-VPN-Tunnel zwischen einem VDC-Organisationsnetzwerk und einem Remotenetzwerk.
- SSL VPN-Plus-Verbindungen zwischen Remotebenutzern, privaten Netzwerken und Webressourcen in Ihrem Organisations-VDC.
- Ein L2 VPN-Tunnel zwischen zwei NSX-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 in der oberen Navigationsleiste unter **Ressourcen 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 **Zertifikate** auf **CSR**.
- 3 Konfigurieren Sie die folgenden Optionen für die CSR:

Option	Beschreibung
Allgemeiner Name	Geben Sie den vollqualifizierten Domännennamen (FQDN) für die Organisation ein, für die Sie das Zertifikat verwenden möchten (z. B. <code>www.example.com</code>). Schließen Sie das Präfix <code>http://</code> oder <code>https://</code> nicht in den allgemeinen Namen ein.
Organisationseinheit	Verwenden Sie dieses Feld, um zwischen Abteilungen innerhalb Ihrer VMware Cloud Director-Organisation zu unterscheiden, denen dieses Zertifikat zugeordnet ist. Zum Beispiel Konstruktion oder Vertrieb.
Name der Organisation	Geben Sie den Namen ein, unter dem Ihr Unternehmen gesetzlich eingetragen ist. Die aufgeführte Organisation muss der gesetzliche Registrant des Domännennamens in der Zertifikatsanforderung sein.
Ort	Geben Sie die Stadt oder den Ort an, in der bzw. dem Ihr Unternehmen gesetzlich eingetragen ist.
Bundesland oder Kanton	Geben Sie den vollständigen Namen (keine Abkürzungen) des Bundeslandes, des Kantons, der Region oder des Gebiets ein, in dem bzw. der Ihr Unternehmen gesetzlich eingetragen ist.
Ländercode	Geben Sie den Namen des Landes ein, in dem Ihr Unternehmen gesetzlich eingetragen ist.
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.

4 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 in der oberen Navigationsleiste unter **Ressourcen 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 Wählen Sie die CSR in der Tabelle auf dem Bildschirm aus, für die Sie das von der Zertifizierungsstelle signierte Zertifikat importieren.

3 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 in der oberen Navigationsleiste unter **Ressourcen 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 Wählen Sie in der Liste die CSR aus, die Sie für dieses selbstsignierte Zertifikat verwenden möchten, und klicken Sie auf **Selbstsignierte CSR**.
- 3 Geben Sie die Anzahl der Tage ein, die das selbstsignierte Zertifikat gültig ist.
- 4 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 in der oberen Navigationsleiste unter **Ressourcen 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 **CA-Zertifikat**.
- 3 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.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 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 in der oberen Navigationsleiste unter **Ressourcen 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 **CRL**.
- 3 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.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 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 in der oberen Navigationsleiste unter **Ressourcen 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 **Dienstzertifikat**.

3 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.

4 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.

5 Geben Sie die Passphrase des privaten Schlüssels ein und bestätigen Sie sie.**6** (Optional) Geben Sie eine Beschreibung ein.**7** 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 VMware Cloud Director-Umgebung bietet die Möglichkeit, Sätze und Gruppen von bestimmten Entitäten zu definieren, die Sie dann beim Angeben weiterer netzwerkbezogener Konfigurationen verwenden können, z. B. in Firewallregeln.

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

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

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 Dienstinstellungen 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	<ul style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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 Diensteeinstellungen eines Edge-Gateways im Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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-Zielfatencenter 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 Diensteeinstellungen 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	a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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 Diensteeinstellungen eines Edge-Gateways im Organisations-VDC	a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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-Zielfatencenter 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 Diensteeinstellungen 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 in der oberen Navigationsleiste unter Ressourcen 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 Diensteeinstellungen eines Edge-Gateways im Organisations-VDC	<ul style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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 **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 Diensteeinstellungen 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 in der oberen Navigationsleiste unter Ressourcen 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	<ol style="list-style-type: none"> a Wählen Sie in der oberen Navigationsleiste unter Ressourcen 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-Zieldatacenter 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.

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

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways** und klicken Sie auf den Namen des Ziel-Edge-Gateways.
- 3 Um die externen Netzwerke mit Informationen über ihre IP-Poolnutzung und Subnetze anzuzeigen, klicken Sie auf die Registerkarte **Externe Netzwerke > Netzwerke und Subnetze**.
- 4 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 VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen 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 NSX Data Center for vSphere-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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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.

Konfiguration	Beschreibung
Kompakt	Benötigt weniger Arbeitsspeicher- und Rechenressourcen.
Groß	Bietet größere Kapazität und höhere Leistung als die Konfiguration „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 in der oberen Navigationsleiste unter **Ressourcen 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 Umschloption **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 Umschloption **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 in der oberen Navigationsleiste unter **Ressourcen 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. VMware Cloud 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 VMware Cloud Director verwendet werden.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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.

Wenn Sie ein Edge-Gateway erneut bereitstellen, löscht VMware Cloud Director es und erstellt es mit den neuesten Konfigurationen neu.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 in der oberen Navigationsleiste unter **Ressourcen 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 VMware Cloud Director-Systemadministrator bereits einen Syslog-Server für die VMware Cloud Director-Umgebung konfiguriert hat, verwendet das System standardmäßig diesen Syslog-Server. Die zugehörige IP-Adresse wird im Bildschirm **Edge-Einstellungen** angezeigt.

3 Aktivieren Sie Protokollierung pro Funktion.

- Klicken Sie auf der Registerkarte **NAT** auf die Schaltfläche **DNAT-Regel** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert die Adressübersetzung.

- Klicken Sie auf der Registerkarte **NAT** auf die Schaltfläche **SNAT-Regel** und aktivieren Sie die Umschaltoption **Protokollierung aktivieren**.

Protokolliert die Adressübersetzung.

- Klicken Sie auf der Registerkarte **Routing** auf **Routing-Konfiguration** und aktivieren Sie unter „Konfiguration für dynamisches Routing“ die Umschaltoption **Protokollierung aktivieren**.

Protokolliert die dynamischen Routing-Aktivitäten. Im Dropdown-Menü **Protokollebene** können Sie die untere Grenze der zu protokollierenden 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 in der oberen Navigationsleiste unter **Ressourcen 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 den SSH-Zugriff auf dieses Edge-Gateway ein.
Kennwort	
Kennwort erneut eingeben	Standardmäßig lautet der SSH-Benutzername admin .
Ablauf des Kennworts	Geben Sie den Ablaufzeitraum für das Kennwort in Tagen ein.
Anmelde-Banner	Geben Sie den Text ein, der Benutzern angezeigt werden soll, wenn sie eine SSH-Verbindung mit dem Edge-Gateway beginnen.

- 4 Aktivieren Sie die Option **Aktiviert**.

Nächste Schritte

Konfigurieren Sie die entsprechenden NAT- oder Firewallregeln, um den SSH-Zugriff auf dieses Edge-Gateway zu ermöglichen.

Verwalten von NSX-T Data Center-Edge-Gateways

8

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

Dieses Kapitel enthält die folgenden Themen:

- [Dedizierte externe Netzwerke](#)
- [Hinzufügen eines NSX-T Data Center-Edge-Gateways](#)
- [Hinzufügen einer Firewallgruppe zu einem NSX-T-Edge-Gateway](#)
- [Hinzufügen einer Firewallregel für NSX-T-Edge-Gateways](#)
- [Hinzufügen einer SNAT- oder DNAT-Regel zu einem NSX-T-Edge-Gateway](#)
- [Konfigurieren eines DNS-Weiterleitungsdiensts auf einem NSX-T-Edge-Gateway](#)
- [Bearbeiten der IP-Zuweisungen für ein NSX-T-Edge-Gateway](#)
- [Schnelle IP-Zuweisung](#)
- [Erstellen von benutzerdefinierten Anwendungsportprofilen](#)
- [Richtlinienbasiertes IPSec-VPN für NSX-T Data Center-Edge-Gateways](#)
- [Konfigurieren dedizierter externer Netzwerkdienste](#)

Dedizierte externe Netzwerke

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

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

Ein logischer Tier-0-Router, der mit einem dedizierten externen Netzwerk verknüpft ist, ist Teil des Mandantennetzwerk-Stacks. Das externe Netzwerk wird als Teil der Routing-Domäne des VMware Cloud Director-Netzwerks betrachtet.

Durch die Reservierung eines externen Netzwerks für ein Edge-Gateway erhalten Mandanten zusätzliche Edge-Gateway-Dienste, wie z. B. die Verwaltung von Routenankündigungen und die BGP-Konfiguration (Border Gateway Protocol).

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

Sie können ein externes Netzwerk entweder während der Erstellung des Edge-Gateways oder zu einem späteren Zeitpunkt für ein NSX-T Data Center-Edge-Gateway reservieren, indem Sie die allgemeinen Einstellungen für das Edge-Gateway bearbeiten.

Hinzufügen eines NSX-T Data Center-Edge-Gateways

Ein NSX-T Data Center-Edge-Gateway verbindet ein geroutetes VDC-Organisationsnetzwerk mit anderen Netzwerken und kann Dienste wie Lastausgleich, Netzwerkadressübersetzung (NAT) und eine Firewall bereitstellen.

Voraussetzungen

Informationen zu den Systemanforderungen für die Bereitstellung eines NSX-T Data Center-Edge-Gateways finden Sie unter *NSX-T Data Center-Administratorhandbuch*.

Ab Version 10.1 unterstützt VMware Cloud Director eine dedizierte externe Netzwerkkonfiguration. Durch die Reservierung eines externen Netzwerks für ein Edge-Gateway erhalten Mandanten zusätzliche Edge-Gateway-Dienste, wie z. B. die Verwaltung von Routenankündigungen und die BGP-Konfiguration (Border Gateway Protocol). Weitere Informationen finden Sie unter [Dedizierte externe Netzwerke](#).

VMware Cloud Director 10.1 unterstützt die grundlegende Konfiguration von NSX-T Data Center-Edge-Clustern. Weitere Informationen zu NSX Edge-Clustern finden Sie im *NSX-T Data Center-Installationshandbuch*.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Klicken Sie im linken Bereich auf **Edge-Gateways**.
- 3 Klicken Sie auf **Neu**.
- 4 Wählen Sie das von NSX-T Data Center gestützte Organisations-VDC aus, in dem Sie das Edge-Gateway erstellen möchten, und klicken Sie auf **Weiter**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für das neue Edge-Gateway ein.
- 6 Zum Aktivieren von BGP und Routenankündigung für das Edge-Gateway aktivieren Sie die Option **Dediziertes externes Netzwerk** und klicken Sie auf **Weiter**.

- 7 Wählen Sie ein externes Netzwerk aus, mit denen das neue Edge-Gateway Verbindungen herstellen kann, und klicken Sie auf **Weiter**.

Wenn Sie die Option **Dediziertes externes Netzwerk** aktiviert haben, können andere Edge-Gateways nicht auf dieses externe Netzwerk zugreifen.

- 8 Wählen Sie einen Edge-Cluster aus, auf dem das Edge-Gateway bereitgestellt werden soll, und klicken Sie auf **Weiter**.

Wenn Sie die Edge-Gateway-Dienste auf einem anderen Edge-Cluster ausführen möchten als dem, der dem externen Netzwerk zugeordnet ist, können Sie das Edge-Gateway zur Verwendung eines anderen Edge-Clusters konfigurieren.

- Verwenden Sie den Edge-Cluster des externen Netzwerks, mit dem das Edge-Gateway verbunden ist.
- Wählen Sie aus einer Liste von Edge-Clustern aus, die für das Organisations-VDC verfügbar sind, auf dem Sie das Edge-Gateway bereitstellen.

- 9 (Optional) Bearbeiten Sie die IP-Adressen oder IP-Adressbereiche, die dem Edge-Gateway zugewiesen sind, und klicken Sie auf **Weiter**.

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

Hinzufügen einer Firewallgruppe zu einem NSX-T-Edge-Gateway

Um Firewallregeln zu erstellen und einem NSX-T-Edge-Gateway hinzuzufügen, müssen Sie zuerst die Firewallgruppen erstellen. Bei Firewallgruppen handelt es sich um Gruppen von Objekten, auf die die Firewallregeln angewendet werden. Durch die Kombination mehrerer Objekte in Firewallgruppen kann die Gesamtzahl der zu erstellenden Firewallregeln reduziert werden.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 das NSX-T-Edge-Gateway und dann auf **Sicherheit**.
- 3 Klicken Sie auf die Registerkarte **Gruppen** und dann auf **Neu**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für die Firewallgruppe ein.
- 5 Geben Sie eine IP-Adresse oder einen IP-Adressbereich für die virtuellen Maschinen ein, die in der Gruppe enthalten sind, und klicken Sie auf **Hinzufügen**.
- 6 Um die Firewallgruppe zu speichern, klicken Sie auf **Speichern**.

Ergebnisse

Sie haben eine Firewallgruppe erstellt und dem NSX-T Edge-Gateway hinzugefügt.

Nächste Schritte

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

Hinzufügen einer Firewallregel für NSX-T-Edge-Gateways

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

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 das Edge-Gateway und dann auf **Dienste**.
- 3 Falls der Bildschirm **Firewall** noch nicht angezeigt wird, klicken Sie auf die Registerkarte **Firewall**.
- 4 Klicken Sie auf **Regeln bearbeiten**.
- 5 Wählen Sie eine Firewallregel aus und klicken Sie auf die Schaltfläche **Darüber hinzufügen**.
Über der ausgewählten Regel wird eine Zeile für die neue Regel hinzugefügt.
- 6 Konfigurieren Sie die Firewallregel.

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

Option	Beschreibung
Ziel	<p>Wählen Sie eine Option aus und klicken Sie auf Beibehalten.</p> <ul style="list-style-type: none"> ■ Um Datenverkehr zu einer beliebigen Zieladresse zuzulassen oder zu verweigern, aktivieren Sie die Umschaltoption Beliebiges Ziel. ■ Um Datenverkehr von bestimmten Firewallgruppen zuzulassen oder zu verweigern, wählen Sie die Firewallgruppen aus der Liste aus.
Aktion	<p>Wählen Sie im Dropdown-Menü Aktion eine Option aus.</p> <ul style="list-style-type: none"> ■ Wählen Sie Annehmen aus, um Datenverkehr von oder zu den angegebenen Quellen, Zielen und Diensten zuzulassen. ■ Wählen Sie Verweigern aus, um Datenverkehr von oder zu den angegebenen Quellen, Zielen und Diensten zu blockieren.
IP-Protokoll	Wählen Sie aus, ob die Regel auf IPv4- oder IPv6-Datenverkehr angewendet werden soll.
Richtung	Wählen Sie die Datenverkehrsrichtung aus, auf die die Regel angewendet werden soll.
Protokollierung aktivieren	Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung aktivieren .

7 Klicken Sie auf **Speichern**.

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

Ergebnisse

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

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

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

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

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

Eine Regel des Typs KEINE SNAT verhindert die Übersetzung der internen IP-Adresse von Paketen, die aus einem VDC-Organisationsnetzwerk an ein externes Netzwerk oder an ein anderes VDC-Organisationsnetzwerk gesendet werden.

Eine DNAT-Regel übersetzt die IP-Adresse und optional den Port von Paketen, die von einem VDC-Organisationsnetzwerk empfangen werden und aus einem externen Netzwerk oder einem anderen VDC-Organisationsnetzwerk stammen.

Eine Regel des Typs KEINE DNAT verhindert die Übersetzung der externen IP-Adresse von Paketen, die ein VDC-Organisationsnetzwerk von einem externen Netzwerk oder einem anderen VDC-Organisationsnetzwerk empfängt.

VMware Cloud Director unterstützt die automatische Routenneuverteilung, wenn Sie NAT-Dienste auf einem NSX-T Data Center-Edge-Gateway verwenden.

Voraussetzungen

Die öffentliche IP-Adresse muss bereits der Edge-Gateway-Schnittstelle, für die Sie die Regel hinzufügen möchten, hinzugefügt worden sein.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 das Edge-Gateway und dann auf **NAT**.
- 3 Klicken Sie auf **Neu**, um eine Regel hinzuzufügen.
- 4 Konfigurieren Sie eine SNAT- oder KEINE SNAT-Regel (von innen nach außen).

Option	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Regel ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.
Zustand	Um die Regel bei der Erstellung zu aktivieren, aktivieren Sie die Umschaltoption Zustand .
Schnittstellentyp	Wählen Sie im Dropdown-Menü SNAT oder KEINE SNAT aus.
Externe IP	<p>Abhängig vom Typ der von Ihnen erstellten Regel wählen Sie eine der Optionen aus.</p> <ul style="list-style-type: none"> ■ Wenn Sie eine SNAT-Regel erstellen, geben Sie die öffentliche IP-Adresse des Edge-Gateways ein, für das Sie die SNAT-Regel konfigurieren. ■ Wenn Sie eine Regel des Typs KEINE SNAT erstellen, lassen Sie das Textfeld leer.
Interne IP	Geben Sie die IP-Adresse oder einen IP-Adressbereich der virtuellen Maschinen ein, für die Sie SNAT konfigurieren, damit Datenverkehr an das externe Netzwerk gesendet werden kann.

Option	Beschreibung
Ziel-IP	(Optional) Wenn Sie möchten, dass die Regel nur für den Datenverkehr zu einer bestimmten Domäne angewendet wird, geben Sie eine IP-Adresse für diese Domäne oder einen IP-Adressbereich im CIDR-Format ein. Wenn Sie dieses Textfeld leer lassen, gilt die SNAT-Regel für alle Ziele außerhalb des lokalen Subnetzes.
Protokollierung	Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung .

5 Konfigurieren Sie eine DNAT- oder KEINE DNAT-Regel (von außen nach innen).

Option	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen für die Regel ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.
Zustand	Um die Regel bei der Erstellung zu aktivieren, verwenden Sie die Umschaltoption Zustand .
Schnittstellentyp	Wählen Sie im Dropdown-Menü DNAT oder KEINE DNAT aus.
Externe IP	Geben Sie die öffentliche IP-Adresse des Edge-Gateways ein, für die Sie die DNAT-Regel konfigurieren. Die eingegebenen IP-Adressen müssen zum unterzugewiesenen IP-Bereich des Edge-Gateways gehören.
Anwendung	(Optional) Wählen Sie ein spezifisches Anwendungsportprofil aus, auf das die Regel angewendet werden soll. Das Anwendungsportprofil enthält einen Port und ein Protokoll, das der eingehende Datenverkehr auf dem Edge-Gateway verwendet, um eine Verbindung mit dem internen Netzwerk herzustellen.
Interne IP	Abhängig vom Typ der von Ihnen erstellten Regel wählen Sie eine der Optionen aus. <ul style="list-style-type: none"> ■ Wenn Sie eine DNAT-Regel erstellen, geben Sie die IP-Adresse oder einen IP-Adressbereich der virtuellen Maschinen ein, für die Sie DNAT konfigurieren, damit Datenverkehr vom externen Netzwerk empfangen werden kann. ■ Wenn Sie eine Regel des Typs KEINE DNAT erstellen, lassen Sie das Textfeld leer.
Interner Port	(Optional) Wählen Sie den Port oder Portbereich aus, in den die DNAT-Regel die Übersetzung für die auf den virtuellen Maschinen eingehenden Pakete vornimmt.
Protokollierung	Damit die von dieser Regel durchgeführte Adressübersetzung protokolliert wird, aktivieren Sie die Umschaltoption Protokollierung .

6 Klicken Sie auf **Speichern**.

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

Konfigurieren eines DNS-Weiterleitungsdiensts auf einem NSX-T-Edge-Gateway

Konfigurieren Sie zur Weiterleitung von DNS-Abfragen an externe DNS-Server eine DNS-Weiterleitung.

Im Rahmen der Konfiguration des DNS-Weiterleitungsdiensts können Sie auch bedingte Weiterleitungszonen hinzufügen. Eine bedingte Weiterleitungszone wird als Liste mit bis zu fünf FQDN-DNS-Zonen konfiguriert. Wenn eine DNS-Abfrage mit einem Domännennamen aus dieser Liste übereinstimmt, wird die Abfrage von der entsprechenden Weiterleitungszone an die Server weitergeleitet.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 das Edge-Gateway und dann auf **Dienste**.
- 3 Klicken Sie auf **DNS** und dann im Abschnitt **DNS-Weiterleitung** auf **Bearbeiten**.
- 4 Um den DNS-Weiterleitungsdienst zu aktivieren, verwenden Sie die Umschaltoption **Zustand**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für die standardmäßige DNS-Zone ein.
- 6 Geben Sie eine oder mehrere, durch Kommas getrennte IP-Adressen für den Upstream-Server ein.
- 7 Klicken Sie auf **Speichern**.
- 8 (Optional) Fügen Sie eine bedingte Weiterleitungszone hinzu.
 - a Klicken Sie im Abschnitt **Bedingte Weiterleitungszone** auf **Hinzufügen**.
 - b Geben Sie einen Namen für die Weiterleitungszone ein.
 - c Geben Sie eine oder mehrere, durch Kommas getrennte IP-Adressen für den Upstream-Server ein.
 - d Geben Sie einen oder mehrere, durch Kommas getrennte Domännennamen ein und klicken Sie auf **Speichern**.

Bearbeiten der IP-Zuweisungen für ein NSX-T-Edge-Gateway

Sie können einem Edge-Gateway mehrere IP-Adressen eines externen Netzwerks zuweisen.

Verfahren

1 Öffnen Sie „Edge-Gateway-Dienste“.

- a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 das Edge-Gateway und dann auf **IP-Zuweisungen**.

In den IP-Verwaltungstabellen können Sie die IP-Adressen sehen, die dem Edge-Gateway zugewiesen sind, sowie die IP-Adressen, die derzeit vom Edge-Gateway verwendet werden.

3 Klicken Sie im Abschnitt **Zugewiesene IPs** auf **IP-Verwaltung**.

In der Tabelle **IP-Verwaltung** können Sie die IP-Nutzung für jedes der externen Netzwerke anzeigen, die für die Verwendung durch das Edge-Gateway zur Verfügung stehen.

4 Geben Sie einen IP-Bereich ein und klicken Sie auf **Hinzufügen**.

5 Klicken Sie auf **Speichern**.

Ergebnisse

Die IP-Adressen werden dem Edge-Gateway zugewiesen.

Nächste Schritte

Zeigen Sie die IP-Adressen an, die dem Edge-Gateway zugewiesen sind, und fügen Sie nach Bedarf weitere IP-Adressen hinzu oder entfernen Sie diese.

Schnelle IP-Zuweisung

Sie können IP-Adressen aus einem externen Netzwerk-Subnetz einem Edge-Gateway zuweisen, ohne bestimmte IP-Adressen oder IP-Adressbereiche einzugeben, indem Sie die schnelle IP-Zuweisung nutzen.

Verfahren

1 Öffnen Sie „Edge-Gateway-Dienste“.

- a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 das Edge-Gateway und dann auf **IP-Zuweisungen**.

In den IP-Verwaltungstabellen können Sie die IP-Adressen sehen, die dem Edge-Gateway zugewiesen sind, sowie die IP-Adressen, die derzeit vom Edge-Gateway verwendet werden.

- 3 Klicken Sie im Abschnitt **Zugewiesene IPs** auf **Schnelle IP-Zuweisung**.
- 4 Wählen Sie im Dropdown-Menü ein Subnetz aus, aus dem IP-Adressen zugewiesen werden sollen.

Wenn mehrere Subnetze verfügbar sind, führt die Auswahl von **Beliebig** zu einer Zuweisung von IP-Adressen aus einem oder mehreren Subnetzen.

- 5 Geben Sie die Anzahl der IP-Adressen ein, die dem Edge-Gateway zugewiesen werden sollen, und klicken Sie auf **Speichern**.

Die Anzahl muss kleiner sein als die Anzahl der verfügbaren IP-Adressen im ausgewählten Subnetz.

Ergebnisse

Die IP-Adressen werden dem Edge-Gateway zugewiesen.

Nächste Schritte

Zeigen Sie die IP-Adressen an, die dem Edge-Gateway zugewiesen sind, und fügen Sie nach Bedarf weitere IP-Adressen hinzu oder entfernen Sie diese.

Erstellen von benutzerdefinierten Anwendungsportprofilen

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

Anwendungsportprofile enthalten eine Kombination aus einem Protokoll und einem Port oder einer Gruppe von Ports, die für Firewall- und NAT-Dienste auf dem Edge-Gateway verwendet wird. Zusätzlich zu den standardmäßigen Portprofilen, die für NSX-T Data Center vorkonfiguriert sind, können Sie benutzerdefinierte Anwendungsportprofile erstellen.

Wenn Sie ein benutzerdefiniertes Anwendungsportprofil auf einem Edge-Gateway erstellen, wird es für alle anderen NSX-T Data Center-Edge-Gateways sichtbar, die sich im selben Organisations-VDC befinden.

Verfahren

- 1 Öffnen Sie „Edge-Gateway-Dienste“.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 das Edge-Gateway und dann auf die Registerkarte **Sicherheit**.
- 3 Klicken Sie auf **Anwendungsportprofile**.
- 4 Klicken Sie im Abschnitt **Benutzerdefinierte Anwendungen** auf **Neu**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für das Anwendungsportprofil ein.

- 6 Wählen Sie ein Protokoll aus dem Dropdown-Menü aus.
- 7 Geben Sie einen Port oder einen durch Kommas getrennten Portbereich ein und klicken Sie auf **Speichern**.

Nächste Schritte

Verwenden Sie Anwendungsportprofile, um Firewall- und NAT-Regeln zu erstellen. Weitere Informationen finden Sie unter [Hinzufügen einer Firewallregel für NSX-T-Edge-Gateways](#) und [Hinzufügen einer SNAT- oder DNAT-Regel zu einem NSX-T-Edge-Gateway](#).

Richtlinienbasiertes IPSec-VPN für NSX-T Data Center-Edge-Gateways

Ab Version 10.1 unterstützt VMware Cloud Director richtlinienbasiertes IPSec-VPN mit Site-to-Site-Konnektivität zwischen einer NSX-T Data Center-Edge-Gateway-Instanz und einer Remote-Site.

IPSec-VPN bietet Site-to-Site-Konnektivität zwischen einem Edge-Gateway und Remote-Sites, die ebenfalls NSX-T Data Center verwenden oder mit Drittanbieter-Hardware-Routern oder VPN-Gateways, die IPSec unterstützen, konfiguriert sind.

Richtlinienbasiertes IPSec-VPN erfordert, dass eine VPN-Richtlinie auf Pakete angewendet wird, um zu ermitteln, welcher Datenverkehr vor dem Passieren eines VPN-Tunnels durch IPSec geschützt werden soll. Dieser VPN-Typ wird als statisch betrachtet, da die VPN-Richtlinieneinstellungen bei einer Änderung der lokalen Netzwerktopologie und -konfiguration ebenfalls aktualisiert werden müssen, um die Änderungen zu berücksichtigen.

NSX-T Data Center-Edge-Gateways unterstützen die Split-Tunnel-Konfiguration, wobei der IPSec-Datenverkehr eine Routing-Priorität hat.

VMware Cloud Director unterstützt die automatische Routenneuverteilung, wenn Sie IPSec-VPN auf einem NSX-T-Edge-Gateway verwenden.

Konfigurieren des richtlinienbasierten NSX-T-IPSec-VPN

Sie können die Site-to-Site-Konnektivität zwischen einem NSX-T Data Center-Edge-Gateway und Remote-Sites konfigurieren. Die Remote-Sites müssen NSX-T Data Center verwenden und über Hardwarerouter von Drittanbietern oder VPN-Gateways verfügen, die IPSec unterstützen.

VMware Cloud Director unterstützt die automatische Route Redistribution, wenn Sie IPSec-VPN auf einem NSX-T Data Center-Gateway konfigurieren.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 unter **Dienste** auf **IPSec-VPN**.

- 4 Um einen IPSec-VPN-Tunnel zu konfigurieren, klicken Sie auf **Neu**.
- 5 Geben Sie einen Namen und, optional, eine Beschreibung für den IPSec-VPN-Tunnel ein.
- 6 Wählen Sie einen vorinstallierten Schlüssel für die Eingabe aus.

Hinweis Der vorinstallierte Schlüssel muss am anderen Ende des IPSec-VPN-Tunnels identisch sein.

- 7 Geben Sie eine der IP-Adressen ein, die für das Edge-Gateway für den lokalen Endpoint verfügbar sind.

Hinweis Bei der IP-Adresse muss es sich entweder um die primäre IP des Edge-Gateways oder um eine IP-Adresse handeln, die dem Edge-Gateway vom externen Netzwerk separat zugeteilt wird.

- 8 Geben Sie mindestens eine lokale IP-Subnetz-Adresse in CIDR-Notation ein, die für den IPSec-VPN-Tunnel verwendet werden soll.
- 9 Geben Sie die IP-Adresse für die Remote-Site ein.
- 10 Geben Sie mindestens eine Remote-IP-Subnetz-Adresse in CIDR-Notation ein, die für den IPSec-VPN-Tunnel verwendet werden soll.
- 11 (Optional) Zum Aktivieren der Protokollierung wählen Sie die Option **Protokollierung** aus.
- 12 Klicken Sie auf **Speichern**.
- 13 Um sicherzustellen, dass der Tunnel funktioniert, wählen Sie ihn aus und klicken auf **Statistik anzeigen**.

Wenn der Tunnel funktioniert, wird für die Optionen **Tunnelstatus** und **IKE-Dienststatus** die Option **Erreichbar** angezeigt.

Ergebnisse

Der neu erstellte IPSec-VPN-Tunnel wird in der Ansicht **IPSec-VPN** angezeigt. Der IPSec-VPN-Tunnel wird mit einem Standardsicherheitsprofil erstellt.

Nächste Schritte

Sie können die IPSec-VPN-Tunnel-Einstellungen bearbeiten und das entsprechende Sicherheitsprofil nach Bedarf anpassen.

Anpassen des Sicherheitsprofils eines IPSec-VPN-Tunnels

Wenn Sie das vom System generierte Sicherheitsprofil, das Ihrem IPSec-VPN-Tunnel bei der Erstellung zugewiesen wurde, nicht verwenden möchten, können Sie es anpassen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 unter **Dienste** auf **IPSec-VPN**.
- 4 Wählen Sie den IPSec-VPN-Tunnel aus und klicken Sie auf **Anpassung des Sicherheitsprofils**.
- 5 Konfigurieren Sie die IKE-Profile.

Die IKE-Profile (Internet Key Exchange) stellen Informationen zu den Algorithmen bereit, die zur Authentifizierung, Verschlüsselung und Einrichtung eines gemeinsamen geheimen Schlüssels zwischen Netzwerksites verwendet werden, wenn Sie einen IKE-Tunnel einrichten.

- a Wählen Sie eine IKE-Protokollversion aus, um eine Sicherheitsverbindung (Security Association, SA) in der IPSec-Protokollsuite einzurichten.

Option	Bezeichnung
IKEv1	Wenn Sie diese Option auswählen, initiiert das IPSec-VPN nur das IKEv1-Protokoll und antwortet auch nur auf dieses Protokoll.
IKEv2	Die Standardoption. Wenn Sie diese Version auswählen, initiiert das IPSec-VPN nur das IKEv2-Protokoll und antwortet auch nur auf dieses Protokoll.
IKE-Flex	Wenn Sie diese Option auswählen und die Tunneleinrichtung mit dem IKEv2-Protokoll fehlschlägt, wird die Quellsite nicht zurückgesetzt und initiiert keine Verbindung mit dem IKEv1-Protokoll. Stattdessen wird die Verbindung akzeptiert, falls die Remote-Site eine Verbindung mit dem IKEv1-Protokoll initiiert.

- b Wählen Sie einen unterstützten Verschlüsselungsalgorithmus aus, der bei der IKE-Verhandlung (Internet Key Exchange) verwendet wird.
- c Wählen Sie im Dropdown-Menü **Digest** einen sicheren Hashing-Algorithmus aus, der während der IKE-Verhandlung verwendet wird.
- d Wählen Sie im Dropdown-Menü **Diffie-Hellman-Gruppe** eines der Kryptografieschemata aus, die es der Peer-Site und dem Edge-Gateway ermöglichen, einen gemeinsamen geheimen Schlüssel über einen unsicheren Kommunikationskanal einzurichten.
- e (Optional) Ändern Sie im Textfeld **Gültigkeitsdauer der Zuordnung** die Standardanzahl von Sekunden, bis der IPSec-Tunnel wiederhergestellt werden muss.

6 Konfigurieren Sie den IPSec-VPN-Tunnel.

- a Um Perfect Forward Secrecy zu aktivieren, wählen Sie die entsprechende Option aus.
- b Wählen Sie eine Defragmentierungsrichtlinie aus.

Die Defragmentierungsrichtlinie hilft bei der Verarbeitung von Defragmentierungsbits im inneren Paket.

Option	Bezeichnung
Kopieren	Kopiert das Defragmentierungsbit aus dem inneren IP-Paket in das äußere Paket.
Löschen	Ignoriert das im inneren Paket anwesende Defragmentierungsbit.

- c Wählen Sie einen unterstützten Verschlüsselungsalgorithmus aus, der bei der IKE-Verhandlung (Internet Key Exchange) verwendet wird.
 - d Wählen Sie im Dropdown-Menü **Digest** einen sicheren Hashing-Algorithmus aus, der während der IKE-Verhandlung verwendet wird.
 - e Wählen Sie im Dropdown-Menü **Diffie-Hellman-Gruppe** eines der Kryptografieschemata aus, die es der Peer-Site und dem Edge-Gateway ermöglichen, einen gemeinsamen geheimen Schlüssel über einen unsicheren Kommunikationskanal einzurichten.
 - f (Optional) Ändern Sie im Textfeld **Gültigkeitsdauer der Zuordnung** die Standardanzahl von Sekunden, bis der IPSec-Tunnel wiederhergestellt werden muss.
- 7** (Optional) Ändern Sie im Textfeld **Prüfintervall** die Standardanzahl der Sekunden für die Erkennung von ausgefallenen Peers.
- 8** Klicken Sie auf **Speichern**.

Ergebnisse

In der Ansicht „IPSec-VPN“ wird das Sicherheitsprofil des IPSec-VPN-Tunnels als **Benutzerdefiniert** angezeigt.

Konfigurieren dedizierter externer Netzwerkdienste

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

Bei Verwendung eines dedizierten externen Netzwerks können Sie zusätzliche Routing-Dienste konfigurieren, wie z. B. die Routenankündigungsverwaltung und die BGP-Konfiguration (Border Gateway Protocol).

Verwalten der Routenankündigung

Mithilfe der Routenankündigung können Sie in einem virtuellen Datacenter (VDC) einer Organisation eine vollständig geroutete Netzwerkumgebung erstellen.

Sie können entscheiden, welches der an das NSX-T Data Center-Edge-Gateway angehängten Subnetze für das dedizierte externe Netzwerk angekündigt werden soll.

Wenn dem Ankündigungsfiler kein Subnetz hinzugefügt wird, wird die Route dorthin dem externen Netzwerk nicht angekündigt. In diesem Fall bleibt das Subnetz privat.

Hinweis VMware Cloud Director kündigt jedes VDC-Organisationsnetzwerk an, das unter die angegebene Route fällt. Aus diesem Grund müssen Sie nicht für jedes Subnetz, das Teil eines angekündigten Netzwerks ist, einen Filter erstellen.

Die Routenankündigung wird automatisch auf dem NSX-T Data Center-Edge-Gateway konfiguriert.

VMware Cloud Director unterstützt die automatische Route Redistribution (Routenneuverteilung), wenn Sie auf einem NSX-T-Edge-Gateway die Routenankündigung verwenden. Die Route Redistribution wird automatisch auf dem logischen Tier-0-Router konfiguriert, der das dedizierte externe Netzwerk darstellt.

Voraussetzungen

- Stellen Sie sicher, dass Sie ein externes Netzwerk einem NSX-T Data Center-Edge-Gateway in der Organisation zugeordnet haben. Weitere Informationen finden Sie im [Dedizierte externe Netzwerke](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 unter **Routing** auf **Routenankündigung** und **Bearbeiten**.
- 4 Um ein anzukündigendes Subnetz hinzuzufügen, klicken Sie auf **Hinzufügen**.
- 5 Fügen Sie ein IPv4- oder IPv6-Subnetz hinzu.

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

Konfigurieren von allgemeinen BGP-Einstellungen

Sie können eine externe oder interne Border Gateway Protocol (eBGP oder iBGP)-Verbindung zwischen einem NSX-T Data Center-Edge-Gateway mit einem dedizierten externen Netzwerk und einem Router in Ihrer physischen Infrastruktur konfigurieren.

BGP trifft wichtige Routing-Entscheidungen mithilfe einer Tabelle mit IP-Netzwerken oder Präfixen, die mehrere Routen zwischen autonomen Systemen (AS) festlegen.

Der Begriff „BGP-Speaker“ bezieht sich auf ein Netzwerkgerät, das BGP ausführt. Zwei BGP-Speaker stellen eine Verbindung her, bevor Routing-Informationen ausgetauscht werden.

Der Begriff „BGP-Nachbar“ bezieht sich auf einen BGP-Speaker, der eine solche Verbindung hergestellt hat. Nachdem die Verbindung hergestellt wurde, tauschen die Geräte Routen aus und synchronisieren ihre Tabellen. Jedes Gerät sendet Keep Alive-Nachrichten, um diese Beziehung beizubehalten.

Voraussetzungen

- Stellen Sie sicher, dass Sie ein externes Netzwerk einem NSX-T Data Center Edge-Gateway in der Organisation zugeordnet haben. Weitere Informationen finden Sie im [Dedizierte externe Netzwerke](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 unter **Routing** auf **BGP** und klicken Sie unter **Konfiguration** auf **Bearbeiten**.
- 4 Wählen Sie die Option **Status** aus, um BGP zu aktivieren.
- 5 Geben Sie die ID-Nummer des autonomen Systems (AS) ein, die für die lokale AS-Funktion des Protokolls verwendet werden soll.

VMware Cloud Director weist dem Edge-Gateway die lokale AS-Nummer zu. Das Edge-Gateway kündigt diese ID an, wenn es eine Verbindung mit seinen BGP-Nachbarn in anderen autonomen Systemen herstellt.

- 6 Wählen Sie im Dropdown-Menü die Option **Graceful Restart-Modus** aus.

Option	Bezeichnung
Hilfsmodus und Graceful Restart	<p>Es ist nicht empfehlenswert, die Funktion „Graceful Restart“ auf dem Edge-Gateway zu aktivieren, da BGP-Peerings von allen Gateways immer aktiv sind.</p> <p>Bei einem Failover verlängert die Funktion „Graceful Restart“ die Zeit, die ein Remotenachbar benötigt, um ein alternatives Tier-0-Gateway auszuwählen. Dies verzögert die BFD-basierte Konvergenz.</p> <p>Hinweis Die Konfiguration des Edge-Gateways gilt für alle BGP-Nachbarn, es sei denn, die spezifische Konfiguration eines Nachbarn überschreibt sie.</p>
Nur Hilfsmodus	Nützlich für das Reduzieren oder Eliminieren der Unterbrechung des Datenverkehrs, der mit Routen verknüpft ist, die von einem Nachbarn gelernt wurden, der einen Graceful Restart ermöglicht. Der Nachbar muss seine Weiterleitungstabelle beibehalten können, während er einen Neustart durchläuft.
Deaktivieren	Deaktivieren Sie den Graceful Restart-Modus auf dem Edge-Gateway.

- 7 (Optional) Ändern Sie den Standardwert für den Graceful Restart-Timer.
- 8 (Optional) Ändern Sie den Standardwert für den Timer für veraltete Routen.
- 9 Wählen Sie die Option **ECMP** aus, um ECMP zu aktivieren.

Nächste Schritte

- [Erstellen einer IP-Präfixliste](#)
- [Hinzufügen eines BGP-Nachbarn](#)

Erstellen einer IP-Präfixliste

Sie können IP-Präfixlisten erstellen, die eine oder mehrere IP-Adressen enthalten. Sie verwenden IP-Präfixlisten, um BGP-Nachbarn Zugriffsberechtigungen für die Routenankündigung zuzuweisen.

Die IP-Präfixlisten werden über BGP-Nachbarfilter referenziert, um die Anzahl der BGP-Updates zu begrenzen, die zwischen BGP-Peers ausgetauscht werden. Mithilfe der Routenfilterung können Sie die Menge an Systemressourcen reduzieren, die für BGP-Updates benötigt wird.

Beispielsweise können Sie die IP-Adresse 192.168.100.3/27 zur IP-Präfixliste hinzufügen und verhindern, dass die Route zum Edge-Gateway neu verteilt wird.

Sie können auch eine IP-Adresse mit den Modifizierern `less than or equal to (le)` (kleiner als oder gleich) und `greater than or equal to (ge)` (größer als oder gleich) anhängen, um die Route Redistribution zu ermöglichen oder einzuschränken. Beispielsweise entsprechen die Modifizierer „ge 26“ und „le 32“ der IP-Adresse 192.168.100.3/27 den Subnetzmasken, die größer oder gleich 26 Bit und kleiner oder gleich 32 Bit sind.

Voraussetzungen

- Stellen Sie sicher, dass Sie ein externes Netzwerk einem NSX-T Data Center Edge-Gateway in der Organisation zugeordnet haben. Weitere Informationen finden Sie im [Dedizierte externe Netzwerke](#).
- [Konfigurieren von allgemeinen BGP-Einstellungen](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 unter **Routing** auf **BGP** und **IP-Präfixlisten**.
- 4 Um eine IP-Präfixliste hinzuzufügen, klicken Sie auf **Neu**.
- 5 Geben Sie einen Namen und, optional, eine Beschreibung für die Präfixliste ein.
- 6 Klicken Sie auf **Neu** und fügen Sie eine CIDR-Notation für das Präfix hinzu.
- 7 Wählen Sie im Dropdown-Menü eine Aktion aus, die auf das Präfix angewendet werden soll.
- 8 (Optional) Geben Sie die Modifizierer `greater than or equal to` und `less than or equal to` ein, um die Route Redistribution zu ermöglichen oder einzuschränken.

Nächste Schritte

- Sie können die IP-Präfixliste nach Bedarf bearbeiten oder löschen.
- Konfigurieren Sie die Routenfilterung. Weitere Informationen finden Sie im [Hinzufügen eines BGP-Nachbarn](#).

Hinzufügen eines BGP-Nachbarn

Sie können einzelne Einstellungen für die BGP-Routing-Nachbarn konfigurieren, wenn Sie sie hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass Sie ein externes Netzwerk einem NSX-T Data Center Edge-Gateway in der Organisation zugeordnet haben. Weitere Informationen finden Sie im [Dedizierte externe Netzwerke](#).
- Stellen Sie sicher, dass Sie die globalen BGP-Einstellungen für das Edge-Gateway konfiguriert haben. Weitere Informationen finden Sie im [Konfigurieren von allgemeinen BGP-Einstellungen](#).
- Wenn Sie die Routenfilterung verwenden, stellen Sie sicher, dass Sie IP-Präfixlisten erstellt haben. Weitere Informationen finden Sie im [Erstellen einer IP-Präfixliste](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen 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 unter **Routing** auf **BGP** und dann auf **Nachbarn**.
- 4 Um einen neuen BGP-Nachbarn hinzuzufügen, klicken Sie auf **Neu**.
- 5 Geben Sie die allgemeinen Einstellungen für den neuen BGP-Nachbarn ein.
 - a Geben Sie eine IPv4- oder IPv6-Adresse für den neuen BGP-Nachbarn ein.
 - b Geben Sie eine Remotenummer des autonomen Systems (AS) im ASPLAIN-Format ein.
 - c Geben Sie ein Zeitintervall zwischen dem Senden von Keep Alive-Nachrichten an einen BGP-Peer ein.
 - d Geben Sie ein Zeitintervall ein, bevor Sie einen BGP-Peer als ausgefallen deklarieren.

- e Wählen Sie im Dropdown-Menü die Option **Graceful Restart-Modus** für diesen Nachbarn aus.

Option	Bezeichnung
Deaktivieren	Überschreibt die Einstellungen des globalen Edge-Gateways und deaktiviert den Graceful Restart-Modus für diesen Nachbarn.
Nur Hilfsmodus	Überschreibt die Einstellungen des globalen Edge-Gateways und konfiguriert den Graceful Restart-Modus für diesen Nachbarn als Nur Hilfsmodus .
Graceful Restart und Hilfsmodus	Überschreibt die Einstellungen des globalen Edge-Gateways und konfiguriert den Graceful Restart-Modus für diesen Nachbarn als Graceful Restart und Hilfsmodus .

- f Wählen Sie die Option **AllowAS-in** aus, um den Empfang von Routen mit demselben AS zu aktivieren.
 - g Wenn der BGP-Nachbar eine Authentifizierung erfordert, geben Sie das Kennwort für den BGP-Nachbarn ein.
- 6** Konfigurieren Sie die Einstellungen für die bidirektionale Weiterleitungserkennung (Bidirectional Forwarding Detection, BFD) für den neuen BGP-Nachbarn.
- a (Optional) Wählen Sie die Option **BFD** aus, um BFD für die Fehlererkennung zu aktivieren.
 - b Legen Sie im Textfeld „BFD-Intervall“ das Zeitintervall für das Senden von Taktsignalpaketen fest.
 - c Geben Sie im Textfeld **Dead Multiple** ein, wie oft das Senden der Taktsignalpakete durch den BGP-Nachbarn fehlschlagen kann, bevor BFD den BGP-Nachbarn als ausgefallen ansieht.
- 7** (Optional) Konfigurieren Sie die Routenfilterung.
- a Wählen Sie im Dropdown-Menü **IP-Adressfamilie** eine IP-Adressfamilie aus.
 - b Um einen eingehenden Filter zu konfigurieren, wählen Sie eine IP-Präfixliste aus.
 - c Um einen ausgehenden Filter zu konfigurieren, wählen Sie eine IP-Präfixliste aus.

Nächste Schritte

Sie können den Status jedes BGP-Nachbarn anzeigen, bearbeiten oder BGP-Nachbarn nach Bedarf löschen.

Verwalten dedizierter vCenter Server-Instanzen

9

Mit dedizierten vCenter Server-Instanzen können Sie VMware Cloud Director als zentralen Verwaltungspunkt (Central Point of Management, CPOM) für Ihre vSphere-Umgebungen verwenden.

Wenn Sie eine vCenter Server-Instanz zu VMware Cloud Director hinzufügen, können Sie den Zweck der Instanz angeben.

Dedizierter vCenter Server

Die Infrastruktur einer angehängten vCenter Server-Instanz wird als Software-Defined Data Center (SDDC) gekapselt und vollständig für einen einzelnen Mandanten reserviert. Erstellen Sie eine dedizierte vCenter Server-Instanz, indem Sie den Mandantenzugriff für diese Instanz aktivieren. Nachdem Sie den Mandantenzugriff aktiviert haben, können Sie eine dedizierte vCenter Server-Instanz in einem Mandanten veröffentlichen.

Gemeinsam genutzter vCenter Server

Der Anbieter kann verschiedene Ressourcenpools der vCenter Server-Instanz über mehrere Provider-VDCs hinweg verwenden und diese Ressourcenpools dann verschiedenen Mandanten zuteilen. Eine gemeinsam genutzte vCenter Server-Instanz kann nicht für Mandanten veröffentlicht werden.

Keines

Die vCenter Server-Instanz hat keinen bestimmten Zweck.

VMware Cloud Director kann für die dedizierten vCenter Server-Instanzen und für die vCenter Server-Instanzen, die keinem festgelegten Zweck dienen, als HTTP-Proxy-Server fungieren.

Mit dedizierten vCenter Server-Instanzen können Sie VMware Cloud Director als zentralen Verwaltungspunkt für alle vSphere-Umgebungen verwenden.

- Sie können die Ressourcen einer vCenter Server-Instanz für einen einzelnen Mandanten reservieren, indem Sie den entsprechenden dedizierten vCenter Server nur für dessen Organisation veröffentlichen. Der Mandant nutzt diese Ressourcen nicht mit anderen Mandanten gemeinsam. Der Mandant kann auf diese dedizierte vCenter Server-Instanz mithilfe einer Benutzeroberfläche oder eines API-Proxys zugreifen, ohne dass ein VPN erforderlich ist.

- Sie können VMware Cloud Director als Lightweight-Verzeichnis verwenden, um alle vCenter Server-Instanzen zu registrieren.
- Sie können VMware Cloud Director als API-Endpoint für alle vCenter Server-Instanzen verwenden.

Sie können den Mandantenzugriff aktivieren und eine vCenter Server-Instanz während oder nach dem Anhängen der vCenter Server-Zielinstanz an VMware Cloud Director als dediziert markieren. Weitere Informationen finden Sie unter [Anhängen einer vCenter Server-Instanz allein oder zusammen mit einer NSX Manager-Instanz](#).

Mit einer angehängten vCenter Server-Instanz können Sie entweder einen freigegebenen vCenter Server oder einen dedizierten vCenter Server erstellen. Wenn Sie eine gemeinsam genutzte vCenter Server-Instanz erstellt haben, können Sie mit dieser vCenter Server-Instanz keinen dedizierten vCenter Server erstellen und umgekehrt.

Sie können Proxys erstellen, die von Mandanten für den Zugriff auf die zugrunde liegende vSphere-Umgebung verwendet werden können. Benutzer können sich mithilfe ihrer VMware Cloud Director-Konten bei der Benutzeroberfläche oder der API der Komponenten mit Proxys anmelden.

Durch dedizierte vCenter Server-Instanzen in VMware Cloud Director entfällt die Notwendigkeit, dass vCenter Server öffentlich zugänglich sein muss. Um den Zugriff zu steuern, können Sie den Mandantenzugriff auf ein SDDC in VMware Cloud Director aktivieren und deaktivieren.

Ein Proxy ist der Zugriffspunkt auf eine Komponente aus einem SDDC, z. B. eine vCenter Server-Instanz, ein ESXi-Host oder eine NSX Manager-Instanz. Durch die Aktivierung und Deaktivierung eines Proxys können Sie den Mandantenzugriff über diesen Proxy zulassen und beenden.

Erstellen und Verwalten dedizierter vCenter Server-Instanzen

Um dedizierte vCenter Server-Instanzen und -Proxys zu erstellen und zu verwalten, können Sie das Dienstanbieter-Admin-Portal oder die VMware Cloud Director OpenAPI verwenden. Weitere Informationen zur VMware Cloud Director OpenAPI finden Sie in *Erste Schritte mit VMware Cloud Director OpenAPI* unter <https://code.vmware.com>.

Wichtig VMware Cloud Director benötigt eine direkte Netzwerkverbindung zu jeder dedizierten vCenter Server-Instanz. Wenn die vCenter Server-Instanz einen externen Platform Services Controller verwendet, benötigt VMware Cloud Director ebenfalls eine direkte Netzwerkverbindung mit dem Platform Services Controller.

Um das VMware OVF Tool in einem dedizierten vCenter Server-Proxy zu verwenden, benötigt VMware Cloud Director eine direkte Verbindung zu jedem ESXi-Host.

- 1 Erstellen Sie eine dedizierte vCenter Server-Instanz.

Wenn Sie eine vCenter Server-Instanz zur VMware Cloud Director-Umgebung hinzufügen, können Sie eine dedizierte vCenter Server-Instanz erstellen, indem Sie den Mandantenzugriff im Assistenten **vCenter Server hinzufügen** aktivieren. Beim Anhängen der vCenter Server-Instanz können Sie auch einen Proxy dafür erstellen. Weitere Informationen finden Sie im [Hinzufügen der vCenter Server-Instanz](#). Sie können den Mandantenzugriff der vCenter Server-Instanzen aktivieren, die bereits zu VMware Cloud Director hinzugefügt wurden und keine festgelegte Verwendung haben. Weitere Informationen finden Sie im [Aktivieren des Mandantenzugriffs eines angehängten vCenter Server](#). Durch die Aktivierung des Mandantenzugriffs wird die vCenter Server-Instanz für die Veröffentlichung für Mandanten zur Verfügung gestellt.

2 Fügen Sie einen Proxy hinzu.

Sie können einen Proxy erstellen, wenn Sie eine vCenter Server-Instanz an VMware Cloud Director anhängen. Sie können dies auch zu einem späteren Zeitpunkt tun. Wenn die vCenter Server-Instanz einen externen Platform Services Controller verwendet, erstellt VMware Cloud Director auch für den Platform Services Controller einen Proxy. Mit über- und untergeordneten Proxys können Sie bestimmte Proxys aus den Mandanten ausblenden oder Sie können Gruppen von untergeordneten Proxys über ihre übergeordneten Proxys aktivieren und deaktivieren. Weitere Informationen über das Erstellen eines Proxys nach dem Hinzufügen einer vCenter Server-Instanz zu VMware Cloud Director finden Sie unter [Hinzufügen eines Proxys für den Zugriff auf die zugrunde liegenden vCenter Server-Ressourcen](#).

Sie können Proxys auf der Registerkarte **Proxys** unter **vSphere-Ressourcen** bearbeiten, aktivieren, deaktivieren und löschen.

Hinweis Wenn Sie einen Proxy zu einer dedizierten vCenter Server-Instanz 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.

Informationen zum Anzeigen und Verwalten von Zertifikaten und Zertifikatswiderrufslisten (CRLs) finden Sie unter [Verwalten der Proxy-Zertifikate und CRLs](#).

- 3 Rufen Sie das Zertifikat und den Fingerabdruck der erstellten Proxys ab und überprüfen Sie, ob das Zertifikat und der Fingerabdruck vorhanden und korrekt sind. Weitere Informationen finden Sie im [Verwalten der Proxy-Zertifikate und CRLs](#).
- 4 Veröffentlichen Sie die dedizierte vCenter Server-Instanz für eine oder mehrere Organisationen.

Sie können eine dedizierte vCenter Server-Instanz in einem Mandanten veröffentlichen und ihn im VMware Cloud Director Tenant Portal sichtbar machen. In den meisten Fällen sollte nur eine vCenter Server-Instanz für einen Mandanten veröffentlicht werden. Weitere Informationen finden Sie im [Veröffentlichen eines dedizierten vCenter Server](#).

- 5 Um Mandanten den Zugriff auf die dedizierten vCenter Server-Instanzen und -Proxys von VMware Cloud 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](#).

Dieses Kapitel enthält die folgenden Themen:

- [Aktivieren des Mandantenzugriffs eines angehängten vCenter Server](#)
- [Veröffentlichen eines dedizierten vCenter Server](#)

Aktivieren des Mandantenzugriffs eines angehängten vCenter Server

Sie können den Mandantenzugriff der vCenter Server-Instanzen aktivieren, die bereits zu VMware Cloud Director hinzugefügt wurden und keine festgelegte Verwendung haben. Durch die Aktivierung des Mandantenzugriffs wird eine dedizierte vCenter Server-Instanz erstellt und für die Veröffentlichung für Mandanten zur Verfügung gestellt.

Mit einer angehängten vCenter Server-Instanz können Sie entweder einen freigegebenen vCenter Server oder einen dedizierten vCenter Server erstellen. Wenn Sie eine freigegebene vCenter Server-Instanz erstellt haben und sie als dedizierten vCenter Server verwenden möchten, müssen Sie zuerst alle Provider-VDCs (VDCs) löschen, die die Ressourcen der vCenter Server-Instanz verwenden. Durch das Löschen aller Provider-VDCs, die mit der freigegebenen vCenter Server-Instanz verknüpft sind, wird der Status in „Keine“ geändert.

Voraussetzungen

Stellen Sie sicher, dass in Ihrer Umgebung mindestens ein angehängter vCenter Server vorhanden ist, der nicht dediziert oder freigegeben ist.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 3 Wählen Sie einen vCenter Server ohne einen bestimmten Zweck in der Spalte **Nutzung** aus.
- 4 Klicken Sie auf **Mandantenzugriff aktivieren**.

Nächste Schritte

[Veröffentlichen eines dedizierten vCenter Server](#).

Veröffentlichen eines dedizierten vCenter Server

Sie können einen dedizierten vCenter Server in einem Mandanten veröffentlichen und ihn über das VMware Cloud Director Tenant Portal sichtbar machen. Standardmäßig sollte ein vCenter Server nur für einen Mandanten veröffentlicht werden.

Standardmäßig ist ein SDDC eine vCenter Server-Instanz, die Sie für einen einzelnen Mandanten reservieren, indem Sie die entsprechende dedizierte vCenter Server-Instanz nur für ihre Organisation veröffentlichen. Der Mandant nutzt die dedizierten vCenter Server-Instanzressourcen nicht mit anderen Mandanten gemeinsam. Das Veröffentlichen einer dedizierten vCenter Server-Instanz für mehrere Mandanten verstößt gegen die Mandantengrenzwerte. Manchmal muss ein Mandant jedoch auf mehrere dedizierte vCenter Server-Instanzen zugreifen können. In diesen Fällen können Sie eine dedizierte vCenter Server-Instanz für mehrere Mandanten veröffentlichen.

Voraussetzungen

- Stellen Sie sicher, dass es mindestens eine vCenter Server-Instanz mit aktiviertem Mandantenzugriff in Ihrer VMware Cloud Director-Umgebung gibt. Weitere Informationen finden Sie im [Kapitel 9 Verwalten dedizierter vCenter Server-Instanzen](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Ressourcen vSphere-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **vCenter Server-Instanzen** aus.
- 3 Wählen Sie einen vCenter Server mit aktiviertem Mandantenzugriff aus.

Die vCenter Server-Instanzen mit aktiviertem Mandantenzugriff weisen einen dedizierten Wert in der Spalte **Nutzung** auf.

- 4 Klicken Sie auf **Mandanten verwalten**.
- 5 Wählen Sie den Mandanten oder die Mandanten aus, für die Sie die vCenter Server-Instanz veröffentlichen möchten.

Wenn Sie die Auswahl eines Mandanten in der Liste aufheben, wird die Veröffentlichung des vCenter Server rückgängig gemacht.

- 6 Klicken Sie auf **Speichern**.

Nächste Schritte

Um Benutzern den Zugriff auf die dedizierten vCenter Server-Instanzen und -Proxys von VMware Cloud 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](#).

Verwalten von Systemadministratoren und Rollen

10

Mithilfe des VMware Cloud Director Service Provider Admin Portal können Sie Systemadministratoren einzeln oder als Teil einer LDAP-Gruppe zu VMware Cloud Director hinzufügen. Sie können auch Rollen hinzufügen und bearbeiten, über die die Berechtigungen der Benutzer in ihrer Organisation festgelegt werden.

Hinweis Ab VMware Cloud Director 9.5 können Dienstleister über das VMware Cloud Director Service Provider Admin Portal oder über die vCloud OpenAPI Anbieterrollen erstellen und Anbieterbenutzer und -gruppen verwalten. Informationen zum Verwalten von Anbieterrollen, Benutzern und Gruppen finden Sie im *VMware Cloud 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 VMware Cloud 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.

VMware Cloud 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 VMware Cloud 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.

Systemadministratoren können mithilfe von Rechtepaketen und globalen Mandantenrollen die Rechte und Rollen verwalten, die für die einzelnen Organisationen verfügbar sind.

Nachdem Sie VMware Cloud 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 VMware Cloud Director von Version 9.1 oder früher aktualisiert haben, enthält das System zusätzlich zum Systemrechtapaket für jede vorhandene Organisation ein Alt-Rechtepaket. Jedes Alt-Rechtepaket 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 Rechtepaketmodell für eine bestehende Organisation verwenden zu können, müssen Sie das entsprechende Alt-Rechtepaket löschen.

Wenn Sie VMware Cloud 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 VMware Cloud 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 VMware Cloud Director enthaltenen Rechte weder erstellen noch ändern.

Rechtepaket

Systemadministratoren können mithilfe von Rechtepaketen die Rechte verwalten, die jeweils für die einzelnen Organisationen verfügbar sind. Ein Rechtepaket 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 VMware Cloud Director Mandantenportal*.

Vordefinierte Rollen und ihre Rechte

Jede vordefinierte VMware Cloud Director-Rolle enthält einen Standardsatz an Rechten, die erforderlich sind, um in gemeinsamen Workflows enthaltene Vorgänge auszuführen. Standardmäßig werden alle globalen vordefinierten Mandantenrollen für jeder Organisation im System veröffentlicht:

Vordefinierte Anbieterrollen

Standardmäßig gibt es als lokale Anbieterrollen für die Anbieterorganisationen nur die Rollen **Systemadministrator** und **Multisite-System**. **Systemadministratoren** können zusätzliche benutzerdefinierte Anbieterrollen erstellen.

Systemadministrator

Die Rolle **Systemadministrator** ist nur in der Anbieterorganisation vorhanden. Die Rolle **Systemadministrator** umfasst alle Rechte im System. Eine Liste der Rechte, die nur für die Rolle **Systemadministrator** verfügbar sind, finden Sie unter [Rechte von Systemadministratoren](#). Die Anmeldeinformationen des **Systemadministrators** werden während der Installation und Konfiguration festgelegt. Ein **Systemadministrator** kann zusätzliche Systemadministrator- und Benutzerkonten in der Anbieterorganisation einrichten.

Multisite-System

Wird zur Ausführung des Heartbeat-Prozesses für Bereitstellungen mit mehreren Standorten verwendet. Diese Rolle verfügt lediglich über das Recht **Multisite: Systemvorgänge**, mit dem eine Cloud Director OpenAPI-Anforderung zum Abrufen des Status des Remotemitglieds einer Sitezuordnung gestellt werden kann.

Vordefinierte globale Mandantenrollen

Standardmäßig werden die vordefinierten globalen Mandantenrollen und die darin enthaltenen Rechte für alle Organisationen veröffentlicht. **Systemadministratoren** können die Veröffentlichung von Rechten und globalen Mandantenrollen einzelner Organisationen rückgängig machen. **Systemadministratoren** können vordefinierte globale Mandantenrollen bearbeiten oder löschen. **Systemadministratoren** können zusätzliche globale Mandantenrollen erstellen und veröffentlichen.

Organisationsadministrator

Nach dem Erstellen einer Organisation kann ein **Systemadministrator** einem beliebigen Benutzer in der Organisation die Rolle **Organisationsadministrator** zuweisen. Ein Benutzer mit der vordefinierten Rolle **Organisationsadministrator** kann Benutzer und Gruppen in seiner Organisation verwalten und ihnen Rollen zuweisen, einschließlich der vordefinierten Rolle **Organisationsadministrator**. Von einem **Organisationsadministrator** erstellte oder geänderte Rollen sind für andere Organisationen nicht sichtbar.

Katalogautor

Die mit der vordefinierten Rolle **Katalogautor** verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu erstellen und zu veröffentlichen.

vApp-Autor

Die mit der vordefinierten Rolle **vApp-Autor** verknüpften Rechte ermöglichen es einem Benutzer, Kataloge zu verwenden und vApps zu erstellen.

vApp-Benutzer

Die mit der vordefinierten Rolle **vApp-Benutzer** verknüpften Rechte ermöglichen es einem Benutzer, vorhandene vApps zu verwenden.

Nur Konsolenzugriff

Die mit den vordefinierten Rolle **Nur Konsolenzugriff** verknüpften Rechte ermöglichen es einem Benutzer, den Status und die Eigenschaften von virtuellen Maschinen anzuzeigen und das Gastbetriebssystem zu verwenden.

Auf Identitätsanbieter zurückstellen

Die mit der vordefinierten Rolle **Auf Identitätsanbieter zurückstellen** verknüpften Rechte werden basierend auf vom OAuth- oder SAML-Identitätsanbieter empfangenen Informationen festgelegt. Um sich für die Aufnahme zu qualifizieren, wenn einem Benutzer oder einer Gruppe die Rolle **Auf Identitätsanbieter zurückstellen** zugewiesen ist, muss ein vom Identitätsanbieter bereitgestellter Rollen- oder Gruppenname exakt (unter Berücksichtigung von Groß-/Kleinschreibung) mit einem innerhalb Ihrer Organisation definierten Rollen- oder Gruppennamen übereinstimmen.

- Wenn ein OAuth-Identitätsanbieter den Benutzer definiert, werden dem Benutzer die im Array `roles` des benutzereigenen OAuth-Tokens angegebenen Rollen zugewiesen.
- Wenn ein SAML-Identitätsanbieter den Benutzer definiert, werden dem Benutzer die Rollen zugewiesen, die in dem SAML-Attribut angegeben werden, dessen Name im Element `RoleAttributeName` angezeigt wird, das sich wiederum im Element `SamlAttributeMapping` in `OrgFederationSettings` der Organisation befindet.

Wenn einem Benutzer die Rolle **Auf Identitätsanbieter zurückstellen** zugewiesen wird, jedoch keine übereinstimmende Rolle bzw. kein übereinstimmender Gruppenname in Ihrer Organisation vorhanden ist, kann sich der Benutzer bei der Organisation anmelden, verfügt jedoch über keine Rechte. Wenn ein Identitätsanbieter einem Benutzer eine Rolle auf Systemebene zuweist, wie beispielsweise die eines **Systemadministrators**, kann sich der Benutzer bei der Organisation anmelden, verfügt jedoch über keine Rechte. Solchen Benutzern müssen Sie eine Rolle manuell zuweisen.

Mit Ausnahme der Rolle **Auf Identitätsanbieter zurückstellen** enthält jede vordefinierte Rolle einen Satz von Standardrechten. Nur ein **Systemadministrator** kann die Rechte in einer vordefinierten Rolle ändern. Wenn ein **Systemadministrator** eine vordefinierte Rolle ändert, werden die Änderungen an alle Instanzen der Rolle im System weitergegeben.

Rechte in vordefinierten globalen Mandantenrollen

Ein **Systemadministrator** kann das Service Provider Admin Portal verwenden, um die Liste der in einer Rolle enthaltenen Rechte anzuzeigen.

- 1 Klicken Sie in der oberen Navigationsleiste auf **Administration**.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Rollen**.
- 3 Klicken Sie auf den Namen der Rolle, die Sie anzeigen möchten.

Ein **Organisationsadministrator** kann das Service Provider Admin Portal oder die Cloud Director OpenAPI verwenden, um die Rechte in einer Rolle anzuzeigen oder lokale Rollen für die Organisation zu erstellen.

Mehrere vordefinierte globale Rollen haben verschiedene Rechte gemein. Diese Rechte werden standardmäßig allen neuen Organisationen gewährt und können in anderen Rollen verwendet werden, die vom **Organisationsadministrator** erstellt werden. Eine Liste der Rechte in vordefinierten Mandantenrollen finden Sie unter [Rechte in vordefinierten globalen Mandantenrollen](#).

Rechte von Systemadministratoren

Die Rolle **Systemadministrator** ist nur in der Anbieterorganisation vorhanden. Standardmäßig verfügt die Rolle **Systemadministrator** über alle VMware Cloud Director-Rechte.

Die Rolle **Systemadministrator** verfügt über alle VMware Cloud Director-Rechte. In dieser Liste finden Sie die Rechte, die nur für **Systemadministratoren** verfügbar sind. Die Rolle **Systemadministrator** umfasst auch die [Rechte in vordefinierten globalen Mandantenrollen](#).

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind

Neu in dieser Version	Name des Rechts
	Zugriffssteuerungsliste: Verwalten
	Zugriffssteuerungsliste: Anzeigen
	Zusätzliche Dienste: Workflows ausführen
	Zusätzliche Dienste: Ausgeführte Workflows anzeigen
	Zusätzliche Dienste: Workflows anzeigen
	Ressourcenpool übernehmen: Anzeigen
	Alternative Administratorentität: Anzeigen
	AMQP-Einstellungen: Verwalten
	AMQP-Einstellungen: Anzeigen
	API-Explorer: Anzeigen
	Katalog: Medien von vSphere importieren
	Katalog: Schatten-VM anzeigen
	Katalog: VCSP-Veröffentlichung/-Abonnement zwischenspeichern
	Zellenkonfiguration: Anzeigen
	Cloud-Tunnel-Server: Verwalten
	Cloud-Tunnel-Server: Anzeigen
	Systemeinstellungen der Inhaltsbibliothek: Verwalten
	Systemeinstellungen der Inhaltsbibliothek: Anzeigen
	Benutzerdefinierte Entität: Benutzerdefinierte Entitätsdefinitionen erstellen

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	Benutzerdefinierte Entität: Benutzerdefinierte Entitätsdefinitionen löschen
	Benutzerdefinierte Entität: Benutzerdefinierte Entitätsdefinitionen bearbeiten
	Benutzerdefinierte Entität: Benutzerdefinierte Entitätsdefinitionen anzeigen
	Datenspeicher: Löschen
	Datenspeicher: Bearbeiten
	Datenspeicher: Aktivieren oder deaktivieren
	Datenspeicher: In vSphere öffnen
	Datenspeicher: Anzeigen
	Direktes vDC-Organisationsnetzwerk: Verwalten
	Verteilter virtueller Switch: In vSphere öffnen
	Edge-Cluster: Verwalten
	Edge-Cluster: Anzeigen
	Definition für Erweiterungsdienst-API: Verwalten
	Definition für Erweiterungsdienst-API: Anzeigen
	Erweiterungsdienste: Anzeigen
	Erweiterungen: Anzeigen
	Externer Dienst: Verwalten
	Externer Dienst: Anzeigen
	Allgemein: Fehlerdetails anzeigen
	Globale Rolle: Bearbeiten
	Globale Rolle: Anzeigen
	Host: Aktivieren oder deaktivieren
	Host: Verwalten
	Host: In vSphere öffnen
	Host: Vorbereiten oder Vorbereitung rückgängig machen
	Host: Reparieren
	Host: Upgrade durchführen
	Host: Anzeigen

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	Kerberos-Einstellungen: Verwalten
	Kerberos-Einstellungen: Anzeigen
	LDAP-Einstellungen: Verwalten
	LDAP-Einstellungen: Anzeigen
	Lizenzbericht: Anzeigen
	Lokalisierungsressourcen: Verwalten
	Multisite: Systemvorgänge
	Netzwerkpool: Erstellen oder löschen
	Netzwerkpool: Bearbeiten
	Netzwerkpool: In vSphere öffnen
	Netzwerkpool: Reparieren
	Netzwerkpool: Anzeigen
	NSX-T: Bearbeiten
	NSX-T: Anzeigen
	Objekterweiterungen: Verwalten
	Objekterweiterungen: Anzeigen
	Organisationsnetzwerk: Erstellen oder löschen
	Organisationsnetzwerk: In vSphere öffnen
	Computing-Richtlinie für Organisations-vDC: Administratoransicht
	Computing-Richtlinie für Organisations-vDC: Verwalten
	Distributed Firewall für Organisations-vDC: Aktivieren/Deaktivieren
	Organisations-vDC-Gateway: BGP-Routing konfigurieren
	Organisations-vDC-Gateway: L2-VPN konfigurieren
	Organisations-vDC-Gateway: OSPF-Routing konfigurieren
	Organisations-vDC-Gateway: Remotezugriff konfigurieren
✓	Organisations-vDC-Gateway: Routenankündigung konfigurieren
	Organisations-vDC-Gateway: SSL-VPN konfigurieren
	Organisations-vDC-Gateway: Systemprotokollierung konfigurieren

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	Organisations-vDC-Gateway: Erstellen
	Organisations-vDC-Gateway: Löschen
	Organisations-vDC-Gateway: Verteiltes Routing
	Organisations-vDC-Gateway: Importieren
	Organisations-vDC-Gateway: Formfaktor ändern
	Organisations-vDC-Gateway: Aktualisieren
	Organisations-vDC-Gateway: Eigenschaften aktualisieren
	Organisations-vDC-Gateway: Upgrade durchführen
	Organisations-vDC-Gateway: BGP-Routing anzeigen
	Organisations-vDC-Gateway: L2-VPN anzeigen
	Organisations-vDC-Gateway: OSPF-Routing anzeigen
	Organisations-vDC-Gateway: Remotezugriff anzeigen
✓	Organisations-vDC-Gateway: Routenankündigung anzeigen
	Organisations-vDC-Gateway: SSL-VPN anzeigen
	Organisations-vDC-Netzwerk: Importieren
	Organisations-vDC-Ressourcenpool: In vSphere öffnen
	Organisations-vDC-Ressourcenpool: Anzeigen
	Organisations-vDC-Speicherrichtlinie: Bearbeiten
	Organisations-vDC-Speicherrichtlinie: Aktivieren oder deaktivieren
	Organisations-vDC-Speicherrichtlinie: In vSphere öffnen
	Organisations-vDC-Speicherrichtlinie: Entfernen
	Organisations-vDC: Erstellen
	Organisations-vDC: Löschen
	Organisations-vDC: Aktivieren oder deaktivieren
	Organisations-vDC: Erweiterte Bearbeitung
	Organisations-vDC: Erweiterte Ansicht
	Organisation: Aktivieren oder deaktivieren
	Organisation: Erstellen oder löschen

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	Organisation: Grenzwerte bearbeiten
	Organisation: Namen bearbeiten
	Organisation: Mandantenspeicher migrieren
	Organisation: Administratorabfragen ausführen
	Organisation: Anbieter-LDAP als Mandanten verwenden
	Portgruppe: In vSphere öffnen
	Einstellungen: Definition von Einstellungen verwalten
	Anbietwork: Erstellen oder löschen
	Anbietwork: Bearbeiten
	Anbietwork: In vSphere öffnen
	Anbietwork: Anzeigen
	Computing-Richtlinie für Anbieter-vDC: Verwalten
	Computing-Richtlinie für Anbieter-vDC: Anzeigen
	Provider-vDC-Ressourcenpool: VMs migrieren
	Provider-vDC-Ressourcenpool: In vSphere öffnen
	Provider-vDC-Ressourcenpool: Anzeigen
	Provider-vDC-Speicherrichtlinie: Bearbeiten
	Provider-vDC-Speicherrichtlinie: Aktivieren oder deaktivieren
	Provider-vDC-Speicherrichtlinie: In vSphere öffnen
	Provider-vDC-Speicherrichtlinie: Entfernen
	Provider-vDC-Speicherrichtlinie: Anzeigen
	Provider-vDC: Ressourcenpool hinzufügen
	Provider-vDC: Erstellen oder löschen
	Provider-vDC: Ressourcenpool löschen
	Provider-vDC: Bearbeiten
	Provider-vDC: Aktivieren oder deaktivieren
	Provider-vDC: Ressourcenpool aktivieren oder deaktivieren
	Provider-vDC: vSphere-VXLAN aktivieren

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	Provider-vDC: Zusammenführen
	Provider-vDC: Anzeigen
✓	Kontingent-Richtlinie: Verwalten
✓	Kontingent-Richtlinie: Anzeigen
	VM neu laden: Verwalten
	Ressourcenklassenaktion: Verwalten
	Ressourcenklassenaktion: Anzeigen
	Ressourcenpool: Öffnen
	Ressourcenpool: In vSphere öffnen
	Ressourcenpool: Anzeigen
	Recht: Verwalten
	Recht: Anzeigen
	Rechtepaket: Bearbeiten
	Rechtepaket: Anzeigen
	SDDC: Verwalten
	SDDC: Proxy verwalten
	SDDC: Anzeigen
	Selektorerweiterungen: Verwalten
	Selektorerweiterungen: Anzeigen
✓	Serverzertifikate: Verwalten
✓	Serverzertifikate: Anzeigen
	Dienstanwendungen: Verwalten
	Dienstanwendungen: Anzeigen
	Dienstautorisierung: Verwalten
	Dienstkonfiguration: Verwalten
	Dienstkonfiguration: Anzeigen
	Dienstbibliothek: Dienstbibliotheken erstellen
	Dienstbibliothek: Dienste aus der Dienstbibliothek löschen

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	Dienstbibliothek: Dienst-Metadaten bearbeiten
	Dienstbibliothek: Inhalte eines Dienstes bearbeiten
	Dienstverknüpfung: Verwalten
	Dienstverknüpfung: Anzeigen
	Dienstressourcentyp: Verwalten
	Dienstressourcentyp: Anzeigen
	Dienstressource: Verwalten
	Dienstressource: Anzeigen
	Gemeinsames vDC-Organisationsnetzwerk: Verwalten
	Site: Bearbeiten
	Site: Anzeigen
✓	SSL-Einstellungen: Anzeigen
	Isoliertes Objekt: Verwalten
	Isoliertes Objekt: Anzeigen
	Systemvorgänge: Systemvorgänge ausführen
	Systemorganisation: Verwalten
	Systemorganisation: Anzeigen
	Systemeinstellungen: Verwalten
	Systemeinstellungen: Anzeigen
	Aufgabe: Fortsetzen, abbrechen oder fehlschlagen lassen
	Aufgabe: Aktualisieren
	Aufgabe: Aufgaben anzeigen
	Token: Verwalten
	Token: Alle verwalten
✓	Truststore: Verwalten
✓	Truststore: Anzeigen
	UI-Plug-Ins: Definieren, hochladen, ändern, löschen, zuordnen oder Zuordnung aufheben
	Branding des UI-Portals: Verwalten

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	vApp-Vorlage: Ablauf der Speicher-Lease erzwingen
	vApp-Vorlage: Importieren
	vApp-Vorlage: In vSphere öffnen
	vApp: Alle zusätzlichen Konfigurationen zulassen
	vApp: Zusätzliche Konfiguration für Ethernet-Zusammenfügung zulassen
	vApp: Zusätzliche Konfiguration für Latenz zulassen
	vApp: Zusätzliche Konfiguration für Abgleich zulassen
	vApp: Zusätzliche Konfiguration für NUMA-Knotenaffinität zulassen
	vApp: Einstellungen für die CPU- und Arbeitsspeicherreservierung der VM bei allen VDC-Typen bearbeiten
	vApp: In Wartungsmodus wechseln/Wartungsmodus beenden
	vApp: Ablauf der Laufzeit-Lease erzwingen
	vApp: Ablauf der Speicher-Lease erzwingen
	vApp: Importoptionen
	vApp: Wartung verwalten
	vApp: In vSphere öffnen
	vApp: Schatten-VM anzeigen
	vApp: VM-Konformität prüfen
	vApp: VM migrieren, Bereitstellungsaufhebung erzwingen, verschieben, konsolidieren
	VCD-Erweiterung: Registrieren, Registrierung aufheben, aktualisieren, zuordnen oder Zuordnung aufheben
	VCD-Erweiterung: Anzeigen
	vCenter: Anhängen oder trennen
	vCenter: Aktivieren oder deaktivieren
	vCenter: In vSphere öffnen
	vCenter: Aktualisieren
	vCenter: Anzeigen
	vDC-Gruppe: Konfigurieren
	vDC-Gruppe: Anzeigen

Tabelle 10-1. Rechte, die nur für Systemadministratoren verfügbar sind (Fortsetzung)

Neu in dieser Version	Name des Rechts
	VDC-Vorlage: Zugriffssteuerungsliste verwalten
	VDC-Vorlage: Erweiterte Ansicht
	VDC-Vorlage: Verwalten
	VMC: SDDC registrieren
	vRealize Orchestrator: Workflows veröffentlichen und deren Veröffentlichung für Mandanten rückgängig machen
	vRealize Orchestrator: vRealize Orchestrator-Server registrieren und deren Registrierung aufheben
	vRealize Orchestrator: Registrierte vRealize Orchestrator-Server anzeigen
	vSphere-Server: Verwalten
	vSphere-Server: Proxy verwalten
✓	vSphere-Server: Proxy-Konfiguration verwalten
	vSphere-Server: Anzeigen

Rechte in vordefinierten globalen Mandantenrollen

Mehrere vordefinierte globale Rollen haben verschiedene Rechte gemein. Diese Rechte werden standardmäßig allen neuen Organisationen gewährt und können in anderen Rollen verwendet werden, die vom **Organisationsadministrator** erstellt werden.

In den globalen Mandantenrollen in VMware Cloud Director enthaltene Rechte

Neu in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	Auf alle Organisations-VDCs zugreifen	✓				
	Katalog: vApp von „Meine Cloud“ hinzufügen	✓	✓	✓		
	Katalog: Besitzer ändern	✓				
	Katalog: CLSP-Veröffentlichung/-Abonnement	✓	✓			
	Katalog: Katalog erstellen/löschen	✓	✓			
	Katalog: Eigenschaften bearbeiten	✓	✓			
	Katalog: Veröffentlichen	✓	✓			

Neu in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	Katalog: Gemeinsame Nutzung	✓	✓			
	Katalog: Zugriffssteuerungsliste anzeigen	✓	✓			
	Katalog: Private und freigegebene Kataloge anzeigen	✓	✓	✓		
	Katalog: Veröffentlichte Kataloge anzeigen	✓				
	Benutzerdefinierte Entität: Alle benutzerdefinierten Entitätsinstanzen in der Organisation anzeigen	✓				
	Benutzerdefinierte Entität: Benutzerdefinierte Entitätsinstanz anzeigen	✓				
	Datenträger: Besitzer ändern	✓	✓			
	Datenträger: Erstellen	✓	✓	✓		
	Datenträger: Löschen	✓	✓	✓		
	Datenträger: Eigenschaften bearbeiten	✓	✓	✓		
✓	Datenträger: Verschlüsselungsstatus anzeigen	✓		✓		
	Datenträger: Eigenschaften anzeigen	✓	✓	✓	✓	
	Allgemein: Administratorsteuerung	✓				
	Allgemein: Administratoransicht	✓				
	Allgemein: Benachrichtigung senden	✓				
	Gruppe/Benutzer: Anzeigen	✓				
	Hybrid Cloud-Betrieb: Ticket zur Steuerung abrufen	✓				
	Hybrid Cloud-Betrieb: Ticket für Aus-der-Cloud-Tunnel abrufen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel-Ticket abrufen	✓				
	Hybrid Cloud-Betrieb: Aus-der-Cloud-Tunnel erstellen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel erstellen	✓				

Neu in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	Hybrid Cloud-Betrieb: Aus-der-Cloud-Tunnel löschen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel löschen	✓				
	Hybrid Cloud-Betrieb: Endpoint-Tag des Aus-der-Cloud-Tunnels aktualisieren	✓				
	Hybrid Cloud-Betrieb: Aus-der-Cloud-Tunnel anzeigen	✓				
	Hybrid Cloud-Betrieb: Cloud-Tunnel anzeigen	✓				
	Organisationsnetzwerk: Eigenschaften bearbeiten	✓				
	Organisationsnetzwerk: Anzeigen	✓				
	Computing-Richtlinie für Organisations-vDC: Anzeigen	✓	✓	✓	✓	
	Distributed Firewall für Organisations-vDC: Regeln konfigurieren	✓				
	Distributed Firewall für Organisations-vDC: Regeln anzeigen	✓				
	Organisations-vDC-Gateway: DHCP konfigurieren	✓				
	Organisations-vDC-Gateway: DNS konfigurieren	✓				
	Organisations-vDC-Gateway: ECMP-Routing konfigurieren	✓				
	Organisations-vDC-Gateway: Firewall konfigurieren	✓				
	Organisations-vDC-Gateway: IPSec-VPN konfigurieren	✓				
	Organisations-vDC-Gateway: Lastausgleichsdienst konfigurieren	✓				
	Organisations-vDC-Gateway: NAT konfigurieren	✓				
	Organisations-vDC-Gateway: Statisches Routing konfigurieren	✓				
	Organisations-vDC-Gateway: Syslog konfigurieren	✓				

Neu in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	Organisations-vDC-Gateway: In erweiterte Netzwerke konvertieren	✓				
	Organisations-vDC-Gateway: Anzeigen	✓				
	Organisations-vDC-Gateway: DHCP anzeigen	✓				
	Organisations-vDC-Gateway: DNS anzeigen	✓				
	Organisations-vDC-Gateway: Firewall anzeigen	✓				
	Organisations-vDC-Gateway: IPSec-VPN anzeigen	✓				
	Organisations-vDC-Gateway: Lastausgleichsdienst anzeigen	✓				
	Organisations-vDC-Gateway: NAT anzeigen	✓				
	Organisations-vDC-Gateway: Statisches Routing anzeigen	✓				
	vDC-Organisationsnetzwerk: Eigenschaften bearbeiten	✓				
	vDC-Organisationsnetzwerk: Eigenschaften anzeigen	✓		✓		
✓	Organisations-vDC-Speicherrichtlinie: Funktionen anzeigen	✓				
	Organisations-vDC-Speicherprofil: Standardwert festlegen	✓				
	Organisations-vDC: Bearbeiten	✓				
	Organisations-vDC: Zugriffssteuerungsliste bearbeiten	✓				
	Organisations-vDC: Firewall verwalten	✓				
	Organisations-vDC: Anzeigen	✓	✓			
	Organisations-vDC: Zugriffssteuerungsliste anzeigen	✓				
	Organisations-vDC: Metriken anzeigen	✓				

Neu in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	Organisations-vDC: VM-VM-Affinität bearbeiten	✓	✓	✓		
	Organisation: Zuordnungseinstellungen bearbeiten	✓				
	Organisation: Verbundeinstellungen bearbeiten	✓				
	Organisation: LDAP-Einstellungen bearbeiten	✓				
	Organisation: Lease-Richtlinie bearbeiten	✓				
	Organisation: OAuth-Einstellungen bearbeiten	✓				
	Organisation: Kennwortrichtlinie bearbeiten	✓				
	Organisation: Eigenschaften bearbeiten	✓				
	Organisation: Kontingent-Richtlinie bearbeiten	✓				
	Organisation: SMTP-Einstellungen bearbeiten	✓				
	Organisation: Benutzer/Gruppe beim Bearbeiten der VDC-Zugriffssteuerungsliste aus Identitätsanbieter importieren	✓				
	Organisation: Anzeigen	✓	✓	✓		
	Organisation: Metriken anzeigen	✓				
	Rolle: Erstellen, bearbeiten, löschen oder kopieren	✓				
	Dienstbibliothek: Dienstbibliotheken anzeigen	✓				
	UI-Plug-Ins: Anzeigen	✓	✓	✓	✓	
	vApp-Vorlage/-Medien: Kopieren	✓	✓	✓		
	vApp-Vorlage/-Medien: Erstellen/Hochladen	✓	✓			
	vApp-Vorlage/-Medien: Bearbeiten	✓	✓	✓		
	vApp-Vorlage/-Medien: Anzeigen	✓	✓	✓	✓	

Neu in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	vApp-Vorlage: Besitzer ändern	✓	✓			
	vApp-Vorlage: Auschecken	✓	✓	✓	✓	
	vApp-Vorlage: Herunterladen	✓	✓			
	vApp: Besitzer ändern	✓				
	vApp: Kopieren	✓	✓	✓	✓	
	vApp: Erstellen/Neu konfigurieren	✓	✓	✓		
	vApp: Löschen	✓	✓	✓	✓	
	vApp: Herunterladen	✓	✓	✓		
	vApp: Eigenschaften bearbeiten	✓	✓	✓	✓	
	vApp: VM-Computing-Richtlinie bearbeiten	✓	✓	✓		
	vApp: CPU der VM bearbeiten	✓	✓	✓		
	vApp: Festplatte der VM bearbeiten	✓	✓	✓		
	vApp: Arbeitsspeicher der VM bearbeiten	✓	✓	✓		
	vApp: VM-Netzwerk bearbeiten	✓	✓	✓	✓	
	vApp: VM-Eigenschaften bearbeiten	✓	✓	✓	✓	
	vApp: VM-Kennwordeinstellungen verwalten	✓	✓	✓	✓	✓
	vApp: Energievorgänge	✓	✓	✓	✓	
	vApp: Gemeinsame Nutzung	✓	✓	✓	✓	
	vApp: Snapshot-Vorgänge	✓	✓	✓	✓	
	vApp: Hochladen	✓	✓	✓		
	vApp: Konsole verwenden	✓	✓	✓	✓	✓
	vApp: Zugriffssteuerungsliste anzeigen	✓	✓	✓	✓	
✓	vApp: VM und Festplatten-Verschlüsselungsstatus der VM anzeigen	✓		✓		
	vApp: VM-Metriken anzeigen	✓		✓	✓	

Neu in dieser Version	Name des Rechts	Organisation administrator	Katalogautor	vApp-Autor	vApp-Benutzer	Nur Konsolenzugriff
	vApp: VM-Startoptionen	✓	✓	✓		
	vApp: VM-Metadaten zu vCenter	✓	✓	✓		
	VDC-Vorlage: Instanzieren	✓				
	VDC-Vorlage: Anzeigen	✓				

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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Rechtepakete** aus.
- 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.

Kategorie	Beschreibung
Erweiterungen	Enthält Rechte für die Ansicht und Verwaltung von VMware Cloud 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](#).

Klonen eines Rechtepakets

Sie können ein vorhandenes Rechtepakete als Vorlage für die Erstellung eines neuen Pakets verwenden.

Voraussetzungen

Stellen Sie sicher, dass Sie über die Rechte zum Hinzufügen neuer Rollen in VMware Cloud Director verfügen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Rechtepakete** aus.
- 3 Wählen Sie das Rechtepakete aus, das Sie klonen möchten, und klicken Sie auf **Klonen**.
- 4 Geben Sie im Fenster **Rechtepakete klonen** einen Namen und eine Beschreibung für das geklonte Paket ein.
- 5 (Optional) Um die geklonten Rechte zu bearbeiten, aktivieren Sie die Umschaltoption **Ausgewählte Rechte ändern** und aktivieren bzw. deaktivieren Sie die Rechte, die Sie für die geklonte Rolle ändern möchten.
- 6 Klicken Sie auf **Speichern**.

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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Rechtepakete** aus.
- 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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Rechtepakete** aus.

- 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 Rechtepakete veröffentlicht wird.

Löschen eines Rechtepakets

Sie können ein Rechtepakete entfernen, wenn Sie es in Ihren Organisationen nicht mehr verwenden.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Rechtepakete** aus.
- 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 VMware Cloud 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 VMware Cloud 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 in der oberen Navigationsleiste **Administration** aus.

- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Globale Rollen** aus.
- 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 VMware Cloud 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 VMware Cloud 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](#).

Klonen einer globalen Mandantenrolle

Sie können eine vorhandene globale Mandantenrolle als Vorlage für die Erstellung einer neuen Rolle verwenden.

Voraussetzungen

Stellen Sie sicher, dass Sie über die Rechte zum Hinzufügen neuer Rollen in VMware Cloud Director verfügen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Globale Rollen** aus.
- 3 Wählen Sie die Rolle aus, die Sie klonen möchten, und klicken Sie auf **Klonen**.
- 4 Geben Sie im Fenster **Globale Rolle klonen** einen Namen und eine Beschreibung für die geklonte Rolle ein.
- 5 (Optional) Um die geklonten Rechte zu bearbeiten, aktivieren Sie die Umschaltoption **Ausgewählte Rechte ändern** und aktivieren bzw. deaktivieren Sie die Rechte, die Sie für die geklonte Rolle ändern möchten.
- 6 Klicken Sie auf **Speichern**.

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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Globale Rollen** aus.
- 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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Globale Rollen** aus.
- 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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Globale Rollen** aus.
- 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 VMware Cloud Director-Anbieters erstellen.

Informationen zum Verwalten von Mandantenrollen finden Sie im *Handbuch für das VMware Cloud Director Mandantenportal*.

Erstellen einer Anbieterrolle

Sie können eine Rolle in der Organisation Ihres VMware Cloud Director-Anbieters erstellen.

Nach der ersten Installation und Einrichtung von VMware Cloud 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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Rollen** aus.
- 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 VMware Cloud 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**.

Ergebnisse

Die neu erstellte Rolle ist für die Zuweisung zu Benutzern in Ihrer Anbieterorganisation verfügbar.

Klonen einer Anbieterrolle

Sie können eine vorhandene Anbieterrolle als Vorlage für die Erstellung einer neuen Rolle verwenden.

Voraussetzungen

Stellen Sie sicher, dass Sie über die Rechte zum Hinzufügen neuer Rollen in VMware Cloud Director verfügen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Rollen** aus.
- 3 Wählen Sie die Rolle aus, die Sie klonen möchten, und klicken Sie auf **Klonen**.

- 4 Geben Sie im Fenster **Rolle klonen** einen Namen und eine Beschreibung für die geklonte Rolle ein.
- 5 (Optional) Um die geklonten Rechte zu bearbeiten, aktivieren Sie die Umschaltoption **Ausgewählte Rechte ändern** und aktivieren bzw. deaktivieren Sie die Rechte, die Sie für die geklonte Rolle ändern möchten.
- 6 Klicken Sie auf **Speichern**.

Anzeigen oder Bearbeiten einer Anbieterrolle

Sie können die Rechte anzeigen, die in einer Rolle enthalten sind, die für Ihre VMware Cloud Director-Anbieterorganisation lokal ist. Sie können den Namen, die Beschreibung und die Rechte einer Rolle bearbeiten.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Rollen** aus.
- 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 VMware Cloud Director-Anbieterorganisation nicht mehr verwenden.

Voraussetzungen

Die Rolle, die Sie löschen möchten, darf keinem Benutzer zugewiesen sein.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Rollen** aus.
- 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 VMware Cloud Director-Anbieterorganisation hinzufügen und in diese importieren.

Informationen zum Verwalten von Organisationsbenutzern und -gruppen finden Sie im *Handbuch für das VMware Cloud 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 VMware Cloud Director Mandantenportal*.

Erstellen eines Anbieterbenutzers

Sie können in der Organisation Ihres VMware Cloud Director-Anbieters einen Benutzer erstellen.

Während der Installation und Einrichtung von VMware Cloud 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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Benutzer** aus.
- 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 VMware Cloud Director-Anbieterorganisation importieren.

Voraussetzungen

[Konfigurieren einer System-LDAP-Verbindung](#) oder [Konfigurieren Ihres Systems für die Verwendung eines SAML-Identitätsanbieters](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Benutzer** aus.
- 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	<ol 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	<ol 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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Benutzer** aus.
- 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 VMware Cloud Director anmelden.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Benutzer** aus.
- 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 VMware Cloud 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 in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Benutzer** aus.
- 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 unter [Konfigurieren der Kennwortrichtlinie](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Benutzer** aus.
- 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 VMware Cloud Director Mandantenportal*.

Importieren einer Anbietergruppe

Sie können Gruppen aus einem zuvor konfigurierten LDAP- oder SAML-Identitätsanbieter in Ihre VMware Cloud Director-Anbieterorganisation importieren.

Voraussetzungen

[Konfigurieren einer System-LDAP-Verbindung](#) oder [Konfigurieren Ihres Systems für die Verwendung eines SAML-Identitätsanbieters](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Gruppen** aus.
- 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 VMware Cloud Director-Anbieterorganisation importiert haben, und Sie können die Rolle der Mitglieder einer Gruppe ändern.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Gruppen** aus.
- 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 VMware Cloud Director-Anbieterorganisation entfernen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Anbieter** die Option **Gruppen** aus.
- 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

VMware Cloud 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:

- Bearbeiten der allgemeinen Systemeinstellungen
- Allgemeine Systemeinstellungen
- Konfigurieren der System-E-Mail-Einstellungen
- Ändern der VMware Cloud Director-Lizenz
- Konfigurieren der Einstellungen für die Katalogsynchronisierung
- Konfigurieren und Überwachen von blockierenden Aufgaben und Benachrichtigungen
- Konfigurieren von öffentlichen Adressen
- Verwalten von Identitätsanbietern
- Verwalten von Plug-Ins
- Anpassen der VMware Cloud Director-Portale
- Konfigurieren der Kennwortrichtlinie
- Konfigurieren von vSphere-Diensten

Bearbeiten der allgemeinen Systemeinstellungen

VMware Cloud Director enthält allgemeine Systemeinstellungen, die sich auf Aktivitätsprotokolle, Netzwerke, Sitzungszeitüberschreitungen, Zertifikate, Unternehmens- und Vorgangsgrenzwerte usw. beziehen. Die Standardeinstellungen sind in vielen Umgebungen geeignet; Sie können die Einstellungen jedoch bei Bedarf an Ihre Anforderungen anpassen.

Eine Liste der änderbaren Eigenschaften finden Sie unter [Allgemeine Systemeinstellungen](#).

Hinweis Informationen zum Ändern von Datum, Uhrzeit oder Zeitzone der VMware Cloud Director-Appliance finden Sie unter <https://kb.vmware.com/kb/59674>.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Einstellungen** auf **Allgemein**.
- 3 Klicken Sie für den zu ändernden Abschnitt auf **Bearbeiten**, bearbeiten Sie die Eigenschaften und klicken Sie auf **Speichern**.

Allgemeine Systemeinstellungen

VMware Cloud Director enthält allgemeine Systemeinstellungen, die Sie an Ihre Anforderungen anpassen können.

Tabelle 11-1. Allgemeine Systemeinstellungen

Name	Kategorie	Beschreibung
Activity log history to keep	Aktivitätsprotokoll	Anzahl der Tage, über die der Protokollverlauf aufbewahrt wird, bevor er gelöscht wird. Geben Sie 0 ein, um Protokolle nie zu löschen.
Activity log history shown	Aktivitätsprotokoll	Anzahl der Tage des Protokollverlaufs, die angezeigt werden. Um alle Aktivitäten anzuzeigen, geben Sie 0 ein.
Display debug information	Aktivitätsprotokoll	Aktivieren Sie diese Einstellung, um die Debug-Informationen im VMware Cloud Director-Aufgabenprotokoll anzuzeigen.
IP address release timeout	Netzwerk	Anzahl an Sekunden, für die freigegebene IP-Adressen gehalten werden, bevor sie erneut für eine Zuweisung verfügbar gemacht werden. Die Standardeinstellung beträgt 2 Stunden (7200 Sekunden), damit alte Einträge aus Client-ARP-Tabellen ablaufen können.
Allow Overlapping External Networks	Netzwerk	Um externe Netzwerke hinzuzufügen, die auf demselben Netzwerksegment ausgeführt werden, aktivieren Sie das Kontrollkästchen. Aktivieren Sie diese Einstellung nur dann, wenn Sie nicht-VLAN-basierte Methoden zum Isolieren Ihrer externen Netzwerke anwenden.
Allow FIPS mode	Netzwerk	Ermöglicht die Aktivierung des FIPS-Modus auf Edge-Gateways. Erfordert NSX 6.3 oder höher. Informationen zum FIPS-Modus finden Sie in der Dokumentation zu <i>VMware NSX for vSphere</i> .
Default syslog server settings for networks	Netzwerk	Geben Sie IP-Adressen für bis zu zwei Syslog-Server ein, die von Netzwerken verwendet werden sollen. Diese Einstellung gilt nicht für von Cloud-Zellen verwendete Syslog-Server.
Provider Locale	Lokalisierung	Wählen Sie ein Gebietsschema für Provider-Aktivitäten aus. Diese Einstellung wirkt sich auf Protokolleinträge, per E-Mail versendete Warnmeldungen usw. aus.

Tabelle 11-1. Allgemeine Systemeinstellungen (Fortsetzung)

Name	Kategorie	Beschreibung
Idle session timeout	Zeitüberschreitungen	Dauer, für die die VMware Cloud Director-Anwendung aktiv bleibt, wenn keine Benutzerinteraktion erfolgt.
Maximum session timeout	Zeitüberschreitungen	Maximale Dauer, für die die VMware Cloud Director-Anwendung aktiv bleibt.
Host refresh frequency	Zeitüberschreitungen	Gibt an, wie häufig VMware Cloud Director überprüft, ob auf seine ESXi-Hosts zugegriffen werden kann.
Host hung timeout	Zeitüberschreitungen	Wählen Sie aus, wie lange gewartet wird, bis ein Host als im Stillstand gekennzeichnet wird.
Transfer session timeout	Zeitüberschreitungen	Dauer, bis eine angehaltene oder abgebrochene Uploadaufgabe (z. B. Upload von Medien oder vApp-Vorlagen) mit Fehler beendet wird. Eine Änderung dieser Einstellung hat keine Auswirkungen auf Uploadaufgaben, die aktuell ausgeführt werden.
Enable upload quarantine with a timeout of __ seconds	Zeitüberschreitungen	Aktivieren Sie dieses Kontrollkästchen und geben Sie eine Zahl ein, die dem Zeitlimit für die Quarantänedauer von hochgeladenen Dateien entspricht.
Verify vCenter and vSphere SSO certificates	Zertifikate	VMware Cloud Director überprüft die Zertifikate immer. Wenn diese Option aktiviert ist, werden die Hostnamen in den vCenter Server-Zertifikaten überprüft.
Verify NSX Manager certificates	Zertifikate	VMware Cloud Director überprüft die Zertifikate immer. Wenn diese Option aktiviert ist, überprüft VMware Cloud Director die Hostnamen in den NSX Manager-Zertifikaten.
Edit Organization Limits	Organisations-VDC-Grenzwerte	Geben Sie die maximale Anzahl virtueller Datacenter pro Organisation ein oder wählen Sie Unbegrenzt aus.
Number of resource intensive operations running per user	Grenzwerte für den Vorgang	Geben Sie die maximale Anzahl von gleichzeitigen ressourcenintensiven Vorgängen pro Benutzer ein oder wählen Sie Unbegrenzt aus.
Number of resource intensive operations to be queued per user (in addition to running)	Grenzwerte für den Vorgang	Geben Sie die maximale Anzahl von ressourcenintensiven Vorgängen pro Benutzer in der Warteschlange ein oder wählen Sie Unbegrenzt aus.
Number of resource intensive operations running per organization	Grenzwerte für den Vorgang	Geben Sie die maximale Anzahl von gleichzeitigen ressourcenintensiven Vorgängen pro Organisation ein oder wählen Sie Unbegrenzt aus.
Number of resource intensive operations to be queued per organization	Grenzwerte für den Vorgang	Geben Sie die maximale Anzahl ressourcenintensiver Vorgänge pro Organisation in der Warteschlange ein oder wählen Sie Unbegrenzt aus.
Provide default vApp names	Andere	Aktivieren Sie dieses Kontrollkästchen, um VMware Cloud Director so zu konfigurieren, dass Standardnamen für neue vApps erzeugt werden.

Tabelle 11-1. Allgemeine Systemeinstellungen (Fortsetzung)

Name	Kategorie	Beschreibung
Make Allocation pool Org VDCs elastic	Andere	Aktivieren Sie das Kontrollkästchen, um den elastischen Zuteilungspool zu aktivieren, sodass alle virtuelle Datencenter der Zuweisungspool-Organisation elastisch werden. Bevor Sie diese Option deaktivieren, stellen Sie sicher, dass alle virtuellen Maschinen für jedes Organisations-VDC in einen einzelnen Cluster migriert wurden.
VM discovery enabled	Andere	Standardmäßig erkennt jedes Organisations-VDC automatisch vCenter-VMs, die in einem Ressourcenpool erstellt wurden, der dem VDC zugrunde liegt. Deaktivieren Sie das Kontrollkästchen, um diese Option für alle VDCs im System zu deaktivieren.

Konfigurieren der System-E-Mail-Einstellungen

Sie können die System-E-Mail-Einstellungen bearbeiten, einschließlich der Konfiguration der SMTP-Servereinstellungen und der VMware Cloud Director-Benachrichtigungseinstellungen.

VMware Cloud Director benötigt einen SMTP-Server, um E-Mails zur Benachrichtigung von Benutzern und für Systemwarnungen an Benutzer des Systems zu versenden.

VMware Cloud Director versendet eine Systemwarnmeldung per E-Mail, wenn wichtige Informationen mitgeteilt werden müssen. So versendet VMware Cloud Director beispielsweise eine Warnung, wenn auf einem Datenspeicher der Speicherplatz knapp wird. Sie können VMware Cloud Director so konfigurieren, dass Warnmeldungen per E-Mail entweder an alle Systemadministratoren oder an eine festgelegte Liste von E-Mail-Adressen gesendet werden.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Fensterbereich unter **Einstellungen** die Option **E-Mail** aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie den DNS-Hostnamen oder die IP-Adresse des SMTP-Mailservers ein.
- 4 Geben Sie die Portnummer des SMTP-Servers ein.
- 5 (Optional) Wenn für den SMTP-Server ein Benutzername erforderlich ist, aktivieren Sie die Option **Authentifizierung erforderlich** und geben Sie einen Benutzernamen und das zugehörige Kennwort für das SMTP-Konto ein.
- 6 Wählen Sie die Registerkarte **Benachrichtigungseinstellungen** aus.
- 7 Geben Sie die E-Mail-Adresse ein, die in den VMware Cloud Director-E-Mail-Nachrichten als Absender angezeigt werden soll.

VMware Cloud Director verwendet die Absender-E-Mail-Adresse, um Warnmeldungen zum Ablauf von Laufzeit- und Speicher-Leases zu versenden.

- 8 (Optional) Geben Sie Text für das Betreffpräfix ein.
- 9 Wählen Sie die Empfänger der Benachrichtigungen aus.
Standardmäßig erhalten nur Organisationsadministratoren die SMTP-Benachrichtigungen.
- 10 Klicken Sie auf **Speichern**.
- 11 (Optional) Testen Sie die SMTP-Einstellungen.
 - a Klicken Sie auf **Testen**.
 - b Wenn Sie die Option **Authentifizierung erforderlich** aktiviert haben, geben Sie das Kennwort für den SMTP-Server ein.
 - c Geben Sie eine E-Mail-Adresse für das Ziel ein und klicken Sie auf **Testen**.

Ändern der VMware Cloud Director-Lizenz

VMware Cloud Director benötigt zur Ausführung einen gültigen Lizenzschlüssel (in Form einer Seriennummer). Sie können die Lizenzierungsinformationen, die Sie während der Erstkonfiguration von VMware Cloud Director eingegeben haben, ändern.

Die VMware Cloud Director-Produktseriennummer und der vCenter Server-Lizenzschlüssel sind nicht identisch. Sie können die VMware Cloud Director-Seriennummer über das VMware-Lizenzportal erhalten.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Fensterbereich **Lizenz** aus und klicken Sie auf **Bearbeiten**.
- 3 Geben Sie eine neue Seriennummer ein und klicken Sie dann auf **Übernehmen**.

Konfigurieren der Einstellungen für die Katalogsynchronisierung

Sie können die Einstellungen für die Katalogsynchronisierung für alle Organisationen und Kataloge bearbeiten, einschließlich der Aktualisierungsrate der Katalogabonnements.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Fensterbereich unter **Einstellungen** die Option **Katalog** aus.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Aktivieren Sie die Katalogsynchronisierung.
- 5 Legen Sie die Start- und Beendigungszeiten für die Synchronisierung fest.

- 6 Legen Sie das Synchronisierungsintervall fest.

Das Synchronisierungsintervall ist die Aktualisierungsrate der Katalogabonnements.

- 7 Klicken Sie auf **Speichern**.

Nächste Schritte

Informationen zur Konfiguration der Drosselung der Katalogsynchronisation finden Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

Konfigurieren und Überwachen von blockierenden Aufgaben und Benachrichtigungen

Sie können blockierende Aufgabe und Benachrichtigungen verwenden, um VMware Cloud Director zum Senden AMQP-Meldungen, die von bestimmten Ereignissen ausgelöst wurden, zu konfigurieren.

Manche dieser Nachrichten sind lediglich Benachrichtigungen darüber, dass das Ereignis stattgefunden hat. Andere Nachrichten veröffentlichen Informationen auf einem designierten AMQP-Endpunkt, die angeben, dass eine angeforderte Aktion blockiert wurde und auf eine Aktion von einem an diesen Endpunkt gebundenen Clientanwendung wartet. Diese Nachrichten werden als blockierende Aufgaben bezeichnet.

Ein **Systemadministrator** kann einen systemweiten Satz von blockierenden Aufgaben konfigurieren, die durch programmatische Aktionen eines AMQP-Clients gesteuert werden.

Konfigurieren eines AMQP Brokers

Wenn Sie möchten, dass VMware Cloud Director durch bestimmte Ereignisse ausgelöste AMQP-Meldungen senden, müssen Sie einen AMQP Broker konfigurieren. Sie können die AMQP-Meldungen verwenden, um die Handhabung einer zugrunde liegenden Benutzeranforderungsrichtlinie zu automatisieren.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie unter **Einstellungen** die Option **Erweiterbarkeit** aus.
Die Registerkarte **AMQP Broker** wird geöffnet.
- 3 Klicken Sie im Abschnitt **AMQP Broker** auf die Schaltfläche **Bearbeiten**.
- 4 Geben Sie den DNS-Hostnamen oder die IP-Adresse des AMQP-Hosts ein.
Den vollqualifizierten Domännennamen des RabbitMQ-Serverhosts, z. B. *amqp.example.com*.
- 5 Geben Sie den AMQP-Port ein.
Der Port, über den der Broker Nachrichten empfängt, lautet 5672.
- 6 Geben Sie den Austausch ein.

- 7 Geben Sie den vHost ein.

Der Standardwert ist /.

- 8 Geben Sie das Präfix ein.

- 9 (Optional) Um SSL zu verwenden, aktivieren Sie die Umschaltoption **SSL verwenden** und wählen Sie eine der Zertifikatoptionen aus.

Der AMQP-Dienst von VMware Cloud Director versendet standardmäßig unverschlüsselte Nachrichten. Sie können den AMQP-Dienst so konfigurieren, dass diese Nachrichten mit SSL verschlüsselt werden. Sie können den Dienst auch so konfigurieren, dass er das Broker-Zertifikat überprüft, indem Sie den standardmäßigen JCEKS Trust Store der Java-Laufzeitumgebung auf der VMware Cloud Director-Zelle verwenden, normalerweise unter `$VCLLOUD_HOME/jre/lib/security/cacerts`.

Option	Beschreibung
Alle Zertifikate akzeptieren	Der CN-Datensatz aus dem Zertifikatbesitzerfeld muss dem Hostnamen des AMQP-Brokers entsprechen. Wenn Sie Zertifikate verwenden möchten, die nicht dem Broker-Hostnamen entsprechen, aktivieren Sie die Umschaltoption Alle Zertifikate akzeptieren .
SSL-Zertifikat	Laden Sie das SSL-Zertifikat hoch.
SSL Key Store (JCEKS)	Laden Sie den SSL Key Store hoch und geben Sie das Kennwort für den Keystore ein.

- 10 Geben Sie einen Benutzernamen und ein Kennwort für die Verbindung zum AMQP-Host ein.
- 11 Klicken Sie auf **Speichern**.
- 12 (Optional) Um die Einstellungen zu testen, klicken Sie unter dem Abschnitt **AMQP Broker** auf die Schaltfläche **Testen** und geben Sie das Kennwort ein.
- 13 (Optional) Zum Veröffentlichen von Prüfungsereignissen für den AMQP Broker klicken Sie unter dem Abschnitt **Nicht blockierende AMQP-Benachrichtigungen** auf die Schaltfläche **Bearbeiten** und aktivieren Sie die Umschaltoption **Benachrichtigungen aktivieren**.

Konfigurieren der Einstellungen von blockierenden Aufgaben

Sie können bestimmte Vorgänge als blockierende Aufgabe konfigurieren. Diese Vorgänge werden angehalten, bis ein **Systemadministrator** darauf reagiert oder ein vorkonfigurierter Timer abläuft. Sie können die Zeitüberschreitungseinstellungen und Standardaktionen für blockierende Aufgaben festlegen. Die Einstellungen gelten für alle Organisationen in der Installation.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie unter **Einstellungen** die Option **Erweiterbarkeit** aus.
- 3 Wählen Sie die Registerkarte **Blockierende Aufgaben** aus.

- 4 Um den Standardwert für die Zeitüberschreitung der Erweiterung und die Standardaktion bei Zeitlimitüberschreitung zu bearbeiten, klicken Sie unter dem Abschnitt **Allgemein** auf die Schaltfläche **Bearbeiten**.
 - a Bearbeiten Sie das **Standard-Zeitlimit für blockierende Aufgabe**.
 - b Bearbeiten Sie die **Standardaktion bei Zeitlimitüberschreitung**.
 Die **Standardaktion bei Zeitlimitüberschreitung** ist die Aktion, die durchgeführt wird, wenn ein **Standard-Zeitlimit für blockierende Aufgabe** überschritten wurde.
 - c Klicken Sie auf **Speichern**.
- 5 Um die Liste der Vorgänge, die als blockierende Aufgaben angesehen werden, zu bearbeiten, klicken Sie im Abschnitt **Vorgänge** auf **Bearbeiten**.
 - a Aktivieren oder deaktivieren Sie die Vorgänge in der Liste der blockierenden Aufgaben.
 - b Klicken Sie auf **Speichern**.

Überwachen blockierter Aufgaben

Sie können die aktuell blockierten Aufgaben überwachen oder die Aufgaben manuell abbrechen, fehlschlagen lassen oder fortsetzen, bevor der vorkonfigurierte Timer abläuft.

Voraussetzungen

Konfigurieren der Einstellungen von blockierenden Aufgaben

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste unter **Überwachen** die Option **Blockierende Aufgaben** aus.

Die Registerkarte zeigt eine Liste der aktuell blockierten Aufgabe an.

- 2 Wählen Sie die Aufgabe aus, die Sie manuell bearbeiten möchten.
- 3 Entscheiden Sie zwischen Abbrechen, Fehlschlagenlassen oder Wiederaufnehmen der Aufgabe und klicken Sie auf die entsprechende Schaltfläche.
- 4 Geben Sie eine Nachricht ein und klicken Sie auf **Speichern**.
 Die Meldung wird in den Aufgabendetails angezeigt.

Konfigurieren von öffentlichen Adressen

Zum Erfüllen der Anforderungen des Lastausgleichsdiensts oder Proxys können Sie die Webadressen des Standard-Endpoints für das VMware Cloud Director-Webportal, die VMware Cloud Director-API und den Konsolen-Proxy ändern.

Öffentliche Adressen sind Webadressen, die für Clients von VMware Cloud Director offengelegt werden. Die Standardwerte für diese Adressen werden während der Installation angegeben. Falls erforderlich, können Sie die Adressen aktualisieren.

Wenn VMware Cloud Director aus einer einzelnen Zelle besteht, erstellt das Installationsprogramm öffentliche Endpoints, die normalerweise ausreichenden API- und Webclient-Zugriff bieten. Installationen und Bereitstellungen, die mehrere Zellen umfassen, platzieren einen Lastausgleichsdienst normalerweise zwischen den Zellen und den Clients. Clients greifen über die Adresse des Lastausgleichsdiensts auf das System zu. Der Lastausgleichsdienst verteilt Client-Anforderungen auf die verfügbaren Zellen. Andere Netzwerkkonfigurationen, bei denen ein Proxy enthalten ist oder die Zellen in einer DMZ platziert werden, erfordern ebenfalls angepasste Endpoints. Endpoint-URL-Details gelten spezifisch für Ihre Netzwerkkonfiguration.

Die Endpoints für das VMware Cloud Director Tenant Portal und die VMware Cloud Director-Webkonsole erfordern vorzugsweise signierte SSL-Zertifikate. Beim Installieren oder Bereitstellen von VMware Cloud Director müssen Sie einen Pfad zu diesen Zertifikaten angeben. Wenn Sie einen dieser Endpoints nach der Installation oder Bereitstellung anpassen, müssen Sie möglicherweise neue Zertifikate installieren, die mit Endpoint-Details wie `hostname` und `subject alternative name` übereinstimmen.

Für die VMware Cloud Director-Appliance müssen Sie die Adresse des öffentlichen VMware Cloud Director-Konsolen-Proxys konfigurieren, da die Appliance eine einzelne IP-Adresse mit dem benutzerdefinierten Port `8443` für den Konsolen-Proxy-Dienst verwendet. Weitere Informationen finden Sie unter [Schritt 6](#).

Voraussetzungen

Stellen Sie sicher, dass Sie sich als **Systemadministrator** angemeldet haben. Nur ein **Systemadministrator** kann öffentliche Endpoints anpassen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Einstellungen** auf **Öffentliche Adressen**.
- 3 Um die öffentlichen Endpoints anzupassen, klicken Sie auf **Bearbeiten**.
- 4 Bearbeiten Sie zum Anpassen der VMware Cloud Director-URLs die **Webportal**-Endpoints.
 - a Geben Sie eine benutzerdefinierte öffentliche VMware Cloud Director-URL für (nicht sichere) HTTP-Verbindungen ein.
 - b Geben Sie eine benutzerdefinierte öffentliche VMware Cloud Director-URL für (sichere) HTTPS-Verbindungen ein und klicken Sie auf **Hochladen**, um die Zertifikate hochzuladen, die die Vertrauenskette für diesen Endpoint bilden.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich um das Zertifikat, das auf alle VMware Cloud Director-Zellen-Keystores mit dem Alias `consoleproxy` hochgeladen wurde. SSL-Terminierung der Konsolen-Proxy-Verbindungen auf einem Lastausgleichsdienst wird nicht unterstützt. Die Zertifikatskette muss ein Endpoint-Zertifikat, Zwischenzertifikate und ein Stammzertifikat im PEM-Format ohne einen privaten Schlüssel enthalten.

- 5 (Optional) Um die Cloud Director REST API- und die OpenAPI-URLs anzupassen, deaktivieren Sie die Option **Webportaleinstellungen verwenden**.

- a Geben Sie eine benutzerdefinierte HTTP-Basis-URL ein.

Wenn Sie die HTTP-Basis-URL beispielsweise auf **http://vcloud.example.com** setzen, können Sie auf die VMware Cloud Director-API unter `http://vcloud.example.com/api` und auf VMware Cloud Director OpenAPI unter `http://vcloud.example.com/cloudapi` zugreifen.

- b Geben Sie eine benutzerdefinierte HTTPS REST API-Basis-URL ein und klicken Sie auf **Hochladen**, um die Zertifikate hochzuladen, die die Vertrauensketten für diesen Endpoint bilden.

Wenn Sie die Basis-URL der HTTPS-REST API beispielsweise auf **https://vcloud.example.com** setzen, können Sie auf die VMware Cloud Director-API unter `https://vcloud.example.com/api` und auf VMware Cloud Director OpenAPI unter `https://vcloud.example.com/cloudapi` zugreifen.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich entweder um das Zertifikat, das auf alle VMware Cloud Director-Zellen-Keystores mit dem Alias `http` hochgeladen wurde, oder um das VIP-Zertifikat des Lastausgleichsdiensts, wenn SSL-Terminierung verwendet wird. Die Zertifikatskette muss ein Endpoint-Zertifikat, Zwischenzertifikate und ein Stammzertifikat im PEM-Format ohne einen privaten Schlüssel enthalten.

- 6 Geben Sie die Adresse eines benutzerdefinierten öffentlichen VMware Cloud Director-Konsolen-Proxys ein.

- Passen Sie die Adresse des öffentlichen Konsolen-Proxys der VMware Cloud Director-Appliance an.

Diese Adresse ist der vollqualifizierte Domänenname (FQDN) der `eth0`-Netzwerkkarte der VMware Cloud Director-Appliance, die entweder durch den FQDN oder die IP-Adresse mit dem benutzerdefinierten Port `8443` für den Konsolen-Proxy-Dienst angegeben wird.

- Passen Sie die Adresse des öffentlichen Konsolen-Proxys für VMware Cloud Director unter Linux an.

Bei dieser Adresse handelt es sich um den vollqualifizierten Domännennamen (FQDN) des VMware Cloud Director-Servers oder Lastausgleichsdiensts mit der Portnummer. Der Standardport lautet `443`.

Geben Sie für eine VMware Cloud Director-Appliance-Instanz mit dem FQDN `vcloud.example.com` beispielsweise **vcloud.example.com:8443** ein.

VMware Cloud Director verwendet die Konsolen-Proxy-Adresse beim Öffnen eines Remote-Konsolenfensters auf einer VM.

- 7 Klicken Sie auf **Speichern**.

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 VMware Cloud 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.

Ab Version 10.1 wird VMware Cloud Director zu einem zentralisierten, mandantenfähigen Speicherbereich für die Zertifikatsverwaltung. Auf diese Weise zentralisiert VMware Cloud Director alle Zertifikate an einem Ort, sodass **Systemadministratoren** und **Organisationsadministratoren** alle Zertifikate, die von verschiedenen Komponenten im System verwendet werden, anzeigen, überprüfen und verwalten können. Sie können die VMware Cloud Director-API zum Hinzufügen, Aktualisieren oder Entfernen von Zertifikaten aus dem neuen mandantenfähigen Speicherbereich verwenden. Weitere Informationen finden Sie im *VMware Cloud Director API-Schema-Referenz*.

Wenn Sie einen neuen LDAP-Server-Endpoint hinzufügen oder bearbeiten, prüft die VMware Cloud Director-Benutzeroberfläche diesen Endpoint für alle von ihm bereitgestellten Zertifikate. VMware Cloud Director fügt alle Zertifikate, denen Sie vertrauen, einem zentralisierten Zertifikatspeicherbereich hinzu.

Konfigurieren einer System-LDAP-Verbindung

Um VMware Cloud 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 in der oberen Navigationsleiste **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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Organisationen** aus.
- 3 Klicken Sie auf den Namen der gewünschten Organisation.
Sie werden zum VMware Cloud Director-Mandantenportal der Organisation umgeleitet.
- 4 Wählen Sie in der oberen Navigationsleiste **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 VMware Cloud 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 konfigurieren möchten, legen Sie die Details des LDAP-Servers fest. Sie können die Verbindung testen, um sicherzustellen, dass Sie die korrekten Einstellungen eingegeben haben und die Benutzer- und Gruppenattribute korrekt zugeordnet sind. Sobald Sie über eine funktionierende LDAP-Verbindung verfügen, können Sie die Benutzer- und Gruppeninformationen jederzeit mit dem LDAP-Server synchronisieren.

Voraussetzungen

Wenn Sie eine Verbindung mit einem LDAP-Server über SSL (LDAPS) herstellen möchten, stellen Sie sicher, dass das Zertifikat Ihres LDAP-Servers mit der in Java 8 Update 181 eingeführten Endpoint-Identifikation konform ist. Der CN (Common Name, allgemeiner Name) oder der SAN (Subject Alternative Name, alternativer Antragstellername) des Zertifikats muss mit dem FQDN des LDAP-Servers übereinstimmen. Weitere Informationen finden Sie in den *Java 8-Versionsänderungen* unter <https://www.java.com>.

Verfahren

- 1 Geben Sie auf der Registerkarte **Verbindung** die erforderlichen Informationen für die LDAP-Verbindung ein.

Erforderliche Informationen	Beschreibung
Server	Der Hostname oder die IP-Adresse des LDAP-Servers.
Port	Die Nummer des Ports, den der LDAP-Server überwacht. Der Standardport für LDAP ist Port 389. Der Standardport für LDAPS ist Port 636.
Base Distinguished Name	Der Base Distinguished Name (DN) ist der Speicherort in dem LDAP-Verzeichnis, in dem VMware Cloud Director verbunden werden soll. Um die Verbindung auf Root-Ebene herzustellen, geben Sie nur die Domänenkomponenten ein, beispielsweise DC=beispiel,DC=com . Wenn Sie eine Verbindung mit einem Knoten in der Domänenbaumstruktur herstellen möchten, geben Sie den Distinguished Name für diesen Knoten ein, beispielsweise OU=ServiceDirector,DC=beispiel,DC=com . Wenn Sie die Verbindung unter Verwendung eines spezifischen Knotens in dem Verzeichnis herstellen, wird der Verzeichnissbereich, auf den VMware Cloud Director zugreifen kann, entsprechend eingeschränkt.
Connector-Typ	Der Typ Ihres LDAP-Servers. Kann Active Directory oder OpenLDAP sein.
SSL verwenden	Wenn es sich bei Ihrem Server um einen LDAPS-Server handelt, aktivieren Sie dieses Kontrollkästchen.
Alle Zertifikate akzeptieren	Wenn es sich bei Ihrem Server um einen LDAPS-Server handelt, aktivieren Sie dieses Kontrollkästchen oder laden Sie das LDAP-SSL-Zertifikat hoch.
Benutzerdefinierter Truststore	Wenn es sich bei Ihrem Server um einen LDAPS-Server handelt, klicken Sie entweder auf das Symbol zum Hochladen () und importieren Sie ein LDAP-SSL-Zertifikat oder wählen Sie Alle Zertifikate akzeptieren aus.
Authentifizierungsmethode	Die einfache Authentifizierung besteht darin, den DN und das Kennwort des Benutzers an den LDAP-Server zu senden. Wenn Sie LDAP verwenden, wird das LDAP-Kennwort als Klartext über das Netzwerk gesendet. Wenn Sie Kerberos verwenden möchten, müssen Sie die LDAP-Verbindung mithilfe der vCloud-API konfigurieren.

Erforderliche Informationen	Beschreibung
Benutzername	<p>Geben Sie den vollständigen LDAP-DN (Distinguished Name) eines Dienstkontos mit Domänenadministratorrechten ein. VMware Cloud Director verwendet dieses Konto, um das LDAP-Verzeichnis abzufragen und Benutzerinformationen abzurufen.</p> <p>Wenn der LDAP-Server so konfiguriert ist, dass Lesezugriff auch ohne Angabe eines Benutzernamens möglich ist, können diese Textfelder frei gelassen werden.</p>
Kennwort	<p>Das Kennwort für das Dienstkonto, das eine Verbindung mit dem LDAP-Server herstellt.</p> <p>Wenn der LDAP-Server so konfiguriert ist, dass Lesezugriff auch ohne Angabe eines Benutzernamens möglich ist, können diese Textfelder frei gelassen werden.</p>

- 2 Klicken Sie auf die Registerkarte **Benutzerattribute**, überprüfen Sie die Standardwerte für die Benutzerattribute und ändern Sie diese, falls in Ihrem LDAP-Verzeichnis ein anderes Schema verwendet wird.
- 3 Klicken Sie auf die Registerkarte **Gruppenattribute**, überprüfen Sie die Standardwerte für die Gruppenattribute und ändern Sie diese, falls in Ihrem LDAP-Verzeichnis ein anderes Schema verwendet wird.
- 4 Klicken Sie auf **Speichern**.
- 5 Wenn Sie das Kontrollkästchen **SSL verwenden** aktiviert haben und das Zertifikat des LDAPS-Servers noch nicht als vertrauenswürdig eingestuft wurde, bestätigen Sie im Fenster **Vertrauenswürdigkeitszertifikat**, dass Sie dem vom Server-Endpoint bereitgestellten Zertifikat vertrauen.
- 6 So testen Sie die LDAP-Verbindungseinstellungen und die LDAP-Attributzuordnungen:
 - a Klicken Sie auf **Testen**.
 - b Geben Sie das Kennwort des von Ihnen konfigurierten Benutzers des LDAP-Servers ein und klicken Sie auf **Testen**.

Wenn die Verbindung erfolgreich hergestellt wurde, wird ein grünes Häkchen angezeigt.

Die abgerufenen Benutzer- und Gruppenattributwerte werden in einer Tabelle angezeigt. Die Werte, die LDAP-Attributen erfolgreich zugeordnet wurden, werden mit grünen Häkchen markiert. Die Werte, bei denen es sich um keine zugeordneten LDAP-Attribute handelt, sind leer und werden mit roten Ausrufezeichen markiert.
 - c Klicken Sie zum Beenden auf **Abbrechen**.

- 7 Um VMware Cloud Director mit dem konfigurierten LDAP-Server zu synchronisieren, klicken Sie auf **Synchronisieren**.

VMware Cloud Director synchronisiert die Benutzer- und Gruppeninformationen regelmäßig mit dem LDAP-Server. Wie häufig dies geschieht, hängt vom Synchronisierungsintervall ab, das Sie in den allgemeinen Systemeinstellungen festlegen.

Warten Sie einige Minuten, bis die Synchronisierung abgeschlossen ist.

Ergebnisse

Sie können Benutzer und Gruppen aus dem neu konfigurierten LDAP-Server importieren.

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 VMware Cloud 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 in der oberen Navigationsleiste **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 VMware Cloud 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

VMware Cloud Director-Plug-Ins erweitern die Funktionen von Service Provider Admin Portal und von VMware Cloud 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 VMware Cloud Director installiert.

CPOM-Erweiterung

Bietet die Möglichkeit zum Anzeigen und Verwalten von dedizierten vCenter Server-Instanzen und -Proxys mithilfe von VMware Cloud Director Tenant Portal.

Portal anpassen

Bietet die Möglichkeit zum Anpassen von VMware Cloud Director Service Provider Admin Portal und VMware Cloud Director Tenant Portal.

vCloud-Verfügbarkeit

Das VMware vCloud[®] Availability[™]-Plug-In bietet die Möglichkeit, auf das vCloud Availability Portal direkt von der VMware Cloud Director-Benutzeroberfläche. Weitere Informationen finden Sie in der [vCloud Availability-Dokumentation](#).

Hochladen eines Plug-Ins

Sie können zusätzliche Plug-Ins in das VMware Cloud 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 in der oberen Navigationsleiste **Mehr > 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 VMware Cloud Director Service Provider Admin Portal zur Verfügung.
Mandanten	Die Plug-In-Funktion steht nun im VMware Cloud 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 in der oberen Navigationsleiste **Mehr > 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 VMware Cloud Director Service Provider Admin Portal entfernen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Mehr > 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 in der oberen Navigationsleiste **Mehr > 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 VMware Cloud Director Service Provider Admin Portal verfügbar.
Mandanten	Die Plug-In-Funktion wird im VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal und für das VMware Cloud Director Tenant Portal jeder Organisation festlegen. Darüber hinaus können Sie benutzerdefinierte Links zu den beiden oberen rechten Menüs in den VMware Cloud 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 VMware Cloud Director OpenAPI* auf <https://code.vmware.com>.

Portal-Branding

Im Rahmen der Installation enthält VMware Cloud 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 VMware Cloud Director Service Provider Admin Portal anpassen können. Das VMware Cloud 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 *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

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.

VMware Cloud Director unterstützt die folgenden benutzerdefinierten Variablen im `url`-Wert für einen benutzerdefinierten Link:

Tabelle 11-2. 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}/vdc
```

im VMware Cloud Director Tenant Portal für die Organisation „myorg“ wird konvertiert in:

```
url: https://host:port/tenant/myorg/vdc
```

Konfigurieren der Kennwortrichtlinie

Um zu verhindern, dass sich ein Benutzer nach einer bestimmten Anzahl von fehlgeschlagenen Versuchen bei VMware Cloud Director anmeldet, können Sie die Kontosperrung aktivieren.

Änderungen an der System-Kontosperrungsrichtlinie gelten für alle neuen Organisationen. Organisationen, die vor dem Ändern der Kontosperrungsrichtlinie erstellt wurden, müssen auf Organisationsebene geändert werden.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Einstellungen** auf **Kennwortrichtlinie**.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Um die Kontosperrung zu aktivieren, aktivieren Sie die Option **Kontosperrung**.
- 5 Wählen Sie die Anzahl der ungültigen Anmeldungen aus, die akzeptiert werden sollen, bevor ein Konto gesperrt wird.
- 6 Wählen Sie das Sperrungsintervall aus.
- 7 Um die **Systemadministrator**-Kontosperrung zu aktivieren, aktivieren Sie die Option **Systemadministratorkonto kann gesperrt werden**.
- 8 Klicken Sie auf **Speichern**.

Konfigurieren von vSphere-Diensten

Sie können VMware Cloud Director für die Verwendung von vCenter Single Sign-On konfigurieren und aktivieren, damit der vSphere-Identitätsanbieter die Systemadministratoren authentifiziert.

vCenter Lookup Service enthält Topologieinformationen über die vSphere-Infrastruktur und ermöglicht es vSphere-Komponenten, sich miteinander sicher zu verbinden.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Fensterbereich unter **Einstellungen** die Option **vSphere Dienste** aus.
- 3 Konfigurieren Sie die vSphere-Dienste.
 - Um VMware Cloud Director beim vCenter Lookup Service zu registrieren, klicken Sie auf **Registrieren**.
 - Um die Registrierung von VMware Cloud Director beim vCenter Lookup Service zu aufheben, klicken Sie auf **Registrierung aufheben**.
- 4 Geben Sie die vCenter Lookup Service-URL ein, z. B. `https://Hostname:443/lookupservice/sdk`.
- 5 Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für den vCenter Single Sign-On-Host ein, z. B. den `administrator@your_domain_name`-Benutzer.

Ergebnisse

Wenn Sie VMware Cloud Director beim vCenter Lookup Service registriert haben, müssen sich **Systemadministratoren** mit ihren vCenter Single Sign-On-Anmeldedaten bei VMware Cloud Director anmelden.

Überwachen von VMware Cloud 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.

Ab Version 9.1 bietet VMware Cloud Director keine Unterstützung von VMware vCenter Chargeback Manager. Weitere Informationen finden Sie unter [VMware-Produktinteroperabilitätstabellen](#).

Dieses Kapitel enthält die folgenden Themen:

- [VMware Cloud Director und Kostenberichte](#)
- [Anzeigen von Nutzungsinformationen für ein virtuelles Provider-Datencenter](#)

VMware Cloud Director und Kostenberichte

Sie können VMware vRealize Operations Tenant App für VMware Cloud Director verwenden, um ein System zur Erstellung von Kostenberichten für VMware Cloud 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 VMware Cloud 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-Mandanten-App für VMware Cloud Director als Dienstanbieter* und *Verwenden der vRealize Operations-Mandanten-App für VMware Cloud 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 in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
- 2 Wählen Sie im linken Bereich **Provider-VDCs** aus und klicken Sie 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director

Sie integrieren vRealize Orchestrator mit VMware Cloud Director über das VMware Cloud Director Service Provider Admin Portal.

Durch die Integration von vRealize Orchestrator mit VMware Cloud Director werden die Basisfunktionen von VMware Cloud Director erweitert, wodurch Dienstanbieteradministratoren komplexe Automatisierungsaufgaben mittels Workflow-Orchestrierung und Nutzung von Drittanbieter-Plug-Ins entwickeln können.

Über das VMware Cloud Director Service Provider Admin Portal können Dienstanbieteradministratoren Workflows aus registrierten vRealize Orchestrator-Serverinstanzen anzeigen, importieren und ausführen.

Im VMware Cloud 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 VMware Cloud Director

Zur Nutzung der Orchestrierung von Workflows und Automatisierung von Aufgaben über vRealize Orchestrator in VMware Cloud Director registrieren Sie eine vRealize Orchestrator-Instanz im VMware Cloud 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 VMware Cloud 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 in der oberen Navigationsleiste **Bibliotheken** 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 **Hinzufügen**.
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 443. Hinweis VMware Cloud 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 VMware Cloud Director registriert.

Erstellen einer Dienstkategorie

Sie können Dienste in Dienstkategorien einteilen.

Verfahren

- Wählen Sie in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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 VMware Cloud Director registriert ist.

Voraussetzungen

- Registrieren Sie eine vRealize Orchestrator-Instanz. Weitere Informationen finden Sie unter [Registrieren einer vRealize Orchestrator-Instanz bei VMware Cloud Director](#).
- Erstellen Sie eine Dienstkategorie. Weitere Informationen finden Sie unter [Erstellen einer Dienstkategorie](#).

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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 VMware Cloud Director-Dienst starten, fügt VMware Cloud 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 <code>True</code> , wenn der Benutzer, der den Dienst ausführt, ein Administrator ist.
_vdc_isAdmin	Veraltet. Hat den Wert <code>True</code> , 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 VMware Cloud Director erhalten haben
_vcd_apiEndpoint	VMware Cloud Director-REST API-Endpoint

Ändern einer Dienstkategorie

Sie können die Kategorie ändern, der ein Dienst angehört.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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 VMware Cloud 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 VMware Cloud Director-Benutzer diese Typen besitzen und entsprechend ihren Bedürfnissen verwalten und ändern. Durch Ausführen von Diensten können Dienstanbieterbenutzer und Organisationsbenutzer die benutzerdefinierten Entitäten instanziierten und Aktionen auf die Instanzen der Objekte anwenden.

Dieses Kapitel enthält die folgenden Themen:

- [Auffinden einer benutzerdefinierten Entität](#)
- [Bearbeiten einer benutzerdefinierten Entitätsdefinition](#)
- [Hinzufügen einer benutzerdefinierten Entitätsdefinition](#)
- [Benutzerdefinierte Entitätsinstanzen](#)
- [Verknüpfen einer Aktion mit einer benutzerdefinierten Entität](#)
- [Aufheben der Verknüpfung einer Aktion mit einer benutzerdefinierten 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 in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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. <code>sshHost</code> .
vRO	Wählen Sie im Dropdown-Menü den vRealize Orchestrator aus, den Sie zum Zuordnen der benutzerdefinierten Entitätsdefinition verwenden möchten. Hinweis Bei mehreren vRealize Orchestrator-Servern müssen Sie für jeden einzelnen Server eine benutzerdefinierte Entitätsdefinition erstellen.
Typ	Klicken Sie auf das Symbol für die Listenanzeige () , um durch die verfügbaren nach Plug-Ins gruppierten vRealize Orchestrator-Objekttypen zu navigieren. Beispielsweise SSH > Host . Wenn Sie den Namen des Typs kennen, können Sie ihn direkt im Textfeld eingeben. Beispiel: <code>SSH:Host</code> .
Überprüfen	Überprüfen Sie die von Ihnen angegebenen Details und klicken Sie auf Fertig , um den Erstellvorgang abzuschließen.

Ergebnisse

Die neue benutzerdefinierte Entitätsdefinition wird in der Kartenansicht angezeigt.


Benutzerdefinierte Entitätsinstanzen

Wenn Sie einen vRealize Orchestrator-Workflow mit einem Eingabeparameter ausführen, der einen Objekttyp darstellt, der bereits als benutzerdefinierte Entitätsdefinition in VMware Cloud Director definiert ist, wird der Ausgabeparameter als Instanz einer benutzerdefinierten Entität angezeigt.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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.
- 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 in der oberen Navigationsleiste **Bibliotheken** 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 in der oberen Navigationsleiste **Bibliotheken** 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 Diensteanbieter, alle Mandanten oder nur für ausgewählte Mandanten veröffentlicht werden soll.

- 4 Klicken Sie auf **Speichern**, um die Änderung zu bestätigen.

Die benutzerdefinierte Entitätsdefinition steht den ausgewählten Gruppen nun zur Verfügung.

Löschen einer benutzerdefinierten Entität

Sie können eine benutzerdefinierte Entitätsdefinition löschen, wenn die benutzerdefinierte Entität nicht mehr verwendet wird, nicht ordnungsgemäß konfiguriert wurde oder der vRealize Orchestrator-Typ einer anderen benutzerdefinierten Entität zugeordnet werden soll.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Bibliotheken** 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.